



# Bereid u voor op de AVG

U heeft nog tot:

**25 mei 2018**



## Zijn de juiste mensen op de hoogte?

Zorg ervoor dat de beleidsbepalers binnen uw organisatie op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op de huidige processen, diensten en goederen en welke aanpassingen eventueel nodig zijn. Er staan hoge boetes tegenover overtredingen, dus onderschatten is geen optie.



## Meer en verbeterde privacyrechten

De AVG regelt dat iedereen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten krijgt. Uw organisatie moet ervoor zorgen dat de betrokkenen hun privacyrechten goed kunnen uitoefenen, zoals het recht op inzage en dataportabiliteit. Bij klachten van betrokkenen is de Autoriteit Persoonsgegevens verplicht om te handelen.

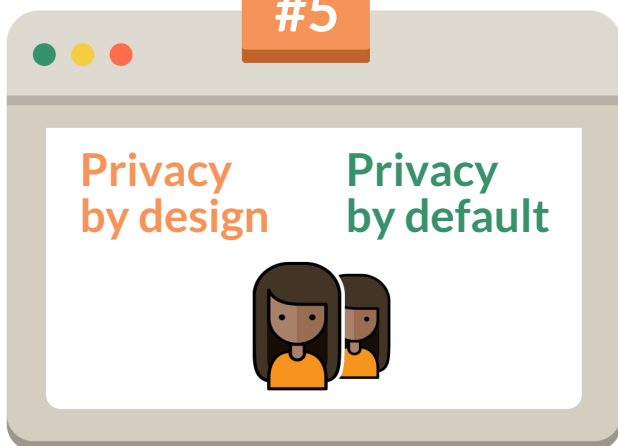
#3



## Documentatieplicht

Breng alle gegevensverwerkingen in kaart binnen uw organisatie. Documenteer welke persoonsgegevens u verwerkt, met welk doel u dit doet, waar de gegevens vandaan komen en met wie u ze deelt. U heeft onder de AVG een documentatieplicht, waarmee u aangeeft dat uw organisatie in overeenstemming is met de AVG.

#5



## Loop voor op de AVG

Zorg dat u de verplichte uitgangspunten van privacy by design en privacy by default implementeert in uw organisatie:

Privacy by design: bij nieuwe producten en diensten zorgt u voor een goede bescherming van de persoonsgegevens.

Privacy by default: neem maatregelen zodat u alleen persoonsgegevens verwerkt die noodzakelijk zijn.

#4



## Brengt privacyrisico's in kaart

U moet een PIA uitvoeren als uw beoogde gegevensverwerking een hoog privacyrisico met zich meebrengt. Een PIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. Vervolgens neemt u maatregelen om de risico's te verkleinen.

#6



## Moet u een FG aanstellen?

Onder de AVG moeten alle overheidsinstellingen en instanties met (semi-)publieke taken, organisaties die op grote schaal betrokkenen observeren en alle organisaties die structureel bijzondere persoonsgegevens of strafrechtelijke persoonsgegevens verwerken, zijn verplicht een functionaris gegevensbescherming (FG) aan te stellen. Dat is een interne onafhankelijke adviseur en toezichthouder die betrokken moet worden bij alle beleidsvraagstukken.

#7

Meldplicht datalekken



## AVG stelt strengere eisen

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde, maar de nieuwe wetgeving stelt wel strengere eisen aan uw Eigen registratie van de datalekken die zich bij uw organisatie hebben voorgedaan. U moet alle datalekken documenteren en die meldplicht gaat verder dan de protocolplicht van de Wbp.

#8

Bewerker-  
overeenkomsten

## Uitbesteden brengt ook verplichtingen met zich mee

Heeft u uw gegevensverwerking uitbesteed aan een andere partij (in de AVG benoemd als 'verwerker'), dan moet u beoordelen of de overeengekomen maatregelen in bestaande contracten met deze partij voldoen aan de vereisten in de AVG.

#9

Leidende  
toezichthouder

## Vestigingen in meerdere EU-lidstaten

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

#10

Toestemming



## Strengere eisen aan toestemming

Nieuw onder de AVG 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.

## Handige tips

Op Rendement.nl vindt u nog meer handige tools over de Algemene Verordening Gegevensbescherming (AVG), zoals 'Wijzigingen AVG ter vervanging van Wbp' en 'Boetes AVG'. Voor meer informatie en een overzicht aan nieuwsartikelen over de AVG bekijkt u de themapagina.



Bron: Autoriteit Persoonsgegevens