Algemene verordening gegevensbescherming (AVG)

Dit betekent het voor u als ondernemer

Interpolis. Glashelder

1

Dezelfde privacywetgeving voor alle lidstaten van de EU

Op 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van kracht gegaan. Sinds die datum geldt voor alle landen van de Europese Unie dezelfde privacywetgeving. De AVG geeft natuurlijke personen meer rechten. En legt bij organisaties meer verantwoordelijkheden neer rondom het verzamelen en bewerken van persoonsgegevens.

Persoonsgegevens moeten optimaal worden beveiligd
De AVG verwacht van organisaties die persoonsgegevens verwerken dat ze deze goed beschermen. Zodat ze niet in verkeerde handen terecht komen of verloren raken. Wist u dat 1 op de 5 mkb'ers al slachtoffer was van cyberproblemen? Veel ondernemers staan niet stil bij de gevolgen van cybercalamiteiten. Deze kunnen desastreus zijn en gaan veel verder dan alleen de financiële schade. Denk bijvoorbeeld aan de negatieve media-aandacht en de gevolgen voor uw klanten! Kortom, het is noodzakelijk om de digitale veiligheid van uw bedrijf goed op orde te hebben. Niet alleen om te voldoen aan uw plichten rondom de AVG, maar ook om uw bedrijfscontinuïteit te waarborgen.

E-book met kort en bondige informatie over de AVG
De privacywet is uitgebreid en niet in een klein boekje samen te vatten. In dit e-book leest u dan ook de belangrijkste punten. Kijk voor uitgebreide informatie over de AVG op de website van de Autoriteit Persoonsgegevens. Daar vindt u ook een overzicht van veelgestelde vragen.

PS: In dit e-book namen we ook de handige beslisboom uit de handleiding van het Ministerie van Justitie en Veiligheid en een link naar de praktische AVG-regelhulp van de Autoriteit Persoonsgegevens op. Deze tools geven u snel inzicht in de stappen die u moet nemen om uw bedrijf AVG-proof te maken.

2 Dezelfde privacywet voor de hele Europese Unie

Dankzij de AVG is de bescherming van persoonsgegevens in alle lidstaten van de EU op dezelfde manier geregeld en gelden in elke lidstaat grotendeels dezelfde afspraken en regels. De AVG regelt voor een groot deel wat al eerder gold onder de Wet bescherming persoonsgegevens (Wbp).

De AVG zorgt onder meer voor:

- versterking en uitbreiding van privacyrechten van natuurlijke personen
- meer verantwoordelijkheden voor organisaties
- dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals bijvoorbeeld de bevoegdheid om boetes tot 20 miljoen euro of 4% van de wereldwijde omzet op te leggen

Door de AVG hebben organisaties die persoonsgegevens verwerken meer verplichtingen
Van u, als verantwoordelijke, wordt verwacht dat u het voor iedereen duidelijk en inzichtelijk maakt waarom uw bedrijf persoonsgegevens verzamelt, waarvoor uw bedrijf ze gebruikt en hoelang uw bedrijf deze data bewaart. En u moet aan de Autoriteit Persoonsgegevens, de toezichthouder op deze wet in Nederland, kunnen aantonen dat uw bedrijf zich aan de AVG houdt.

De AVG versterkt de positie van natuurlijke personen van wie gegevens worden verwerkt
De AVG zorgt ervoor dat natuurlijke personen meer zeggenschap krijgen over de persoonlijke data die een bedrijf opslaat. Zo mogen mensen hun toestemming om gegevens te verwerken niet alleen intrekken, maar mag men onder bepaalde voorwaarden ook gebruikmaken van het recht om vergeten te worden. Niet alleen door het bedrijf dat de gegevens heeft verzameld, maar bij álle organisaties die hun gegevens hebben ontvangen via dat bedrijf.

U hebt meer verplichtingen bij de verwerking van persoonsgegevens
De AVG legt de nadruk op uw verantwoordelijkheid om aan te tonen dat u zich aan de wet houdt. Dit heet de verantwoordingsplicht. De verantwoordingsplicht houdt in dat u met documenten moeten kunnen aantonen dat u de juiste organisatorische en technische maatregelen hebt genomen om aan de AVG te voldoen:

- **Soms moet u een gegevensbeschermingsbeleid hebben**
  U bent alleen verplicht om een gegevensbeschermingsbeleid op te stellen als dat in verhouding staat tot uw verwerkingsactiviteiten. Een gegevensbeschermingsbeleid wordt ook wel privacybeleid genoemd. Of u verplicht bent om zo'n privacybeleid op te stellen, hangt af van de concrete omstandigheden. Zoals de aard, de omvang, de context en het doel van de gegevensverwerking. In de AVG staat niet precies omschreven welke gegevens u in uw privacybeleid moet opnemen. Uit het beleid moet in ieder geval wel blijken hóe u voldoet aan de AVG.

2

- **Uw (digitale) beveiliging moet op orde zijn**
  Uw beveiligingsniveau moet zijn afgestemd op de risico's die de gegevensverwerking met zich meebrengt. Bijvoorbeeld risico's van vernietiging, verlies, wijziging of ongeoorloofde verwerking van persoonsgegevens. Het maakt daarbij niet uit of dat per ongeluk of doelbewust gebeurt.
- **Soms moet u een register aanleggen met alle verwerkingen**
  Dat betekent dat u moet documenteren welke persoonsgegevens u verwerkt, waarom u dat doet, hoe u aan deze gegevens komt en met wie u deze gegevens deelt.

Uw klanten hebben het recht op dataportabiliteit
Een deel van de rechten van uw klanten die in de AVG omschreven staan, gold ook al onder de Wbp (bijvoorbeeld recht op inzage en correctie). Onder de AVG is daar het recht op verwijderen van gegevens en het recht op dataportabiliteit bij gekomen. Dataportabiliteit betekent dat uw klant de persoonsgegevens mag opvragen die u van hem hebt gekregen. U moet deze gegevens aanleveren in een machinaal leesbaar formaat. Zo kan hij zijn gegevens eenvoudig doorgeven. Bijvoorbeeld aan een andere leverancier van eenzelfde soort dienst. Uw klant kan ook van u vragen om zijn gegevens rechtstreeks over te dragen aan een andere organisatie.

U mag persoonsgegevens alleen voor een uitdrukkelijk beschreven doel verwerken

Daarnaast hebt u een rechtmatige grondslag nodig om persoonsgegevens te verwerken. Dat betekent dat het doel van de verwerking op 1 van de 6 rechtsgrondslagen gebaseerd kan worden:

- Toestemming van de gebruiker
- Noodzakelijk voor de uitvoering of het aangaan van de overeenkomst met de betrokkene
- Noodzakelijk om te voldoen aan een Wettelijke verplichting die op u rust
- Noodzakelijk voor de vitale belangen van de betrokkene
- Noodzakelijk voor een taak van algemeen belang en uitoefening openbaar gezag
- Noodzakelijk voor een gerechtvaardigd belang. Dit betekent dat uw belang zwaarder weegt dan dat van de betrokkene. U moet uw belang wél communiceren

Kijk voor uitgebreide informatie over de AVG op de website van de Autoriteit Persoonsgegevens.

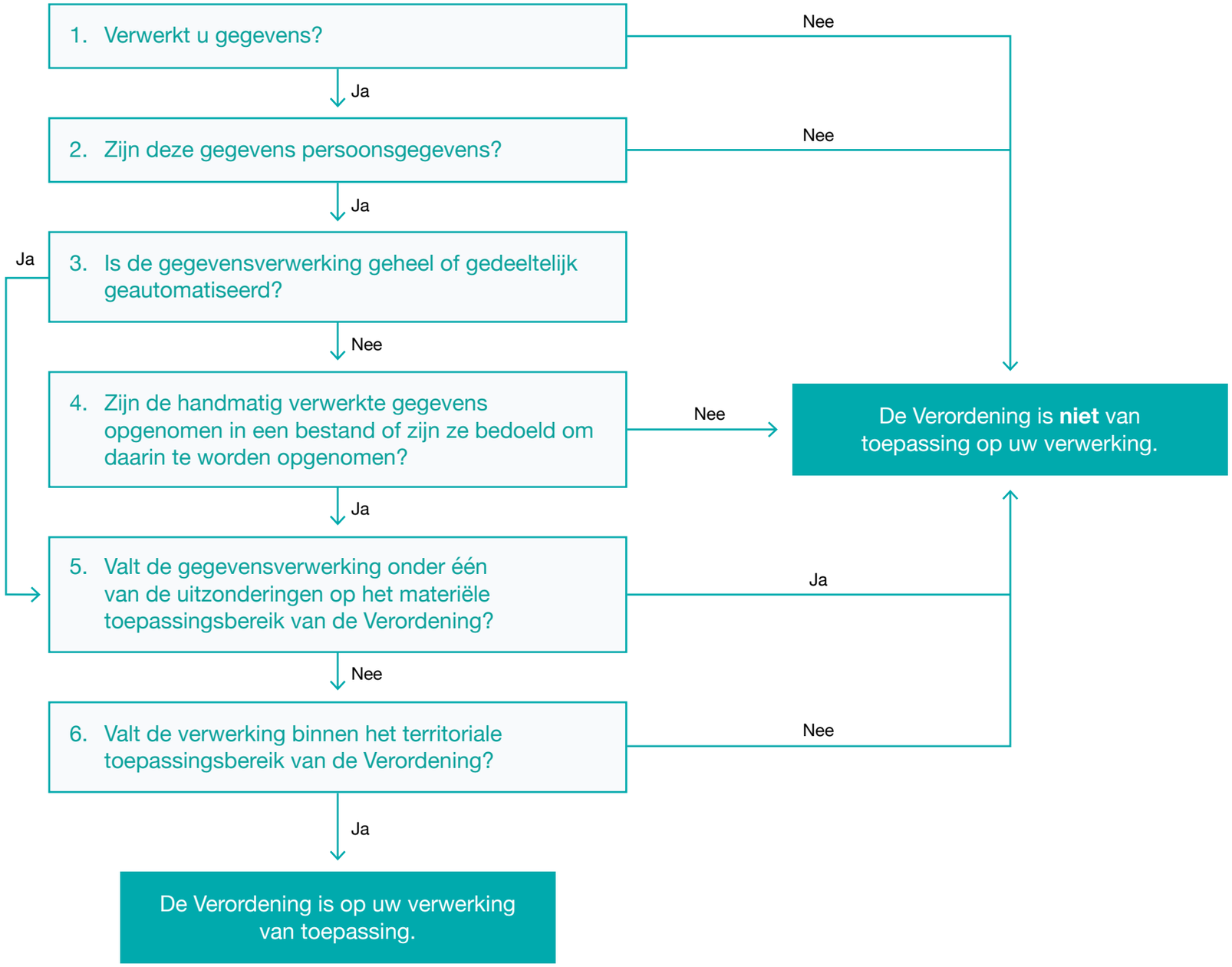
3 Geldt de AVG ook voor mijn bedrijf?

De AVG gaat over het verwerken van persoonsgegevens. En daar is al snel sprake van. Want onder verwerken valt niet alleen ‘opslaan’, maar ook gebruiken, analyseren, combineren of verwijderen. De wet geldt dus ook voor zzp’ers en kleine mkb’ers die gegevens van klanten opslaan. Zoals het bijhouden van afspraken met klanten, telefoonnummers van klanten of persoonlijke gegevens van uw medewerkers.

Persoonsgegevens gaan over een natuurlijke persoon
Een persoonsgegeven is alle informatie die direct over een natuurlijke persoon gaat of waarmee deze persoon te herleiden is. Zoals bijvoorbeeld iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Ook IP-adressen, e-mailadressen, kentekens en locatiegegevens kunnen bijvoorbeeld persoonsgegevens zijn, als deze te herleiden zijn naar een natuurlijk persoon.

Bijzondere persoonsgegevens mag u niet verwerken
Ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. De verwerking van bijzondere persoonsgegevens is verboden. Tenzij u zich kunt beroepen op een wettelijke uitzondering én op 1 van de grondslagen voor het verwerken van ‘gewone’ persoonsgegevens. In de AVG staan 10 uitzonderingen op het verbod om bijzondere persoonsgegevens te verwerken.

3 Is de AVG op uw bedrijf van toepassing?



Bron: Ministerie van Justitie en Veiligheid - Handleiding Algemene verordering gegevensbescherming 2018, schema 1, pagina 10.

4

Hoe zorg ik ervoor dat mijn bedrijf aan de privacyregels voldoet?

Vanaf 25 mei 2018 moet uw bedrijf voldoen aan de AVG. En dat moet u kunnen aantonen als de Autoriteit Persoonsgegevens dat van u vraagt. Maar wat moet u dan allemaal geregeld hebben om aan deze privacywet te voldoen?

De checklist hieronder geeft u een beeld van de globale vereisten uit de AVG.

Inventarisatie van privacyrisico's

Sommige bedrijven moeten in een verwerkingsregister vastleggen welke privacygevoelige gegevens worden verwerkt en waarom, wie toegang tot die gegevens heeft en hoelang deze gegevens worden bewaard. Soms wordt van u verwacht dat u een analyse uitvoert om uw privacyrisico's te inventariseren. Bijvoorbeeld als u met zeer vertrouwelijke gegevens werkt of als veel medewerkers eenvoudig toegang hebben tot deze gegevens. Of als er ernstige gevolgen zijn voor de betrokken personen als u de gegevens kwijtraakt. Aan de hand van de uitkomst van deze analyse neemt u passende technische én organisatorische maatregelen om deze risico's te beheersen.

Privacy by design

Privacy by design betekent dat u bij het (door)ontwikkelen van systemen waar persoonsgegevens in worden verwerkt, zoveel mogelijk de privacyregels toepast. U verwerkt de privacyregels dus direct in het systeem.
U kunt bijvoorbeeld in uw systemen de persoonsgegevens:

- **Pseudonimiseren**
  Persoonsgegevens zijn niet meer direct herleidbaar naar een persoon. Let op: de gegevens zijn nog wel indirect te herleiden, dus het blijven persoonsgegevens.
- **Minimaliseren**
  U verwerkt alleen de gegevens die strikt noodzakelijk zijn.

4

Privacy by default

Privacy by default betekent dat u technische en organisatorische maatregelen neemt om ervoor te zorgen dat uw bedrijf alleen die persoonsgegevens verzamelt die nodig zijn voor het specifieke doel dat u ermee hebt. Bijvoorbeeld:

- Door een app niet de locatie van een persoon te laten registreren als dat niet nodig is.
- Door op een website het vakje ‘ja, ik wil aanbiedingen ontvangen’, niet vooraf aan te vinken.
- Door aan een nieuwe abonnee op uw nieuwsbrief niet méér gegevens te vragen dan voor de verzending van de nieuwsbrief noodzakelijk.

Sommige bedrijven zijn verplicht om een functionaris gegevensbescherming aan te stellen

Overheden, publieke organisaties, maar ook bedrijven die als kernactiviteit op grote schaal personen volgen of op grote schaal bijzondere persoonsgegevens verwerken, zijn verplicht een functionaris gegevensbescherming (FG) aan te stellen. Dat is een interne toezichthouder die alles rondom de verwerking van persoonsgegevens bewaakt en erop toeziet dat de AVG wordt nageleefd.

U hebt een meldplicht bij datalekken

Als persoonsgegevens die u bewaart in handen van derden komen door verlies of bijvoorbeeld een hack, bent u verplicht dit binnen 72 uur te melden bij de Autoriteit Persoonsgegevens. Dat is niet nieuw, deze meldplicht stond ook in de oude Wet Bescherming Persoonsgegevens. Echter, er wordt nu van u verwacht dat u eigen datalekken registreert en documenteert. Zo kan de autoriteit op ieder gewenst moment controleren of u aan uw meldplicht hebt voldaan.

Sluit verwerkersovereenkomsten af met andere partijen die namens u uw persoonsgegevens verwerken

Onder de Wbp had u al dezelfde verplichting: volgens de AVG moet u deze overeenkomst uitbreiden. U legt nu bijvoorbeeld vast hoelang de gegevens worden bewaard en wie verantwoordelijk is voor de beveiliging ervan bij een eventueel datalek. Houd bij het maken van de afspraken goed voor ogen dat de verwerker de data daadwerkelijk beschermt zoals u het in uw privacyreglement hebt beloofd aan uw klanten!

Sluit u contracten af met een ander bedrijf die onder de AVG ‘zelfstandig verantwoordelijke’ is in plaats van verwerker? Dan is zo’n verwerkersovereenkomst niet nodig. Ga dus goed na of er werkelijk sprake is van een verwerkersrelatie.

4

De AVG wil dat u helder bent over wat u met persoonsgegevens doet

De meest praktische manier om dat te communiceren is in een privacyverklaring. Stel deze op in begrijpelijke taal, zodat het voor iedereen snel en eenvoudig duidelijk is wat u met de gegevens doet en waarom.

Creëer privacy-bewustzijn bij uw medewerkers

Bekijk wie er binnen uw bedrijf met de wet te maken heeft en zorg ervoor dat deze medewerkers goed op de hoogte zijn van de privacyregels.

Kijk voor uitgebreide informatie over de AVG op de website van de Autoriteit Persoonsgegevens.

5 Toezicht op de AVG

Vanaf mei 2018 gaat de Autoriteit Persoonsgegevens bedrijven die in Nederland gegevens verwerken op de vingers tikken als ze niet AVG-proof zijn. Dat blijft niet bij een waarschuwing. Als uw bedrijf niet voldoet aan de AVG kunt u een boete krijgen tot maximaal 4 procent van uw jaaromzet of maximaal 20 miljoen euro.

Iedere lidstaat heeft zijn eigen toezichthouder
Uw bedrijf valt onder het toezicht van de lidstaat van waaruit u uw gegevens verwerkt. Hoewel het toezicht door de instelling van de AVG in principe voor alle EU-landen op dezelfde manier wordt uitgevoerd, is oplettendheid toch geboden. Iedere lidstaat mag een eigen nadere invulling op specifieke onderdelen van de AVG maken. Deze nadere invulling wordt geregeld aan de hand van AVG-uitvoeringswetten die per lidstaat kunnen verschillen. De overheid van het land van waaruit u werkt, kan u hierover meer informatie geven.

De AVG-regelhulp
De Autoriteit Persoonsgegevens ontwikkelde de interactieve tool ‘de AVG-regelhulp’. Als u de vragen uit de regelhulp beantwoordt, krijgt u een praktisch advies op maat over wat u moet regelen om aan de AVG te voldoen. De AVG-regelhulp is ontwikkeld in samenwerking met de Rijksdienst voor Ondernemend Nederland (RVO).

Kijk voor uitgebreide informatie over de AVG op de website van de Autoriteit Persoonsgegevens.

6 De AVG raakt iedereen!

Na het lezen van dit e-book weet u dat de AVG vrijwel ieder bedrijf, groot én klein, raakt. En dat u, als u optimaal wilt voldoen aan de AVG-wetgeving, moet kijken naar de juridische aspecten en de ICT- en organisatiegerelateerde procedures binnen uw bedrijf. En dat het daarnaast belangrijk is dat uw medewerkers goed zijn geïnformeerd over alle regels die gelden.

Doe er uw voordeel mee!
De AVG brengt veel duidelijkheid voor uw klanten. Maar ook voor uw bedrijf brengt deze privacywet voordelen met zich mee. Een helder privacy beleid maakt bijvoorbeeld dat het vertrouwen van uw klanten in uw bedrijf toeneemt. En door beter na te denken over de beveiliging van persoonsgegevens wordt de kans op een datalek kleiner en beperkt u uw cyberrisico.

Meer informatie
Zoals we aan het begin al schreven, is de AVG te complex om samen te vatten in een e-book. Kijk daarom voor uitgebreide informatie op de website van de Autoriteit Persoonsgegevens of download de handleiding die het Ministerie van Justitie en Veiligheid samenstelde.

En komt u tot de conclusie dat uw bedrijfsvoering te ingewikkeld is om de regels van de AVG zelf toe te passen? Schroom dan niet om een professionele privacy-expert met u mee te laten kijken. Bijvoorbeeld een jurist of advocaat die gespecialiseerd is in privacy.