https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg

Verantwoordingsplicht

De Algemene verordening gegevensbescherming (AVG) legt meer verantwoordelijkheid bij u als organisatie om aan te tonen dat u aan de privacyregels voldoet. Door te voldoen aan uw verantwoordingsplicht (accountability) levert u een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

De nieuwe regels dwingen u om goed na te denken over hoe uw organisatie persoonsgegevens verwerkt en beschermt. De verantwoordingsplicht houdt in dat u moet kunnen aantonen dat uw verwerkingen aan de regels van de AVG voldoen.

U moet bijvoorbeeld kunnen aantonen dat een verwerking aan de belangrijkste beginselen van verwerking voldoet, zoals:

- rechtmatigheid;
- transparantie;
- doelbinding;
- juistheid.

Ook moet u kunnen laten zien dat u de juiste technische en organisatorische maatregelen hebt genomen om de persoonsgegevens te beschermen.

U bent verplicht verantwoording af te leggen over uw gegevensverwerkingen wanneer de Autoriteit Persoonsgegevens daar om vraagt. Zorg daarom dat u aan uw verantwoordingsplicht voldoet vanaf 25 mei 2018. Vanaf dan geldt de AVG.

Lees meer over de voorbereiding op de AVG.

Bekijk binnen het onderwerp Verantwoordingsplicht

- Alle antwoorden op mijn vragen

Alle antwoorden op mijn vragenVragen over de verantwoordingsplicht

- Hoe voldoe ik aan de verantwoordingsplicht?

  In de Algemene verordening gegevensbescherming (AVG) staan een aantal verplichte maatregelen genoemd waarmee u aan uw verantwoordingsplicht (accountability) voldoet. Naast de verplichte maatregelen kunt u ervoor kiezen om extra maatregelen te nemen.

  ### Verplichte maatregelen

  De verplichte maatregelen die de AVG concreet noemt zijn:

- het bijhouden van een register van verwerkingsactiviteiten;
- het uitvoeren van een data protection impact assessment (DPIA);
- het bijhouden van een register van datalekken die zijn opgetreden;
- het aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer u voor een verwerking toestemming nodig heeft.
- wanneer onduidelijk is of u verplicht bent om een Functionaris voor gegevensbescherming aan te stellen, moet u goed kunnen onderbouwen waarom u ervoor gekozen hebt om al dan niet een FG aan te stellen.

Meer informatie over deze verplichtingen vindt u in ons AVG-dossier en in de AVG zelf.

Extra maatregelen

Naast de verplichte maatregelen kunt u ervoor kiezen om extra maatregelen te nemen waarmee u aantoont dat u voldoet aan de eisen van de AVG. Bijvoorbeeld:

- het aansluiten bij een gedragscode;
- het behalen van een bepaald certificaat;
- het hanteren van een specifiek ICT-beveiligingsbeleid;
- het afleggen van verantwoording over de verwerking van persoonsgegevens in uw jaarverslag of in een speciaal privacy-jaarverslag.

Hoewel deze maatregelen niet verplicht zijn, helpen zij u wel om aan de toezichthouder te laten zien dat u voldoet aan de eisen van de AVG. Daarom moedigen wij deze vrijwillige maatregelen aan.

- Ben ik verplicht om een register van verwerkingsactiviteiten op te stellen?

In de Algemene verordening gegevensbescherming (AVG) staan een aantal verplichte maatregelen genoemd waarmee u aan uw verantwoordingsplicht (accountability) kunt voldoen. Een van die verplichtingen is het 'register van verwerkingsactiviteiten'. Of u zo'n verwerkingsregister moet opstellen, hangt af van de omvang van uw organisatie en het type gegevens dat u verwerkt.

Organisaties met meer dan 250 medewerkers

Heeft uw organisatie meer dan 250 medewerkers? Dan bent u verplicht om een verwerkingsregister bij te houden.

Organisaties met minder dan 250 medewerkers

Heeft uw organisatie minder dan 250 medewerkers? Dan moet u over een verwerkingsregister beschikken wanneer u persoonsgegevens verwerkt:

- die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt en/of;
- waarvan de verwerking niet incidenteel is en/of;

- die vallen onder de categorie bijzondere persoonsgegevens. Zoals gegevens over godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens.

Bent u verplicht om een verwerkingsregister op te stellen? Dan moet u dit register kunnen verstrekken wanneer de Autoriteit Persoonsgegevens daar om vraagt.

- Wat moet er in het register van verwerkingsactiviteiten staan?

  Het register van verwerkingsactiviteiten bevat informatie over de persoonsgegevens die u verwerkt. U mag zelf weten hoe u het register opstelt. Wel schrijft de AVG voor welke informatie u als verantwoordelijke of verwerker in het register moet zetten. Als de Autoriteit Persoonsgegevens (AP) daar om vraagt, moet u het register direct kunnen laten zien.

Is uw organisatie de 'verwerkingsverantwoordelijke'?

Stelt uw organisatie zelf het doel en de middelen voor de verwerking van de persoonsgegevens vast? Dan is uw organisatie de verwerkingsverantwoordelijke. De wet schrijft voor dat deze verantwoordelijken de volgende informatie in het register moeten opnemen:

- de naam en contactgegevens van:
  - uw organisatie, of de vertegenwoordiger van uw organisatie;
  - eventuele andere organisaties met wie u gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld;
  - de Functionaris voor de gegevensbescherming (FG) als u die heeft aangesteld;
  - eventuele andere internationale organisaties waar u persoonsgegevens mee deelt.
- de doelen waarvoor u de persoonsgegevens verwerkt. Bijvoorbeeld voor de werving en selectie van personeel, het bezorgen van producten of direct marketing;
- een beschrijving van de categorieën van personen van wie u gegevens verwerkt. Bijvoorbeeld uitkeringsgerechtigden, klanten of patiënten;
- een beschrijving van de categorieën van persoonsgegevens. Zoals het BSN, NAW-gegevens, telefoonnummers, camerabeelden of IP-adressen;
- de datum waarop u de gegevens moet wissen (als dat/deze bekend is);
- de categorieën van ontvangers aan wie u persoonsgegevens verstrekt;
- deelt u de gegevens met een land of internationale organisatie buiten de EU? Dan moet u dit aangeven in het register;
- een algemene beschrijving van de technische en organisatorische maatregelen die u hebt/heeft genomen om persoonsgegevens die u verwerkt te beveiligen.

Is uw organisatie een 'verwerker'?

Verwerkt u in opdracht van een verantwoordelijke persoonsgegevens? Bijvoorbeeld omdat u werkt bij een administratiekantoor of een online dienst voor gegevensopslag? Dan moet de volgende informatie in uw verwerkingsregister staan:

- De naam en contactgegevens van;

        - uw organisatie, of de vertegenwoordiger van uw organisatie, of de verwerkingsverantwoordelijke;
        - een Functionaris voor de gegevensbescherming (FG) als u die heeft aangesteld;
        - een beschrijving van de categorieën van verwerkingen die u in opdracht van iedere verantwoordelijke uitvoert;
        - eventuele andere internationale organisaties met wie u persoonsgegevens deelt.
        - deelt u de gegevens met een land of internationale organisatie buiten de EU? Dan moet u dit aangeven in het register;
    - een algemene beschrijving van de technische en organisatorische maatregelen die u hebt/heeft genomen om persoonsgegevens die u verwerkt te beveiligen.

- Wat moet er volgens de AVG in een gegevensbeschermingsbeleid staan?

  In de Algemene verordening gegevensbescherming (AVG) staat niet precies omschreven welke gegevens u in uw gegevensbeschermingsbeleid (ook wel privacybeleid genoemd) moet opnemen. Uit het beleid moet in ieder geval wèl blijken hoe u voldoet aan de AVG. Dat is onderdeel van uw verantwoordingsplicht.

  ## Informatie gegevensbeschermingsbeleid

  U kunt laten zien hoe u voldoet aan de AVG door onder andere deze informatie op te nemen:

    - een omschrijving van de categorieën persoonsgegevens die u verwerkt;
    - een beschrijving van de doeleinden waarvoor u persoonsgegevens verwerkt en wat de juridische grondslag daarvan is;
    - hoe u voldoet aan de beginselen van verwerking van persoonsgegevens. Zoals de verplichting om niet meer gegevens te verwerken dan noodzakelijk;
    - welke rechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen. Zoals het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Maar ook het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens;
    - welke organisatorische en technische maatregelen u genomen heeft om de persoonsgegevens te beveiligen;
    - hoe lang u de persoonsgegevens bewaart.

  Het opstellen van een gegevensbeschermings- of privacybeleid is niet altijd verplicht. Toch kan het nuttig zijn om zo'n beleid wel op te stellen.

- Hoe kan ik aantonen dat ik toestemming heb ontvangen?

  Verwerkt u persoonsgegevens die gebaseerd is op toestemming van de betrokken personen? Dan moet u onder de Algemene verordening gegevensbescherming (AVG) aan de Autoriteit Persoonsgegevens (AP) kunnen laten zien dat u die toestemming daadwerkelijk heeft. Dat maakt onderdeel uit van de verantwoordingsplicht die u onder de AVG heeft.

Specifiek en geïnformeerd

Twee van de eisen die de AVG stelt aan ‘toestemming’ zijn dat deze ‘geïnformeerd’ en ‘specifiek’ gegeven is. Om geldige toestemming aan te tonen is het dan ook essentieel dat u kunt laten zien op basis van welke informatie de betrokken personen de toestemming hebben gegeven. Het is dus onvoldoende om alleen de toestemming zelf vast te leggen.

Online toestemming

Vraagt u online toestemming aan mensen voor het verwerken van hun persoonsgegevens? Dan kunt u de informatie over het websitebezoek, waarin zij de toestemming hebben gegeven, vastleggen. Deze informatie kunt u combineren met:

- documentatie over het proces waarin u heeft vastgelegd op welke manier u toestemming ontvangt en vastlegt.
- een kopie van de informatie die de betrokkenen hebben ontvangen voorafgaand aan de gegeven toestemming.

Verwijzen naar automatische registratie van toestemming door uw website is onvoldoende om geldige toestemming aan te kunnen tonen. De informatie die aan de betrokkenen is verstrekt, ontbreekt dan namelijk.

Ten slotte moet u ervoor zorgen dat u voldoende data heeft waarmee u een link tussen de verwerking én de toestemming van een betrokkene kunt aantonen. Let wel, u mag hierbij niet méér data verzamelen dan strikt noodzakelijk is om geldige toestemming aan te kunnen tonen.

Meer informatie over de verantwoordingsplicht

- Wat moet er volgens de AVG in een gegevensbeschermingsbeleid staan?

In de Algemene verordening gegevensbescherming (AVG) staat niet precies omschreven welke gegevens u in uw gegevensbeschermingsbeleid (ook wel privacybeleid genoemd) moet opnemen. Uit het beleid moet in ieder geval wèl blijken hoe u voldoet aan de AVG. Dat is onderdeel van uw verantwoordingsplicht.

Informatie gegevensbeschermingsbeleid

U kunt laten zien hoe u voldoet aan de AVG door onder andere deze informatie op te nemen:

- een omschrijving van de categorieën persoonsgegevens die u verwerkt;
- een beschrijving van de doeleinden waarvoor u persoonsgegevens verwerkt en wat de juridische grondslag daarvan is;
- hoe u voldoet aan de beginselen van verwerking van persoonsgegevens. Zoals de verplichting om niet meer gegevens te verwerken dan noodzakelijk;
- welke rechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen. Zoals het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens

(AP). Maar ook het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens;
    - welke organisatorische en technische maatregelen u genomen heeft om de persoonsgegevens te beveiligen;
    - hoe lang u de persoonsgegevens bewaart.

Het opstellen van een gegevensbeschermings- of privacybeleid is niet altijd verplicht. Toch kan het nuttig zijn om zo'n beleid wel op te stellen.

- Wanneer is een gegevensbeschermingsbeleid volgens de AVG verplicht?

U bent alleen verplicht om een gegevensbeschermingsbeleid op te stellen als dat in verhouding staat tot uw verwerkingsactiviteiten. Een gegevensbeschermingsbeleid wordt ook wel privacybeleid genoemd. Of u verplicht bent om zo'n privacybeleid op te stellen, hangt af van de concrete omstandigheden. Zoals de aard, de omvang, de context en het doel van de gegevensverwerking.

Ziekenhuizen, gemeenten, social mediabedrijven en handelsinformatiebureaus zullen daarom vaak verplicht zijn om een gegevensbeschermingsbeleid op te stellen. Ook kleine organisaties kunnen verplicht zijn een gegevensbeschermingsbeleid op te stellen.

Vrijwillig opstellen van een gegevensbeschermingsbeleid

Bent u niet verplicht om een gegevensbeschermingsbeleid op te stellen? Dan kan het toch nuttig zijn om dat wél te doen. Het helpt u namelijk om te zien of u voldoende maatregelen heeft genomen om de persoonsgegevens van uw klanten, patiënten, cliënten e.d. te beschermen. Daarnaast is het een manier waarmee u aan zowel uw doelgroep als de Autoriteit Persoonsgegevens kunt laten zien dat u voldoet aan de AVG.

Let op: een gegevensbeschermingsbeleid is iets anders dan een privacyverklaring. Alle organisaties die persoonsgegevens verwerken, moeten mensen heldere informatie geven over de persoonsgegevens die zij verwerken en voor welk(e) doel(en) zij deze gegevens verwerken. De meest aangewezen manier hiervoor is het opstellen van een online privacyverklaring.