

Aandachtsgebieden voor AVG volgens de AP

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU).



Bewustwording (1)

Zorg ervoor dat de relevante mensen in uw organisatie op de hoogte zijn. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen.



Rechten van betrokkenen (2)

Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen.



Overzicht verwerkingen (3)

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt. Onder de AVG heeft u een verantwoordingsplicht.



Data Protection Impact Assessment (4)

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen.



Privacy by Design en Privacy by Default (5)

Privacy by design houdt in dat u er al bij het ontwerp voor zorgt voor goede bescherming van persoonsgegevens. Privacy by default houdt in dat u maatregelen neemt om alléén noodzakelijke persoonsgegevens te verwerken.



Functionaris voor de gegevensbescherming (6)

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensbescherming (FG) aan te stellen (verplicht bij overheidsinstanties). Bepaal nu alvast of dit voor uw organisatie geldt.



Meldplicht datalekken (7)

U moet een eigen registratie bijhouden van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan.



Verwerkersovereenkomsten (8)

Heeft u uw gegevensverwerking uitbesteed aan een verwerker? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw verwerkers nog steeds toereikend zijn en voldoen aan de eisen van de AVG.



Leidende toezichthouder (9)

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Bepaal welke.



Toestemming (10)

Voor sommige gegevensverwerkingen hebt u toestemming nodig van de betrokkenen. U moet kunnen aantonen dat u geldige toestemming van mensen heeft en het moet makkelijk zijn deze toestemming weer in te trekken.

