AUTORITEIT
PERSOONSGEGEVENS

Uitslag AVG-Regelhulp

Stap 1.

U weet welk type persoonsgegevens u verwerkt. Heel goed!

U heeft aangegeven dat uw organisatie persoonsgegevens verwerkt. Dat betekent dat uw organisatie op 25 mei 2018 klaar moet zijn voor de Algemene verordening gegevensbescherming (AVG).

Wat betekent dit voor u?

Besef dat het tijd en capaciteit kost om u voor te bereiden op de nieuwe Europese privacyregels. De AVG brengt nieuwe verplichtingen voor organisaties met zich mee die waarschijnlijk veel impact hebben op de manier waarop u nu persoonsgegevens verwerkt. Bijvoorbeeld op de inrichting van uw werkprocessen en online beveiligingssystemen.

Wat moet u doen?

Actiepunt:
De tips en adviezen van deze AVG-regelhulp helpen u op weg.

Stap 2.

U heeft een grondslag om persoonsgegevens te verwerken. Een onmisbaar begin.

U heeft aangegeven dat u voor één of meerdere verwerkingen een grondslag heeft. Als dat klopt dan heeft u het recht om ‘gewone’ persoonsgegevens te verwerken. Maar u moet dat wel zorgvuldig doen. Hieronder staan bij bepaalde grondslagen nog een aantal aandachtspunten.

Wat moet u doen?

Actiepunt:
Zorg ervoor dat u goed kunt onderbouwen dat u de verwerking op deze grondslag(en) mag baseren. Bijvoorbeeld wanneer uw doelgroep of de Autoriteit Persoonsgegevens (AP) daar om vraagt. Op autoriteitpersoonsgegevens.nl vindt u meer informatie over de grondslagen.

Actiepunt:
Zorg ervoor dat u uw doelgroep goed informeert over wat u met hun persoonsgegevens doet. Op autoriteitpersoonsgegevens.nl vindt u meer informatie over de informatieplicht.

Extra actiepunten bij grondslag 'Toestemming'

U heeft aangegeven dat u voor uw verwerking(en) toestemming heeft. Daarvoor hebben wij nog een aantal extra tips. Het is belangrijk dat de mensen uit uw doelgroep goed weten waarvoor zij toestemming hebben gegeven. Zodat zij weten wat u met hun gegevens doet. En dat zij hun toestemming even makkelijk kunnen intrekken als dat zij gegeven is.

Actiepunt:
Check of u de toestemming op de juiste manier vraagt.

Actiepunt:
Kunt u aantonen dat u geldige toestemming heeft wanneer uw doelgroep of de AP daar om vraagt? Check autoriteitpersoonsgegevens.nl hoe u kunt aantonen dat u toestemming heeft gevraagd.

Actiepunt:
Is uw website of app bedoeld voor minderjarigen (onder de 16 jaar), of weet u dat veel kinderen er gebruik van maken? Dan moet u controleren of er toestemming is verleend door de persoon die de ouderlijke verantwoordelijkheid draagt. Let er op dat er kinderen extra goed beschermd worden tegen marketing. Er gelden bijvoorbeeld strengere regels voor het opstellen van profielen aan de hand van het gebruik van apps.

Actiepunt:
Verwerkt u de gegevens als werkgever of overheidsinstelling? Dan is toestemming in de meeste gevallen niet de juiste grondslag.

Actiepunt:
Richt uw systemen zo in dat betrokkenen hun toestemming ook weer kunnen intrekken.

Extra actiepunten bij grondslag 'Noodzakelijk voor de uitvoering van een overeenkomst'

U heeft aangegeven dat uw verwerkingen noodzakelijk zijn om de overeenkomst na te komen met betrokkenen.

Actiepunt:
Zorg ervoor dat u goed kunt onderbouwen dat u zich op deze grondslag mag baseren.

U heeft geen grondslag om bijzondere persoonsgegevens te verwerken. Stop onmiddellijk met de verwerking.

U heeft aangegeven dat u zich niet op de twee eisen kunt beroepen die gelden voor de verwerking van bijzondere persoonsgegevens. Dat betekent dat het verwerken van bijzondere persoonsgegevens voor uw organisatie verboden is.

Actiepunt:
Zorg ervoor dat uw organisatie deze bijzondere persoonsgegevens niet langer verzamelt.

Verwijder nauwkeurig álle bijzondere persoonsgegevens die onder deze verwerking vallen.

Op autoriteitpersoonsgegevens.nl vindt u meer informatie over het verwerken van bijzondere persoonsgegevens.

U heeft geen grondslag om strafrechtelijke persoonsgegevens te verwerken. Stop onmiddellijk met de verwerking.

U heeft aangegeven dat u zich niet kunt beroepen op een van de twee uitzonderingen die gelden voor het mogen verwerken van strafrechtelijke persoonsgegevens. Dat betekent dat het verwerken van strafrechtelijke persoonsgegevens voor uw organisatie verboden is.

Actiepunt:
Zorg ervoor dat uw organisatie de strafrechtelijke persoonsgegevens niet langer verzamelt. Verwijder nauwkeurig álle strafrechtelijke persoonsgegevens die onder deze verwerking vallen.

Op autoriteitpersoonsgegevens.nl vindt u meer informatie over het verwerken van strafrechtelijke persoonsgegevens.

Stap 3.

U heeft waarschijnlijk geen FG nodig. Een privacyexpert kan wel nuttig zijn.

U heeft aangegeven dat u aan geen van de criteria voor het aanstellen van een functionaris gegevensbescherming (FG) voldoet. Als dat klopt dat bent u niet verplicht om een FG aan te stellen.

Maar let op:
De genoemde criteria zijn een hulpmiddel. U moet zelf een inschatting maken of uw organisatie een FG nodig heeft.

Actiepunt:
Stelt u geen FG aan? Zorg ervoor dat u goed kunt onderbouwen waarom u daarvoor kiest wanneer de Autoriteit Persoonsgegevens daar om vraagt.

Actiepunt:
Ook al bent u het niet verplicht, het kan heel nuttig zijn om iemand aan te nemen of in te huren die gespecialiseerd is in de bescherming van persoonsgegevens.

Op autoriteitpersoonsgegevens.nl vindt u meer informatie en veelgestelde vragen over de FG.

Stap 4.

Het lijkt erop dat u geen DPIA hoeft uit te voeren.

U heeft aangegeven dat uw verwerking(en) aan geen of slechts 1 van de criteria voldoet. Dat betekent dat er waarschijnlijk geen sprake is van een hoog privacyrisico. Als dat inderdaad zo is, dan hoeft u geen DPIA uit te voeren.

Maar let op:
Ook als u geen of maar één van de criteria hebt aangevinkt, kan het toch zijn dat er sprake is van een hoog privacyrisico. De genoemde criteria zijn slechts een hulpmiddel. U moet zelf een inschatting maken van de risico's van uw gegevensverwerking voor de betrokken personen.

Actiepunt:
Kiest u ervoor om geen DPIA uit te voeren? Zorg er dan voor dat u documenteert waarom. En dat u kunt motiveren waarom u hiervoor heeft gekozen. Dat maakt onderdeel uit van uw verantwoordingsplicht aan de Autoriteit Persoonsgegevens.

Op autoriteitpersoonsgegevens.nl vindt u meer informatie en veelgestelde vragen over DPIA's en de verantwoordingsplicht.

Stap 5.

Gefeliciteerd! U bent goed op weg met privacy by design & default.

U heeft aangegeven dat u voldoet aan een aantal algemene uitgangspunten voor privacy by design en by default. En dat de instellingen van uw producten, diensten en interne systemen standaard privacyvriendelijk zijn ingesteld. Dat betekent dat u goed op weg bent.

Maar privacy by design en by default blijven maatwerk. Dat betekent dat u goed moet onderzoeken of er nog meer maatregelen nodig zijn.

Actiepunt:
Kijk nog eens kritisch naar de persoonsgegevens die u verwerkt. Zijn die gegevens echt noodzakelijk voor het doel van de verwerking? Verwijder de 'nice to haves'.

Actiepunt:
Leg voorstellen voor nieuwe systemen, apparaten of verwerkingen in een vroeg stadium voor aan een expert. Bijvoorbeeld aan uw FG, privacy officer of externe privacyjurist. Zodat hij of zij mee kan kijken of in het ontwerp voorzien is in passende technische en organisatorische maatregelen.

Actiepunt:
Bekijk uw eigen producten, diensten en interne systemen vanuit het perspectief van een buitenstaander: is alles daadwerkelijk privacyvriendelijk ingericht?

Actiepunt:
Controleer steekproefsgewijs de oudst aanwezige gegevens in uw eigen bestanden en back-ups. Op die manier kunt u checken of de door u ingevoerde bewaartermijnen ook daadwerkelijk worden nageleefd.

Stap 6.

U hoeft waarschijnlijk geen register van verwerkingsactiviteiten op te stellen.

U bent waarschijnlijk niet verplicht om een register van verwerkingsactiviteiten bij te houden omdat u heeft aangegeven dat uw organisatie niet voldoet aan de criteria die daarvoor gelden.

Tip:
Ook als u niet verplicht bent om een verwerkingsregister bij te houden, kan het wel nuttig zijn om dat te doen. Zo’n register geeft u namelijk een goed overzicht van de verwerkingen die plaatsvinden binnen uw organisatie.

Stap 7.

Goed bezig! U heeft al hele belangrijke beveiligingsmaatregelen genomen.

U heeft aangegeven dat uw organisatie een beleidsdocument voor informatiebeveiliging heeft opgesteld en dat u voldoende technische en organisatorische maatregelen heeft genomen om de persoonsgegevens goed te beveiligen. Dat betekent dat u goed op weg bent.

Maar beveiliging is maatwerk. Dat betekent dat er geen standaardpakket aan maatregelen te geven is waar u aan moet voldoen. Bovendien is beveiligen een continu proces (plan, do, check, act). U moet continu monitoren of de getroffen beveiligingsmaatregelen nog adequaat zijn.

Actiepunt:
Zorg er voor dat u uw medewerkers duidelijk informeert over de AVG-beveiligingseisen en -plichten. Niet alleen eenmalig bij indiensttreding, maar door hierover vaak en zichtbaar te communiceren.

Actiepunt:
Maakt u gebruik van verwerkers? Blijf ook hun werkwijze monitoren door gebruik te maken van uw recht om auditrapporten op te vragen.

Tip:
Overweeg of het, gezien de risico's voor betrokkenen, verstandig is om af en toe een beveiligingstest te laten doen door een extern bedrijf.

Stap 8.

Uw verwerkersovereenkomst voldoet aan de AVG: Chapeau!

U heeft aangegeven dat uw verwerkersovereenkomst(en) volledig is/zijn. Dat betekent dat u

goed op weg bent.

Actiepunt:
Zorg ervoor dat u dit blijft monitoren. Mogelijk dat de verwerking of situatie in de toekomst verandert waardoor er nieuwe afspraken met uw verwerker nodig zijn.

Stap 9.

Het lijkt erop dat u goed bent voorbereid op de informatieplicht. Bij u weten mensen waar ze aan toe zijn!

U heeft aangegeven dat u een document heeft opgesteld waarin u betrokken personen informeert over de verwerking van privacygegevens. Bijvoorbeeld in de vorm van een privacyverklaring.

U heeft ook aangegeven dat dit document voldoet aan de AVG. Als dat klopt dan bevat uw verklaring voldoende informatie, biedt u deze op een toegankelijke plek aan en heeft u deze in begrijpelijke taal geschreven. Uw doelgroep weet bij u dus precies wat er met hun gegevens gebeurt. U bent goed bezig!

Stap 10.

U onderscheidt zich positief van anderen. Mensen hebben bij u controle over hun rechten.

U heeft aangegeven dat u bent voorbereid op de privacyrechten die mensen onder de AVG kunnen uitoefenen. Dan bent u goed op weg. U geeft daarmee de personen van wie u gegevens verwerkt controle over wat er met hun persoonsgegevens gebeurt.

Twijfelt u nog over bepaalde punten? Op autoriteitpersoonsgegevens.nl vindt u meer informatie over alle rechten die personen onder de AVG hebben en hoe u zich daar op voorbereidt.