De Nieuwe Wet Privacy

AVG

- Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing
- Geldt voor de hele EU
- Wet bescherming persoonsgegevens geldt dan niet meer

AVG

- De AVG versterkt de positie van de mensen van wie gegevens worden verwerkt. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De organisaties moeten kunnen aantonen dat zij zich aan de wet houden

Basisprincipe

- Noodzakelijk
- Doel kan niet worden bereikt op manier die minder inbreuk maakt op privacy
- Verwerking is proportioneel

Persoonsgegevens

Voorbeelden

- Naam
- Adres
- Woonplaats
- Telefoonnummer
- Postcode
- Huisnummers

Wat is verwerking van persoonsgegevens?

al dan niet uitgevoerd via geautomatiseerde procedés

verzamelen / vastleggen / ordenen / structureren / opslaan / bijwerken of wijzigen / opvragen / raadplegen / gebruiken / verstrekken door middel van doorzending / verspreiden of op andere wijze ter beschikking stellen / aligneren of combineren / afschermen / wissen of vernietigen van gegevens

Verwerkingsverantwoordelijke – Verwerker

Verwerkingsverantwoordelijke:

- verwerkt gegevens voor eigen doeleinden
- heeft eigen klantrelatie met betrokkene

Verwerker:

- gegevens mogen alleen in opdracht van verwerkingsverantwoordelijke worden verwerkt (niet voor eigen doeleinden)
- uitbestede / gedelegeerde verwerkingsactiviteiten

Beginselen verwerking persoonsgegevens (art. 5 AVG)

- Rechtmatig / behoorlijk / transparant
- Voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld
- Minimale gegevensverwerking

Rechtmatigheid van de verwerking

Aan ten minste één voorwaarde is voldaan – art 6 AVG

- Noodzakelijk voor uitvoering van de overeenkomst waarbij betrokkene partij is
- Noodzakelijk om te voldoen aan wettelijke verplichting
- Betrokkene heeft toestemming gegeven voor verwerking van persoonsgegevens voor één of meer specifieke doeleinden

Toestemming

in arbeidsverhouding, waarin werknemer financieel afhankelijk is van werkgever:

over algemeen geen sprake van ‘vrije’ toestemming

Mag werkgever foto's van werknemers op internet publiceren? Ja,

- van iedere werknemer van wie foto wordt gepubliceerd toestemming nodig; werknemers jonger dan 16 jaar toestemming ouders / voogd / wettelijk vertegenwoordiger
- specifiek doel; mag foto's niet voor ander doel gebruiken zonder daar apart toestemming voor te vragen

Verwerking van bijzondere categorieën van persoonsgegevens – artikel 9 AVG

- Verwerking van persoonsgegevens waaruit ras of etnische afkomst / politieke opvattingen / religieuze of levensbeschouwelijke overtuigingen
- Gegevens over gezondheid / gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid is verboden

Verwerking van bijzondere categorieën van persoonsgegevens – uitzonderingen (artikel 9, lid 2):

- verwerking is noodzakelijk met oog op uitvoering van verplichtingen en uitoefening op gebied van arbeidsrecht en sociale zekerheidsrecht
- betrokkene heeft uitdrukkelijke toestemming gegeven voor verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden

Hoe bereid je je voor op de AVG?

AVG stap 1

Bewustwording

- Relevante mensen in de organisatie moeten op de hoogte zijn van de nieuwe privacy regels. Zij moeten inschatten wat de impact is van de AVG op de huidige processen, diensten en goederen en welke aanpassingen nodig zijn.
- AP heeft guidlines opgesteld.

AVG stap 1

Boete

Komt verantwoordelijke (één van de) verplichtingen niet na:

- kan AP boete opleggen van maximaal € 10 miljoen
- of boete van 2% van wereldwijde jaaromzet (mocht dat bedrag hoger uitkomen)

Overtreedt verantwoordelijke beginselen of grondslagen van AVG / privacyrechten van betrokkenen:

- kan AP boete opleggen van maximaal € 20 miljoen
- of boete van 4% van wereldwijde jaaromzet (mocht dat bedrag hoger uitkomen)

AVG stap 2

Rechten van betrokkenen

Betrokkenen krijgen meer en verbeterde privacyrechten, zoals:

Het recht op inzage

Zij mogen vragen of eigen persoonsgegevens zijn vastgelegd en zo ja, welke. Zij hoeven geen reden op te geven. Vraagt iemand om inzage, dan moet de organisatie diegene op een duidelijke en begrijpelijke manier laten weten:

- of de organisatie zijn persoonsgegevens gebruikt, en zo ja:
  - om welke gegevens het gaat;
  - wat het doel is van het gebruik;
  - aan wie de organisatie de gegevens eventueel heeft verstrekt;
  - wat de herkomst is van de gegevens, als deze bekend is.

AVG Stap 2

Elektronische opgave loonbedrag 7:626 BW (loonstrook).

Voor verstrekken van elektronische opgave is uitdrukkelijke instemming van werknemer vereist.

Tip: neem dit op in de arbeidsovereenkomst

AVG stap 2

<u>Het recht op correctie en verwijdering</u>

Iemand kan om correctie vragen als zijn persoonsgegevens:

- feitelijk onjuist zijn;
- onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld;
- op een andere manier in strijd met een wet worden gebruikt.

Eisen dat organisatie correctie / verwijdering doorgeeft aan alle andere organisaties die deze gegevens hebben gekregen.

AVG Stap 2

Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zo ver deze ter zake doen.

Wel mag diegene van de organisatie verwachten dat deze in ieder geval zijn schriftelijke mening toevoegt aan het dossier. Dat kan vooral een oplossing bieden bij situaties waarbij het om niet objectief vast te stellen feiten gaat.

AVG stap 2

Recht op dataportabiliteit (nieuw)

Oftewel overdraagbaarheid van persoonsgegevens. Het houdt in dat betrokkenen het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft.

- Vervolgens kunnen betrokkenen deze gegevens zelf opslaan voor persoonlijk (her)gebruik. Ook kunnen ze de gegevens doorgeven aan een andere organisatie. Bijvoorbeeld als ze willen overstappen naar een andere telecomprovider of als ze een dienst van een andere organisatie willen gebruiken, zoals een online huishoudboekje.
- De organisatie die de gegevens verstrekt, mag betrokkenen hierin niet tegenwerken. En moet ervoor zorgen dat de betrokkenen hun gegevens makkelijk kunnen krijgen en doorgeven.

AVG stap 3

Documentatieplicht (art 30 AVG)

- Breng de gegevensverwerkingen in kaart
- Documenteer welke persoonsgegevens u verwerkt en met wel doel, waar de gegevens vandaag komen en met wie u ze deelt
- Er geldt een verantwoordingsplicht (u moet aantonen dat uw organisatie conform AVG handelt).
- Vermeld in het overzicht ook per categorie de wettelijke grondslag (beroept u zich bijvoorbeeld op een gerechtvaardigd belang of vraagt u toestemming aan de betrokkenen?)

AVG stap 3

<u>Documentatieplicht niet van toepassing</u>

- Niet van toepassing op ondernemingen of organisaties die minder dan 250 personen in dienst hebben
- Tenzij waarschijnlijk is dat:
  - verwerking risico inhoudt voor rechten en vrijheden van betrokkenen *of*
  - verwerking niet incidenteel is *of*
  - verwerking bijzondere persoonsgegevens.

AVG stap 4

Data protection impact assessment

- U kunt verplicht zijn een data protection impact assessment (DPIA) uit te voeren
- Het is een instrument om vooraf de privacyrisico's van gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.
- Een DPIA is alleen 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).

AVG stap 4

Wat is op “grote schaal”?

Kijk dan naar deze criteria:

- het aantal betrokkenen (de mensen van wie u gegevens verwerkt);
- de hoeveelheid gegevens die u verwerkt;
- de duur van de gegevensverwerking;
- de geografische reikwijdte van de verwerking.

AVG Stap 4

Grootschalig is:

- Een ziekenhuis dat patiëntgegevens verwerkt als onderdeel van de gebruikelijke werkzaamheden.
- Een vervoersmaatschappij die reisinformatie verwerkt van mensen die met het openbaar vervoer in een bepaalde stad reizen. Bijvoorbeeld door hen te volgen via reiskaarten.
- Een verwerker die gespecialiseerd is in marktonderzoek en die in opdracht van een internationale fastfoodketen de actuele locatiegegevens van klanten verwerkt voor statistische doeleinden.
- Een verzekeringsmaatschappij of bank die klantgegevens verwerkt als onderdeel van de gebruikelijke werkzaamheden.
- Een zoekmachine die persoonsgegevens verwerkt om advertenties te kunnen tonen op basis van internetgedrag.

Grootschalig is NIET: verwerking persoonsgegeven door individuele artsen of advocaten (‘eenpitters’).

AVG stap 5

Privacy by design & privacy by default

Dit zijn verplichten uitgangspunten onder AGV die u moet invoeren.

Privacy by design houdt in dat u al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Ten tweede houdt u rekening met dataminimalisatie: u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Op deze manier kunt u een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen.

AVG stap 5

Bij ontwerpen van producten en diensten zorgen dat persoonsgegevens goed worden beschermd.

- Afvragen of het écht nodig is om persoonsgegevens te verwerken
- Kan bijvoorbeeld ook gewerkt worden met geanonimiseerde gegevens
- Toch persoonsgegevens verwerken; nadenken over beveiliging van deze gegevens, bijvoorbeeld door pseudonimiseren

AVG Stap 5

Voorbeeld:

online-bestelproces

- vragen naar adres zal mogelijk noodzakelijk zijn om product te kunnen afleveren; niet noodzakelijk bij e-tickets voor concert / voorstelling
- geboortedatum is hoogstwaarschijnlijk niet noodzakelijk, tenzij bierpakket wordt besteld

Privacy by default

Houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje ‘Ja, ik wil aanbiedingen ontvangen’ niet vooraf aan te vinken;
- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

AVG stap 6

Functionaris voor de gegevensbescherming

Organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen.

Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. Op grond van artikel 37 van de AVG is een FG in drie situaties verplicht:

1. Overheden en publieke organisaties
2. Bij organisaties die vanuit hun kernactiviteit op grote schaal individuen volgen (profilering van mensen, cameratoezicht, monitoring van iemands gezondheid via wearables)
3. Bij organisaties die op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is (gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijk verleden)

AVG stap 7

Meldplicht datalekken

De meldplicht datalekken blijft onder AVG nagenoeg hetzelfde. Deze meldplicht houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben (bijvoorbeeld kwijtraken usb-stick, diefstal laptop, inbraak hacker). Alleen melden als er ook persoonsgegevens verloren zijn gegaan.

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens.

Wel strengere eisen aan de eigen registratie van de datalekken. U moet alle datalekken documenteren. AP moet kunnen controleren of u aan de meldplicht heeft voldaan.

AVG Stap 7

Persoonsgegevens van gevoelige aard meldplicht datalekken

- Gegevens over financiële of economische situatie van betrokkene
- (Problematische) schulden / salaris / …
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude
- Kopieën van identiteitsbewijzen / Burgerservicenummer / …
- Bijzondere persoonsgegevens: godsdienst / levensovertuiging / ras / gezondheid / …

AVG Stap 7

Inbreuken documenteren artikel 33 lid 5 AVG

- Verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens
- Dus ook niet-meldingsplichtige datalekken
- Feiten omtrent inbreuk in verband met persoonsgegevens / gevolgen daarvan / genomen corrigerende maatregelen

AVG Stap 7

Inbreuken melden - verwerker artikel 33 lid 2 AVG

Verwerker informeert verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van inbreuk in verband met persoonsgegevens

AVG stap 8

Bewerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een bewerker? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Een bewerker is een persoon of organisatie aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed. Bijvoorbeeld een administratiekantoor.

Een bewerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens. Maar de bewerker heeft wel een aantal afgeleide verplichtingen, voor onder meer beveiliging en geheimhouding van de gegevens.

AVG Stap 8

Verwerkersovereenkomst (data processing agreement) – artikel 28 lid 3 AVG

Verwerkingsverantwoordelijke en verwerker verplicht om aantal onderwerpen vast te leggen in schriftelijke overeenkomst:

- Algemene beschrijving
- Onderwerp / duur / aard en doel van verwerking / soort persoonsgegevens / categorieën van betrokkenen / …
- Geheimhoudingsplicht / beveiliging / …

Inzien van gegevens door externe helpdesk is verwerking.

AVG stap 9

Leidende toezichthouder

Heeft u vestigingen in meerdere EU-lidstaten? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

De hoofdregel is dat de toezichthouder van de EU-lidstaat waar de hoofdvestiging van een organisatie is gevestigd, de leidende toezichthouder is.

AVG stap 10

Toestemming

Uw gegevensverwerking kan gebaseerd zijn op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

Bewaren van persoonsgegevens

Geen concrete bewaartermijn in AVG

- Organisaties bepalen zelf hoe lang zij persoonsgegevens bewaren
- AVG: niet langer bewaren dan noodzakelijk is voor doel
- Psychologische test / loonbeslag / …
- Wel concrete bewaartermijnen in andere wetten
- Belastingwetgeving / verzuim
- Richtlijn: bewaartermijn van (maximaal) 2 jaar nadat werknemer uit dienst is

Checklist

- Zorg dat u weet welke regels gelden voor type (bijzondere) gegevens dat u verwerkt en probeer gebruik ervan zoveel mogelijk te beperken
- Stel overzicht verwerken persoonsgegevens op (artikel 13 + 14 AVG)
- Begin op tijd met in kaart brengen van alle verwerkingsactiviteiten, zodat alle informatie op tijd in register is opgenomen (artikel 30 AVG)
- Ook verstandig indien niet verplicht

Checklist

- Stel privacybeleid op en zorg dat werknemers op de hoogte zijn van / handelen naar inhoud
- Stel privacystatement op
- Loop alle bestaande verwerkersovereenkomsten na en kijk of deze (nog) voldoen aan alle eisen
- Denk tijdens ontwerp- en ontwikkelingsproces van systemen en processen al na over privacy
- Meldplicht datalekken; neem kennis van procedure (draaiboek) / stel procedure op

Checklist

- Ga na of er binnen organisatie verwerkingen plaatsvinden met hoog risico en bepaal of DPIA op zijn plaats is (ook verstandig indien niet verplicht)
- Ga na of uw bedrijf functionaris voor de gegevensbescherming (FG) nodig heeft (artikel 37 AVG)
- Bereid u voor op
  - recht beperking van de verwerking (artikel 18 AVG)
  - recht op dataportabiliteit (artikel 20 AVG)

begin op tijd!