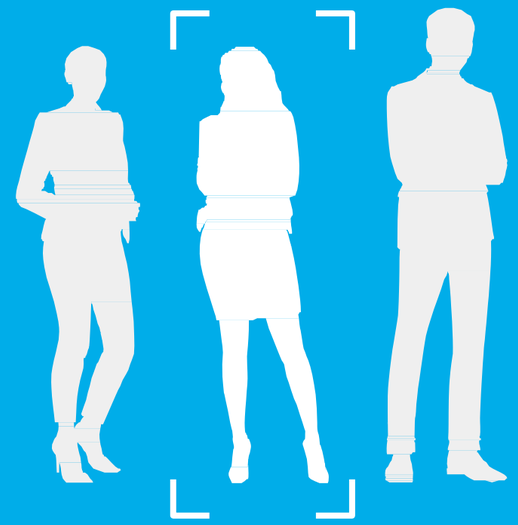
XpertHR College

AVG een jaar later. Hoe staat het er voor?



Wat komt er onder meer aan bod?

- AVG in een notendop;
- Acties AP sinds 25 mei 2018
- Datalekker door personeelsleden;
- Wat te doen met e-mailaccount van ex-werknemer?
- Wat mag je bewaren in een personeelsdossier?
- Bewaartermijnen persoonsgegevens personeelsleden;
- Inzage werknemer in personeelsdossier.

Wat regelt de AVG?

- De AVG geeft regels ten aanzien van het verwerken van persoonsgegevens;
- Een persoonsgegeven is elk gegeven aan de hand waarvan een levend persoon (de betrokkene) kan worden geïdentificeerd;
- Onder het verwerken vallen alle handelingen die uitgevoerd kunnen worden met persoonsgegevens.

Welke verplichtingen volgen uit de AVG? (1/2)

Iedere organisatie (verwerkersverantwoordelijke) is verantwoordelijk en moet aantonen dat de in de AVG opgenomen regels worden nageleefd.

Concreet moet:

- onder bepaalde omstandigheden een FG aangesteld worden;
- in kaart gebracht worden welke en hoe verwerkingen plaatsvinden;
- in bepaalde gevallen een DPIA uitgevoerd worden;
- een privacybeleid opgesteld worden (niet altijd verplicht, wordt wel door ons geadviseerd);
  - Welke maatregelen heeft de organisatie genomen om persoonsgegevens te beschermen?
  - Manier om aan de AP te laten zien dat de organisatie aan de AVG voldoet;
  - Medewerkersbewustzijn.
- passende beveiligingsmaatregelen getroffen worden (ook geheimhoudingsverklaringen);
- een register verwerkingen opgesteld en bijgehouden worden;

Welke verplichtingen volgen uit de AVG? (2/2)

- een register datalekken opgesteld en bijgehouden worden. In bepaalde gevallen moet melding plaatsvinden aan AP;
- vastgesteld worden wat het doel en de grondslag is van de gegevensverwerking;
- de manier waarop toestemming wordt gevraagd, verkregen en geregistreerd geëvalueerd worden;
- een betrokkene (bijv. werknemer) geïnformeerd worden door middel van een privacyverklaring;
- waar nodig verwerkersovereenkomsten gecontroleerd en gesloten worden;
- bepaald worden onder welke toezichthouder de organisatie valt en medewerking verleend worden.

Tips verwerkingsregister

- Maak gebruik van een geschikt model;
- Schakel van iedere afdeling een persoon in die kennis van zaken heeft (bijvoorbeeld de leidinggevende van de afdeling: productie, inkoop, verkoop, financiën en ICT);
- Geef duidelijk aan op welke locatie of in welk bestand persoonsgegevens bewaard worden en neem deze locaties of bestanden op in het register;
- Stel het verwerkingsregister vooral niet op per klant of werknemer, maar maak één register waarin je alles van alle klanten en werknemers benoemd.

De AP heeft niet stilgezeten sinds 25 mei 2018 (1/4)

Sinds 25 mei 2018 controleert de AP regelmatig of organisaties de regels naleven. Zo heeft de AP o.a.:

- ziekenhuizen en verzekeraars gecontroleerd op FG-verplichting;
- gecontroleerd of ondernemingen een register van verwerkingsactiviteiten bijhouden;
- verwerkersovereenkomsten gecontroleerd bij dertig organisaties;
- gecontroleerd of organisaties die hiertoe verplicht zijn een privacybeleid hebben.

De AP heeft niet stilgezeten sinds 25 mei 2018 (2/4)

Ook heeft de AP sinds de inwerkingtreding sancties opgelegd. Zo heeft zij o.a.:

- het UWV met sanctie (last onder dwangsom) gedwongen om gegevens beter te beveiligen;
- Uber een boete opgelegd voor het te laat melden van datalek;
- de Nationale Politie een last onder dwangsom opgelegd.

De AP heeft niet stilgezeten sinds 25 mei 2018 (3/4)

Naast het houden van toezicht en het doen van onderzoek, verstrekt de AP ook informatie, geeft zij adviezen en voorlichting. Zo heeft de AP:

- spelregels bekend gemaakt rond direct marketing;
- inzicht gegeven in gebruik camera's voor beveiligen eigendommen;
- aanbevelingen gedaan voor registers van verwerkingen;
- 10 tips gegeven voor professionele datalekregistratie;
- Aanbevelingen gedaan voor een privacybeleid.

N.B. AP organiseert 'Dag van de FG' op 27 mei 2019

De AP heeft niet stilgezeten sinds 25 mei 2018 (4/4)

- Tot slot moet de AP alle ingediende klachten in behandeling nemen (in tweede half jaar van 2018 waren dit er bijna 10.000).
  - 720 klachten en 298 datalekken zijn afgehandeld via een interventie.

- Ook heeft zij in 2018 bijna 21.000 meldingen van datalekken ontvangen.

Verplichtingen rondom datalekken

- De AVG kent verplichting register datalekken bij te houden;
- Register datalekken = document waaruit blijkt welke datalekken zich in de organisatie hebben voorgedaan;
- Datalekken moeten dus altijd geregistreerd worden in een intern register;
- Soms melden bij de AP (binnen 72 uur) en bij de betrokkene(n). Dit hangt af van de kans op nadelige gevolgen voor de betrokkene(n).

Maak beleid en informeer personeelsleden

- Zorg voor een register;
- Stel een of meerdere verantwoordelijke medewerkers aan;
- Zorg voor beleid / protocol datalekken;
  - Hierin staat hoe de organisatie en de medewerkers om moeten gaan met een datalek (meldingsprocedure):
  - bijvoorbeeld: instructie melden bij bepaalde medewerker, bepaalde medewerker beslist of gemeld wordt bij de AP en of betrokkene wordt geïnformeerd, datalek registreren in register datalekken (dit laatste altijd verplicht);
- Maak het personeel bekend met de inhoud van het beleid.

Omgang meldingen vanuit personeel

Wat doe je als een medewerker aangeeft dat een datalek heeft plaatsgevonden?

- Stap 1: Controleer of sprake is van een datalek;
- Stap 2: Zo ja, registreer datalek in register en neem zo nodig verbeteracties;
- Stap 3: Ga na of melding dient plaats te vinden aan AP en/of betrokkene(n).

Wanneer is sprake van een datalek?

1. Het moet gaan om persoonsgegevens;
2. De persoonsgegevens moeten blootgesteld zijn aan misbruik of verlies;
3. Dit blootstellen moet te wijten zijn aan een inbreuk op de beveiliging.

In welke situatie is er GEEN datalek?

A. Een HR-medewerker laat een personeelsbeoordeling van een accountmanager met daarin opgenomen zijn slechte financiële resultaten liggen in de kantine terwijl hij even lunch koopt. Collega's kunnen die beoordeling inzien terwijl ze daar niet toe bevoegd zijn;

B. Een door jullie ingehuurde ICT-er verwijdert een virus van een laptop van HR-medewerker en opent daarbij toevalligerwijs een adressenlijst van alle werknemers;

C. Een crimineel breekt in bij het interne netwerk van de organisatie en kopieert de gegevens van de werknemers.

Melden aan de AP?

- Hoofdregel: ieder datalek moet worden gemeld aan de AP;
- Uitzondering: wanneer het onwaarschijnlijk is dat er risico's zijn voor de privacy van betrokkenen (doel = echt onschuldige datalekken buiten beeld te houden);
- Datalek kan kwantitatief (omvang) en/of kwalitatief (gevoeligheid gegevens) ernstig zijn.

In welke situatie NIET melden aan de AP?

A. Een HR-medewerker laat een personeelsbeoordeling van een accountmanager met daarin opgenomen zijn slechte financiële resultaten liggen in de kantine terwijl hij even lunch koopt. Collega's kunnen die beoordeling inzien terwijl ze daar niet toe bevoegd zijn;

B. Een lijst met vakantieverzoeken van een medewerker is na het printen in het algemene kopieerhok achtergelaten;

C. Een medewerker mailt een e-mail met als bijlage een lijst met klantgegevens (bedrijfsnamen, contactpersonen en adressen van bedrijven) naar een verkeerd persoon buiten de organisatie.

Melden aan betrokkene(n)?

Melding moet plaatsvinden als het waarschijnlijk is dat het datalek een groot risico voor de betrokkene oplevert.

Kijk naar omstandigheden van geval. Let op kans op bijv. schade aan gezondheid, financiële schade of (identiteits)fraude.

In welke situatie niet melden aan betrokkene(n)?

A. Een HR-medewerker laat een personeelsbeoordeling van een accountmanager met daarin opgenomen zijn slechte financiële resultaten liggen in de kantine terwijl hij even lunch koopt. Collega's kunnen die beoordeling inzien terwijl ze daar niet toe bevoegd zijn;

B. Medewerkster verliest versleutelde telefoon met daarop toegang tot werk mailbox met e-mail van sollicitant inclusief CV en krantenmailing;

C. Medewerker verliest niet versleutelde laptop met daarop gegevens van klanten om facturen via automatische incasso te innen.

Wat mag je bewaren in een personeelsdossier? (1/2)

Hoofdregel luidt: alleen gegevens opnemen in dossier als dit noodzakelijk is voor het doel waarvoor het personeelsdossier is aangelegd.

Ook hier weer gelden algemene regels uit AVG:

- beschikken over doel en grondslag;
- niet meer gegevens bewaren dan nodig;
- gegevens niet langer bewaren dan noodzakelijk;
- informatieplicht richting werknemers;
- rekening houden met rechten werknemers.

Wat mag je bewaren in een personeelsdossier? (2/2)

Gegevens die opgenomen mogen worden in het personeelsdossier:

- klachten;
- waarschuwingen;
- verzuimfrequentie (hoe vaak de werknemer er niet is);
- verslagen van beoordelings- of functioneringsverslagen die de werknemer kent;
- kopie van het ID-bewijs;
- persoonlijke werkaantekeningen van de leidinggevende;
- arbeidsovereenkomst en eventuele addenda.

Bewaartermijnen persoonsgegevens personeelsleden (1/2)

- AVG kent geen concrete termijn voor het bewaren van gegevens;
- Wel richtlijn: gegevens bewaren tot het moment dat ze niet meer nodig zijn voor het doel waarvoor ze zijn verzameld of gebruikt;
- Andere wetten kennen wel concrete termijnen. Ook voor gegevens uit het personeelsdossier:
  - Uitvoeringsregeling loonbelasting: kopie identiteitsbewijs werknemer en loonbelastingverklaring tot vijf jaar na het einde van het dienstverband;
  - Wet op de Rijksbelastingen: gegevens salarisafspraken en andere gegevens die fiscaal relevant zijn tot zeven jaar na het einde van het dienstverband.

Bewaartermijnen persoonsgegevens personeelsleden (2/2)

Wat houdt richtlijn AVG in als geen andere wettelijke bewaartermijn geldt?

De AP geeft aan dat deze gegevens mogen worden bewaard tot twee jaar na het eindigen van het dienstverband.

Denk aan volgende gegevens:

- verslagen van functionerings- en beoordelingsgesprekken;
- arbeidsovereenkomsten;
- afspraken over promotie;
- degradatie of ontslag; of
- administratieve verzuimgegevens.

Zijn gegevens eerder niet meer nodig? Dan direct verwijderen!

Gegevens langer nodig? Denk aan conflict of rechtszaak. Dat mag.

Inzagerecht werknemer

Werknemers moeten de mogelijkheid krijgen om hun persoonsgegevens in te zien. Dit geldt in principe voor het gehele personeelsdossier, maar bijvoorbeeld ook voor in- en uitkloktijden bij de receptie.

Inzage weigeren?

- Alleen als hier een grond voor bestaat. Bijvoorbeeld als de privacy van een andere persoon daardoor onevenredig wordt geschaad.

Enkele tips om privacyrisico's te verkleinen

- Zorg ervoor dat niet iedereen binnen de organisatie toegang heeft tot alle gegevens: scherm gevoelige gegevens af;
- Beperk de opslag van persoonsgegevens zo veel mogelijk: reken af met die overvolle mailbox;
- Zorg dat er geen drempel bestaat om datalekken te melden.

Het volgende XpertHR college op 28 mei 2019

Wat staat er zoal op het programma?

- Ziekteverzuim: voldoet uw HR systeem en de verzuimregistratie al aan de eisen van de AVG?
- Gebruik foto’s en video’s van personeelsleden;
- Cameratoezicht op de werkplek;
- Controleren / testen van personeelsleden.

Bedankt voor het kijken!

Advocaat Steffie Schepers heeft ook een aantal stukken geschreven.

Deze zijn gratis te bekijken op XpertHR Actueel

Whitepaper AVG: Aandachtspunten voor HR **>> lees meer**

Checklist: in 10 stappen klaar voor de nieuwe privacywet >> **lees meer**