AVG / GDPR

VAN KRACHT PER 25 MEI 2018

AVG / GDPR

- De Algemene Verordening Gegevensbescherming (AVG/GDPR) is de vervanger van een Europese Richtlijn over privacy uit 1995, de basis voor onze Wet bescherming persoonsgegevens (Wbp).

- De AVG is vanaf 25 mei 2018 in de hele Europese Unie direct van toepassing. Dan geldt in alle landen van de EU hetzelfde recht als het om de privacy van burgers gaat en hebben toezichthouders overal dezelfde bevoegdheden.

- Vanaf die datum vervalt in Nederland de Wpb en zal de Autoriteit Persoonsgegevens controleren of de AVG wordt gevolgd.

PERSOONSGEGEVENS

- Wat zijn persoonsgegevens?

De AVG is van toepassing op het verwerken van persoonsgegevens.

Wanneer is daar sprake van?

‘persoongegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’

Dus elk gegeven dat kan leiden tot een natuurlijk persoon, direct of indirect, is dus een persoonsgegeven! Voorbeelden zijn:

Naam, foto, postcode+huisnummer, emailadres, kenteken, IP-adres, locatie

BIJZONDERE PERSOONSGEGEVENS

Verboden te verwerken, tenzij

Het is verboden om bijzondere persoonsgegevens te verwerken, tenzij in de AVG een specifieke grondslag is vermeld. Let er dus op dat deze gegevens niet zomaar worden verwerkt/verzameld.

Het gaat om:

- Ras of etnische afkomst
- Gezondheidsgegevens
- Biomedische gegevens
- Politieke opvattingen
- Lidmaatschap van een vakbond
- Strafrechtelijke gegevens
- Religieuze overtuigingen
- Genetische gegevens
- Gegevens m.b.t. seksueel gedrag of voorkeur

VERWERKEN

Wanneer verwerk je?

Alleen als je persoonsgegevens verwerkt, moet je je aan de privacyregels van de AVG houden. Maar, van verwerking is al heel snel sprake. Verwerking begint eigenlijk al bij toegang tot persoonsgegevens.

De AVG somt op dat je verwerkt bij:

- verzamelen, vastleggen, ordenen,
- structureren, opslaan, bijwerken of wijzigen,
- opvragen, raadplegen, gebruiken,
- verstrekken dmv doorzending,
- verspreiden of anders ter beschikking stellen,
- aligneren of combineren, afschermen,
- wissen of vernietigen van gegevens

VERWERKEN

Wanneer mag je verwerken?

Verwerking van persoonsgegevens is alleen toegestaan als daar een grondslag voor bestaat. Dat mag alleen als het noodzakelijkis:

- Voor de uitvoering van een overeenkomst;
- Voor de uitvoering vam een wettelijke plicht;
- Voor een vitaal belang van de betrokkene;
- Voor de goede vervulling publiekrechtelijke taak;
- Voor een gerechtvaardigd belang (als dat niet ism grondrechten/fundamentele vrijheden van de betrokkene).
- Of met ondubbelzinnige toestemming van betrokkene. Als de betrokkene goed is geïnformeerd en voorafgaand aan de verwerking.

LET OP! toestemming is geen geldige grondslag in de arbeidsrelatie en kan worden ingetrokken.

HOOFDROLSPELERS

Met wie krijg je te maken?

Verwerkingsverantwoordelijke:

Degene die doel en middelen van de verwerking vaststelt en voor zichzelf persoonsgegevens verwerkt. Bijv.: de werkgever die gegevens van werknemers vastlegt voor loonbetaling.

Betrokkene:

De natuurlijk persoon over wie persoonsgegevens worden verzameld. Bijv.: de werknemer of de klant.

Verwerker:

Degene die voor een ander verwerkt. Bijv.: loonburo

LET OP! Met de verwerker moet je een verwerkersovereenkomst sluiten die aan de eisen voldoet.

RECHT VAN BETROKKENEN

Betrokkenen hebben meer rechten

Door de AVG krijgen betrokkenen meer rechten als hun persoonsgegevens verwerkt worden. Zij hebben het:

- Recht om geïnformeerd te worden;
- Recht van inzage;
- Recht op rectificatie
- Recht op vergetelheid (‘to be forgotten’);
- Recht op beperking van de verwerking;
- Recht op dataportabiliteit;
- Recht van bezwaar;
- Recht om toestemming in te trekken.

STAPPENPLAN

En nu concreet

Je realiseert je nu waarschijnlijk dat binnen jouw onderneming meer persoonsgegevens worden verwerkt, dan je dacht.

De personeelsdossiers van werknemers staan vol met persoonsgegevens, binnen en buiten hangen camera's in verband met veiligheid en fraude, werknemers houden hun uren bij, er is een volgsysteem voor de bedrijfsauto's, laat staan alle (bijzondere) persoonsgegevens die verzameld worden m.b.t. zieke werknemers.

TIP: wijs één werknemer aan die verantwoordelijk is voor privacy binnen het bedrijf. Die kan voorbereidingen treffen en is tegelijkertijd aanspreekpunt bij vragen.

Leg alle stappen vast, zodat u bij controle kunt laten zien dat u aan de AVG voldoet.

STAP 1

Welke persoonsgegevens worden verwerkt?

Nu je weet wat persoonsgegevens zijn en wanneer sprake is van verwerking, breng in kaart waar en welke persoonsgegevens worden verwerkt binnen het bedrijf. Met welk doel worden die gegevens verzameld of bewaard?

Is er wel een goed grondslag voor verwerking en worden gegevens niet onnodig of te lang bewaard?

Doelbinding

De AVG kent het begrip ‘doelbinding’. Dat betekent dat persoonsgegevens niet met een ander dan het oorspronkelijke doel mogen worden verwerkt.

LET OP!

Toestemming voor verwerking moet altijd expliciet en goed geïnformeerd zijn gegeven.

STAP 2

Leg alle verwerkingen vast in een verwerkingsregister.

Volgens de Autoriteit Persoonsgegevens is elk bedrijf/werkgever verplicht om een verwerkingsregister bij te houden. Daar moet het volgende instaan:

- Contactgegevensbedrijf en evt. Functionaris;
- Doelen verwerkingen;
- Categorieën personen (bijv. werknemers);
- Categorieën persoonsgegevens (bijv. NAW, BSN, videobeelden);
- Bewaartermijnen (bijv. 2 jaar mbt personeelsdossier na ontslag);
- Categorieën ontvangers van persoonsgegevens;
- Algemene beschrijving technische en organisatorische beveiligingsmaatregelen.

Spreadsheets zoals Excel zijn praktisch om als register te gebruiken.

STAP 3

Privacybeleid

Het opstellen van een privacybeleid is niet altijd verplicht, maar helpt bij een goede voorbereiding op de komst van de AVG. Bij het opstellen daarvan kan weer eens kritisch worden gekeken naar alle verwerkingen, grondslagen en de manier van werken met persoonsgegevens binnen het bedrijf.

Naast de informatie die ook in het verwerkingsregister staat, bevat het beleid uitleg hoe aan de beginselen van de AVG wordt voldaan, of er wel of niet een functionaris is, hoe wordt gezorgd dat rechten van betrokkenen uitgeoefend kunnen worden en uitleg tav beveiliging.

Bijv.; inzage in het personeelsdossier en het correctierecht bij feitelijke onjuistheden.

LET OP!
Is er een OR, dan moet toestemming worden gevraagd mbt het privacybeleid

STAP 4

Protocol datalekken

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen vaan persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie.

Het is verstandig om een datalek protocol te maken. Daarin staat vermeld hoe te handelen als een datalek wordt geconstateerd.

Datalekken moeten alleen gemeld worden bij ernstige nadelige gevolgen of een risico daarop.

Er moet wel een datalekregister komen met:

- Feiten en gegevens over de aard van het datalek
- Categoerieën van de getroffen betrokkenen
- Gevolgen en maatregelen van het datalek
- Of datalek is gemeld bij AP/betrokkenen

STAP 5

Beveiliging

Persoonsgegevens mogen niet zomaar op straat komen te liggen. Je moet passende technologische en organisatorische maatregelen nemen om de persoonsgegevens te beveiligen. Dus moderne technieken gebruiken en de organisatie er bewust van maken van mogelijke datalekken en privacyrisico's.

Bewustwording

Organiseer bijv. een bijeenkomst waarin de werknemers worden geïnformeerd over wat privacy inhoudt en wat de AVG inhoudt.

STAP 6

Informeer de werknemers

Nu alle verwerkingen van persoonsgegevens in kaart zijn gebracht, en niet meer teveel of te lang wordt verwerkt, is het zaak de werknemers te informeren.

Laat de werknemers weten:

- Welke gegevens van ze worden verwerkt. Denk aan gegevens in het dossier, bij ziekte, videobeelden, track and trace, etc.;
- Met welk doel en grondslag wordt verwerkt;
- Hoe lang de gegevens bewaard worden;
- Aan wie worden die gegevens verstrekt. Denk aan de arbodienst, loonburo of klanten;
- Welke rechten hebben ze.

Laat expliciet tekenen voor verwerkingen waar toestemming onvermijdelijk voor nodig is.

De eenmalige informatie kan nu per brief worden gegeven en daarna verwerkt in een reglement of handboek.

STAP 7

Functionaris gegevensbescherming (FG)

Het is verplicht als je:

- Een overheidsinstantie bent of een publieke taak hebt;
- Als kerntaak op grote schaal personen regelmatig en stelselmatig observeert of;
- Op grote schaal bijzondere persoonsgegevens verwerkt.

- Een FG moet worden aangemeld bij de AP en opgenomen in het register, ook bij vrijwillige aanstelling.
- Gebruik daarom een andere titel voor de interne verantwoordelijke voor privacy.

STAP 8

Gegevensbeschermingseffectbeoordeling (DPIA)

Een gegevensbeschermingseffectbeoordeling of Data Protection Impact Assessment (DPIA) is een toets voor risico's bij verwerking.

Het is altijd verplicht als je:

- Systematisch en uitgebreid persoonlijke aspecten van personen beoordeelt, op grond waarvan besluiten worden genomen en waaraan voor de persoon rechtsgevolgen zijn verbonden. Bijv. Profilering, een bedrijf dat bezoekers opzijn website volgt en op basis daarvan profielen van deze mensen opstelt, een bedrijf dat DNA testen aan consumenten levert om gezondheidsrisico's te testen;
- Op grote schaal bijzondere persoonsgegevens verwerkt;
- Op grote schaal en stelselmatig mensen volgt in openbare ruimte (bijv aan de hand van cameratoezicht).

STAP 9

Verwerkersovereenkomsten aanpassen

Als je persoonsgegevens door anderen laat verwerken, dan moet je met die verwerkers een verwerkersovereenkomst sluiten.

Door die overeenkomst moet nakoming van de AVG gegarandeerd worden.

Wat staat erin?

- Algemene beschrijving verwerkingen;
- Verwerking uitsluitend obv schriftelijke instructies;
- Geheimhoudingsplicht;
- Beveiliging;
- Alleen subverwerking met toestemming
- Bijstand bij vervullen rechten van betrokkenen;
- Bijstand bij vervullen plichten ogv AVG;
- Gegevens verwijderen na einde overeenkomst;
- Audits.

CONTROLE EN BOETES

Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens controleert in Nederland of de AVG niet wordt overschreven. De AP kan maximale boetes opleggen van EUR 20 miljoen of 4% van de omzet.

Recent is door de Tweede Kamer de Nederlandse Uitvoeringswet aangenomen. Specifieke regels voor het arbeidsrecht zijn niet afgesproken.

Wel dat de AP het eerste jaar vooral praktische informatie verschaft over de AVG aan het MKB.

COOKIES

OP HET PLAATSEN VAN COOKIES IS OOK VANAF 25 MEI 2018 DE AVG VAN TOEPASSING.

Cookie-popups en cookie wall zijn in ieder geval niet meer toegestaan.

Soorten cookies:

- Functionele cookies. Dit zijn cookies die nodig zijn voor het functioneren van je website. Deze kunnen zonder toestemming van de bezoeker geplaatst worden.

- Analytics cookies. Worden gebruikt om statistieken over je website te verzamelen. Kan zonder toestemming, tenzij de gebruikersgegevens verzameld worden en de informatie geheim blijft.

- Marketing cookies. Worden geplaatst om bezoekers te volgen en info over een websitegedrag te verzamelen. Dit kan zonder expliciete toestemming niet meer. Indien je deze cookies wel wenst te gebruiken is het verstandig een cookiebeleid en verklaring op te stellen. Het best is om gespecialiseerde partijen zoals Cookieinfo.net te benaderen om AVG bestendig cookies te kunnen gebruiken.

WELKE VERANDERINGEN KOMEN ERAAN

DE BELANGRIJKSTE VERANDERINGEN IN HET GEBRUIK VAN COOKIES ZIJN:

- Het verkrijgen van toestemming (consent) voordat de cookies geplaatst worden;
- De ‘keuzevakjes’ voor soorten cookies mogen niet vooraf zijn aangevinkt;
- De website moet toegankelijk zijn gedurende de toestemming keuze;
- Dat de toestemming net zo makkelijk aangepast of verwijderd kan worden als dat deze gemaakt is;
- Het registreren van de gemaakte toestemming in een log.

IN EEN NOTENDOP