La Gro Geelkerken advocaten

STEPPING STONES

GDPR

1 Breng de gegevensstromen binnen uw organisatie in kaart

Breng alle gegevensstromen binnen uw organisatie in kaart. Bepaal vervolgens welke van deze gegevens ook daadwerkelijk persoonsgegevens bevatten.

2 Bepaal of u persoonsgegevens mag verwerken

Als organisatie mag u niet zomaar persoonsgegevens verwerken. U moet daarvoor een wettelijke grondslag hebben. De AVG kent 6 grondslagen, ex artikel 6 AVG:

1. Toestemming van de betrokken persoon;
2. De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst;
3. De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting;
4. De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen;
5. De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag;
6. De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Indien u de gegevensverwerking niet kan baseren op minimaal één van deze grondslagen, dan heeft u niet het recht om de persoonsgegevens te verwerken.
Controleer derhalve of u persoonsgegevens mag verwerken op basis van voornoemde grondslagen van de AVG.

3 Verwerkingsregister invullen

Op grond van uw verantwoordingsplicht als organisatie houdt u een register bij van alle verwerkingsactiviteiten. In het verwerkingsregister registreert u o.a. welke persoonsgegevens u verwerkt, met welk doel u dit doet, waar deze gegevens vandaan komen, waar u ze opslaat, hoe u ze beveiligt, met wie u ze deelt en hoe lang u ze bewaart.

4 Functionaris voor de gegevensbescherming (FG)

Op grond van de AVG kan uw organisatie verplicht zijn om een Functionaris voor de Gegevensbescherming aan te stellen. Bepaal of uw organisatie hiertoe verplicht is.

Verplicht?

- Overheden en publieke organisaties;
- Regelmatige en stelselmatige observatie op grote schaal;
- Grootschalige verwerking van bijzondere gegevens als dit een kernactiviteit is.

5 Stel uw eigen privacybeleid op | informatieplicht

Leg schriftelijk vast hoe u omgaat met persoonsgegevens binnen uw organisatie. Stel uw eigen privacybeleid op en informeer uw betrokkenen (zoals uw werknemers en klanten). Werk het beleid verder uit in uw personeelshandboek. Zorg ervoor dat uw medewerkers op de hoogte zijn van het privacybeleid en hiernaar handelen. Zet een awareness training jaarlijks op de agenda! De meeste datalekken ontstaan immers door menselijke 'fouten'.

Maak ook gebruik van een privacy statement voor klanten of leveranciers, zodat zij ook kunnen teruglezen (op uw website bijvoorbeeld) hoe uw organisatie omgaat met eventuele verwerkingen van persoonsgegevens van de klant c.q. betrokkene(n).

6 Privacy by design & privacy by default

Pas uw processen, procedures en systemen aan. Denk hierbij aan privacy by design waarbij u bij het ontwikkelen van (nieuwe) informatiesystemen en diensten vanaf het begin af aan rekening houdt met privacy aspecten van personen.

Privacy by default houdt in dat de instellingen van bijvoorbeeld een socialmediaplatform of een programma, app, website of dienst standaard de hoogst mogelijke privacy garandeert. Het privacy by default principe dient ervoor te zorgen dat de privacy van gebruikers in dit soort situaties maximaal wordt beschermd.

7 Zorg voor dataportabiliteit

Onder de AVG hebben mensen het recht op dataportabiliteit, oftewel overdraagbaarheid van persoonsgegevens. U dient hierop voorbereid te zijn indien u zo'n verzoek krijgt, omdat u hieraan gevolg dient te geven. Zorg er daarom voor dat personen hun persoonsgegevens kunnen opvragen en door kunnen geven aan een andere organisatie.

8 Inventariseer verwerkersovereenkomsten

Controleer aan de hand van het verwerkingsregister met welke partijen uw bedrijf nog verwerkersovereenkomsten dient te sluiten. Hierbij is het aan te raden om uw eigen modelverwerkersovereenkomst te verstrekken, zodat u zelf grip heeft op de te maken afspraken.

9 Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. Daarentegen stelt de AVG wel strengere eisen aan uw eigen administratie van de datalekken die zich binnen uw organisatie hebben voorgedaan. Zo moet u bijvoorbeeld al uw datalekken documenteren. Op grond hiervan dient de Autoriteit Persoonsgegevens (AP) te kunnen controleren of u heeft voldaan aan de meldplicht.

10 Data protection impact assessment (DPIA)

Op grond van de AVG kunt u verplicht zijn een zogeheten data protection impact assessment uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. Op de website van de Autoriteit Persoonsgegevens vindt u een lijst van soorten verwerkingen waarvoor het uitvoeren van een DPIA verplicht is vóórdat u met verwerken begint. U dient zelf te bepalen als verwerkingsverantwoordelijke of u hiertoe verplicht bent. Hierbij dient opgemerkt te worden dat u niet mag beginnen met het verwerken van gegevens voordat u een DPIA heeft uitgevoerd.

La Gro Geelkerken advocaten

Contact

Heeft u vragen over de implementatie van de Algemene Verordening Gegevensbescherming (AVG) of zou u graag een privacy audit willen laten uitvoeren binnen uw organisatie? Neem dan contact op met de afdeling privacy van La Gro Geelkerken Advocaten. Zij zijn gespecialiseerd in het begeleiden van bedrijven bij de implementatie van de Europese privacywetgeving en staan bedrijven bij in procedures over privacy-vraagstukken.

Mr. B. (Benjamin) Niemeijer

0172-503250
b.niemeijer@lgga.nl
Mr. B. (Benjamin) Niemeijer

Mr. N.M.M. (Nathalie) van der Zande

0172-503250
n.vanderzande@lgga.nl
Mr. N.M.M. (Nathalie) van der Zande

Denk vooruit. La Gro Geelkerken.