RendementOnline

Voldoe aan de privacyregels van de AVG in 9 stappen

Dit schrijft de Algemene verordening gegevensbescherming allemaal voor

CHECKLIST
Publicatiedatum:
28 september 2023

De strenge privacyregels van de Algemene verordening gegevensbescherming (AVG) hebben betrekking op alle gevallen waarbij persoonsgegevens worden opgeslagen en verwerkt. Inmiddels mag van ondernemingen wel verwacht worden dat de AVG geïmplementeerd is in de operationele processen. Toch blijken er nog steeds onduidelijkheden te zijn, en is een onbedoelde overtreding van de AVG snel begaan.
Deze toolbox bevat de belangrijkste tools en uitleg om te zorgen dat uw onderneming echt wel voldoet aan de AVG Ook de rol van de OR komt aan bod..

Deze toolbox bestaat uit de volgende stappen:

Dit u moet doen voor de Algemene verordening gegevensbescherming

De in 2018 ingevoerde Algemene verordening gegevensbescherming (AVG) heeft een flink aantal verplichtingen voor de bescherming van persoonsgegevens met zich meegebracht. U moet onder meer rekening houden met een goede beveiliging van persoonsgegevens, met een juiste verwerking van gegevens van werknemers en leveranciers door externe partijen, en u moet dit voor elk nieuw initiatief binnen uw onderneming opnieuw beoordelen.
Onderstaande stappen geven voor de voornaamste aspecten van de AVG essentiële informatie en direct toepasbare tools. Zo zorgt u ervoor dat uw onderneming daadwerkelijk voldoet aan de AVG.

Stap 1 Download de interactieve checklist

☐ CHECKLIST **Voldoe aan de privacyregels van de AVG in 9 stappen**

De eerste checklist heeft u nu voor u. Hierin staan alle onderdelen van deze toolbox benoemd. U kunt de status van de te nemen stappen in deze checklist bijhouden en afvinken welke onderdelen u heeft afgerond. Dit vinkje kunt u dus vast zetten.

Opmerkingen

Stap 2 De AVG in het algemeen

☐ ARTIKEL Hindernissen bij het werken met de AVG

In tegenstelling tot grote multinationals heeft uw onderneming waarschijnlijk geen grote afdeling beschikbaar die zorgt dat u voldoet de AVG. Onderzoek laat zien dat de uitvoering van deze privacywet niet altijd even gemakkelijk is. Daarom geeft dit verdiepingsartikel een opfrisser van de regels rondom drie mogelijke struikelblokken.

Opmerkingen

CHECKLIST Checklist implementatie AVG

Met de introductie van de AVG zijn de onderwerpen privacybescherming en informatiebeveiliging definitief onderdeel geworden van de verplichtingen voor een ondernemer. Deze checklist neemt u aan de hand van een aantal vragen mee door het opzetten van de belangrijkste aspecten van de AVG binnen uw onderneming. Voor een aantal onderwerpen van de checklist zijn aanvullende tools beschikbaar.

Opmerkingen

CHECKLIST De rechten van betrokkenen volgens de AVG

Sinds de invoering van de AVG zijn de regels over de omgang met persoonsgegevens veranderd. Zorg dat u weet op welke rechten een betrokkene — degene van wie u de gegevens heeft verwerkt — allemaal een beroep kan doen. U vindt die rechten in deze checklist.

Opmerkingen

CHECKLIST Controleer uw privacyverklaring

De AVG verlangt dat u transparant bent over de verwerkingen van persoonsgegevens binnen uw onderneming. Een privacyverklaring op de website is niet verplicht, maar is wel een handige manier om aan deze verplichting te voldoen. Deze checklist helpt u om te controleren of u alle belangrijke elementen benoemt in uw privacyverklaring.

Opmerkingen

V & A

[Wanneer krijgen we een boete van de AP?]

De Autoriteit Persoonsgegevens (AP) zal nooit zomaar boetes uitdelen. Daar gaat een heel proces aan vooraf. Maakt u onbedoeld een foutje, dan is het dus onwaarschijnlijk dat de AP meteen op de stoep staat. In deze Vraag & Antwoord staan de overtredingen waarbij de AP wél een onderzoek start.

Opmerkingen

INFOGRAPHIC

[Boetebedragen AVG]

Met de AVG pakt de Europese Unie ondernemingen die slordig omgaan met de privacy van klanten of werknemers hard aan. De boetebedragen zijn dan ook niet kinderachtig; bekijk ze in deze infographic.

Opmerkingen

NIEUWS

[Nieuwe regels voor berekenen van AVG-boetes ingegaan]

De Autoriteit Persoonsgegevens heeft nieuwe regels voor de berekening van de boetes voor de AVG bekendgemaakt die ook meteen zijn ingegaan. Zo gaat de grootte van een organisatie nu ook een rol spelen bij de start van de berekening en gelden er drie categorieën voor de ernst van de overtreding. Lees de nieuwe regels in dit nieuwsartikel.

Opmerkingen

Stap 3 De verwerking van persoonsgegevens door uw onderneming

☐  INFOGRAPHIC [Persoonsgegevens volgens de AVG]

Persoonsgegevens zijn ruim gedefinieerd: ze moeten unieke informatie over de persoon bevatten, op zichzelf dan wel in combinatie met elkaar. Wat voor persoonsgegevens zijn er? In deze infographic staan ze overzichtelijk opgesomd.

Opmerkingen

☐  VIDEO [Persoonsgegevens beveiligen volgens de AVG]

Volgens de Algemene verordening gegevensbescherming, beter bekend als de AVG, moet uw organisatie voor het beveiligen van persoonsgegevens passende technische en organisatorische maatregelen nemen. Carlijn van der Wild legt uit welke dat zijn, in 1 minuut. Bekijk de video.

Opmerkingen

☐  V & A [Wanneer is verwerken van persoonsgegevens toegestaan?]

Ondernemingen mogen onder de AVG alleen gewone persoonsgegevens verwerken als ze aan één van de zes grondslagen voldoen. Voor bijzondere persoonsgegevens zijn de regels nog strenger. De verwerking van bijzondere persoonsgegevens is verboden, tenzij ondernemingen zich kunnen beroepen op een specifieke wettelijke uitzondering én op één van de zes grondslagen voor het verwerken van 'gewone' persoonsgegevens. De zes grondslagen onder de AVG leest u in deze Vraag & Antwoord.

Opmerkingen

V & A

[Wanneer mag ik bijzondere persoonsgegevens verwerken?]

Volgens de AVG mag u geen bijzondere persoonsgegevens verwerken. Bijzondere persoonsgegevens kunnen zeer precaire informatie over betrokkenen bevatten, waardoor een hoog beveiligingsniveau is vereist. Alleen in een aantal uitzonderingssituaties moeten bijzondere persoonsgegevens wél verwerkt worden. Deze Vraag & Antwoord biedt een overzicht.

Opmerkingen

ARTIKEL

[Werken met toestemming verwerking persoonsgegevens]

Sinds de invoering van de AVG is er meer dan ooit om toestemming gevraagd voor de verwerking van persoonsgegevens. Veel van deze toestemmingen zijn echter helaas ongeldig, overbodig, onbruikbaar, verwarrend, en/of onzinnig. Weet hoe u moet omgaan met de grondslag 'toestemming' van de AVG? Lees het in dit verdiepingsartikel.

Opmerkingen

CHECKLIST

[Controleer de toestemming verwerking persoonsgegevens]

Veel van de toestemmingen voor de verwerking van persoonsgegevens zijn helaas ongeldig. Tegelijkertijd worden persoonsgegevens zonder geldige rechtsgrond verwerkt, wat feitelijk verboden is. Gebruik deze checklist gebruiken om te controleren of u de grondslag 'toestemming' op een juiste manier toepast.

Opmerkingen

☐ FORMULIER [Verwerkingsregister persoonsgegevens AVG]

De AVG verlangt dat ondernemingen een overzicht maken van alle verwerkingen van persoonsgegevens binnen de onderneming; een verwerkingsregister. Dit verwerkingsregister blijkt er in de praktijk ook voor te zorgen dat onlogische handelingen boven water komen, en zwakke plekken in de beveiliging worden opgespoord. Zet met behulp van dit formulier snel een eenvoudig maar doeltreffend verwerkingsregister op.

Opmerkingen

Stap 4 De verwerking van persoonsgegevens door externe partijen

☐ V & A [Met welke partijen is een verwerkersovereenkomst nodig?]

Als u persoonsgegevens van uw werknemers doorgeeft aan een verwerker in de zin van de AVG, bent u verplicht om een verwerkersovereenkomst te sluiten. Lees in deze Vraag & Antwoord welke partijen gezien worden als verwerker, en met welke verwerkingsverantwoordelijken u géén verwerkersovereenkomst hoeft op te stellen.

Opmerkingen

☐ ARTIKEL [De verantwoordelijkheden voor gegevensbescherming vaststellen]

Zolang bij een verwerking van persoonsgegevens maar één partij betrokken is, dan is het duidelijk wie de verantwoordelijkheid draagt. Als er echter meerdere partijen betrokken zijn, moet er duidelijkheid zijn over de eigenaar van de verantwoordelijkheid. In dit verdiepingsartikel leest u hoe het zit met dit ingewikkelde onderwerp.

Opmerkingen

☐  **FORMULIER** Overzicht leveranciers voor controle gegevensbeveiliging

Een goed overzicht van uw leveranciers helpt u, om te controleren of er aanvullende eisen moeten worden gesteld op het gebied van informatiebeveiliging. Verwerkt de leverancier persoonsgegevens namens u, en blijven de gegevens dan wel binnen de Europese Unie? Is er een verwerkersovereenkomst noodzakelijk, en zo ja, is deze ook al getekend? Dit formulier helpt u om zo'n overzicht op te stellen, en daarmee uw leveranciers onder controle te krijgen.

Opmerkingen

☐  **STAPPENPLAN** Sluit met de juiste leveranciers een verwerkersovereenkomst

Waarschijnlijk is er geen onderwerp van de AVG zo veel bediscussieerd en besproken als het onderwerp verwerker en verwerkingsverantwoordelijke. Hierbij zijn helaas veel foute aannames gemaakt en verwerkersovereenkomsten ten onrechte wel, of juist niet, opgesteld. Dit stappenplan helpt u te bepalen of u een verwerkersovereenkomst (of een andere overeenkomst) moet afsluiten.

Opmerkingen

☐  **OVEREENKOMST** Voorbeeld verwerkersovereenkomst AVG

Als duidelijk is dat het nodig is, kunt u met dit voorbeelddocument eenvoudig een complete en passende verwerkersovereenkomst opstellen. Ook bevat dit document een voorbeeldformulier 'overzicht van verwerkingen', een voorbeeld 'meldingsformulier beveiligingsincident en/of vermoedelijk datalek' en een overzicht van de beveiligingsmaatregelen. De verwerkersovereenkomst kunt u met dit voorbeeld op maat afstemmen met de betrokken partijen of voor een specifieke branche.

Opmerkingen

CHECKLIST Toets uw verwerkersovereenkomst

Heeft u al een verwerkersovereenkomst gesloten, maar twijfelt u of deze wel voldoet aan de eisen van de AVG? Of biedt een andere partij u een overeenkomst aan, en moet u bepalen of u deze kunt tekenen? Dan kunt u deze checklist gebruiken om de inhoud te controleren op de aanwezigheid van de verplichte elementen van de AVG.

Opmerkingen

Stap 5 Zorg voor een goede beveiliging van persoonsgegevens

REKENTOOL Meet het privacymanagement van uw organisatie

Informatiebeveiliging is onlosmakelijk verbonden aan het beschermen van persoonsgegevens, en een passend beschermingsniveau is verplicht volgens de AVG. Deze rekentool geeft u de mogelijkheid het privacymanagementniveau te meten van uw onderneming op het gebied van de AVG.

Opmerkingen

FORMULIER Controleer de toegangsrechten

Bij een goede gegevensbeveiliging hoort ook een goed toegangsrechtenbeheer. Iedereen mag alleen maar bij informatie die nodig is voor de werkzaamheden; in de AVG wordt dit als eis genoemd. In dit formulier staan verschillende controles of toegangsrechten op een correcte manier zijn toegekend. De controles sluiten elkaar niet uit, maar kunnen het beste allemaal worden uitgevoerd.

Opmerkingen

TOOLBOX [Zo verbetert u de cybersecurity van uw onderneming]

De AVG ziet een veilige digitale omgeving binnen uw onderneming als voorwaarde voor een goede beveiliging van persoonsgegevens. In deze toolbox leest u niet alleen hoe uw onderneming zich zo goed mogelijk kan beschermen tegen digitale aanvallen, maar ook hoe uw werknemers daaraan kunnen bijdragen.

Opmerkingen

Stap 6 De risico's op het gebied van informatiebeveiliging

ARTIKEL [Risicoanalyse, privacybescherming en informatiebeveiliging]

De basis voor privacybescherming en informatiebeveiliging is het analyseren en beheersen van risico's. Zonder risico's zouden er geen maatregelen voor bescherming nodig zijn. Elke onderneming, groot of klein, moet weten welke risico's er bestaan, hoe groot de risico's zijn, en vervolgens de juiste stappen ondernemen om de risico's zo goed mogelijk in de hand te houden. Dit verdiepingsartikel is een inleiding op het onderwerp, zodat u goed begrijpt wat nu eigenlijk een risico is.

Opmerkingen

FORMULIER [Risicoanalyse informatiebeveiliging en AVG]

Informatiebeveiliging is een onderwerp dat op basis van risico's wordt aangepakt. Er hoeven geen maatregelen genomen te worden voor een situatie die nooit zal voorkomen, of die geen enkel negatief effect kunnen hebben. Omgekeerd moeten juist wel maatregelen genomen worden als het waarschijnlijk is dat een ongunstige situatie zich op afzienbare tijd kan voordoen. Met dit formulier brengt u eenvoudig de risico's op het gebied van informatiebeveiliging en de AVG in kaart, en weet u waar u uw energie in moet steken.

Opmerkingen

☐ FORMULIER Risicobehandelplan AVG

Dit formulier is een voorbeeldtekst voor het opstellen van een risicobehandelplan voor de AVG. In een risicobehandelplan beschrijft u alle AVG-risico's die nog moeten worden aangepakt, en de resultaten van de genomen maatregelen van de overige AVG-risico's. Doordat u alles vastlegt, kunt u op een later tijdstip terugvinden (en zo nodig aantonen) hoe u bepaalde risico's heeft aangepakt.

Opmerkingen

Stap 7 Voer een Data Privacy Impact Assessment (DPIA) uit

☐ V & A Is een Data Privacy Impact Assessment (DPIA) verplicht?

U moet een Data Privacy Impact Assessment (DPIA) vooraf uitvoeren bij verwerkingen met een potentieel hoog risico voor de betrokkenen. Denkt u zelf dat het wel meevalt met het hoge risico, controleer dan voor de zekerheid toch de lijst in deze Vraag & Antwoord. Dan weet u zeker of een DPIA wel of niet verplicht is.

Opmerkingen

☐ INFOGRAPHIC Wel of geen DPIA voor de AVG?

U bent verplicht een DPIA uit te voeren wanneer de gegevensverwerking van uw onderneming een privacyrisico oplevert. Als u in deze infographic minstens twee vinkjes kunt zetten, is dat al het geval.

Opmerkingen

☐ FORMULIER [Data Privacy Impact Assessment (DPIA)]

Als de uitvoering van een DPIA verplicht is, dan is het wel fijn als u geen overbodig werk doet. Dit formulier zorgt ervoor dat u alles precies voldoende beschrijft, zodat de DPIA voldoet aan de eisen. Het resultaat is een rapport waarmee u de privacyaspecten van een nieuwe ontwikkeling goed onder controle kunt houden.

Opmerkingen

Stap 8 De functionaris voor de gegevensbescherming (FG)

☐ V & A [Is een functionaris voor de gegevensbescherming (FG) verplicht?]

In deze Vraag & Antwoord kunt u lezen of uw onderneming verplicht is een FG aan te stellen. Ook als uw onderneming niet verplicht is om een FG aan te stellen, is het wel toegestaan en soms ook zeer aan te bevelen. Een goede FG brengt kennis en kunde in de onderneming op het gebied van gegevensbescherming.

Opmerkingen

☐ CHECKLIST [De positie en taken van de FG volgens de AVG]

Heeft u een FG aangesteld? Dan stelt de AVG eisen aan de positie van de FG binnen uw onderneming. Ook verwacht de AVG dat deze FG een aantal specifieke taken uitvoert. Met deze checklist controleert u of de positie van de FG op een goede manier is vormgegeven, en of de juiste taken zijn toegekend.

Opmerkingen

☐ V & A [Wat is het verschil tussen de FG en de privacy officer?]

De taken van een functionaris gegevensbescherming en een privacy officer kunnen overlappen. Het belangrijkste verschil is dat de FG toezicht houdt op het beleid van de organisatie. Een privacy officer heeft (ook) een belangrijke rol heeft bij de ontwikkeling, implementatie en de uitvoering van beleid. De rollen van een FG en die van een privacy officer mogen niet door één en dezelfde persoon worden uitgevoerd. Lees in deze Vraag en Antwoord waarom dit zo is.

Opmerkingen

Stap 9 De rol van de OR bij de AVG

☐ ARTIKEL [OR waakt over privacy]

Volgens de AVG is uw bestuurder verplicht om zorgvuldig om te gaan met persoonsgegevens. Privacy is daarom een belangrijk aandachtspunt voor iedere organisatie en voor de ondernemingsraad (OR) in het bijzonder. Uw OR heeft namelijk instemmingsrecht bij het privacybeleid en kan aan de bel trekken als uw bestuurder zich niet aan de regels houdt. Lees in dit verdiepingsartikel wat de OR mag en moet doen.

Opmerkingen

☐ NIEUWS [OR moet waken voor dubbelrol FG]

Om de kwaliteit van het privacybeleid binnen de organisatie te waarborgen, is er onderscheid nodig tussen de taken van een functionaris gegevensbescherming (FG) en die van een privacy officer. Zijn deze taken gecombineerd in één functie, dan is er sprake van belangenverstrengeling. Lees in dit nieuwsartikel waarom dit ook een aandachtspunt is voor de OR.

Opmerkingen

Toch nog vragen?
Als u na het bestuderen van deze toolbox nog vragen heeft over de AVG, kunt u die voorleggen aan de adviseurs van de adviesdesk. Stel als abonnee gratis uw vraag via rendement.nl/adviesdesk en ontvang binnen vijf werkdagen een antwoord.