PGO support

10 checks voor de privacywet (AVG)

Hulpmiddel voor patiënten- en cliëntenorganisaties om aan de verplichtingen te voldoen van de Europese Algemene Verordening Gegevensbescherming.

PGO support

Inhoud

Inleiding

Sinds 25 mei 2018 is de Europese Algemene verordening gegevensbescherming ("*AVG*") van kracht. In de hele Europese Unie geldt dan dezelfde privacywetgeving.

De AVG:

- legt meer verantwoordelijkheden bij de organisatie die persoonsgegevens verwerkt ("verwerkingsverantwoordelijke")
- beschermt en versterkt de rechten van de personen van wie persoonsgegevens worden verwerkt ("betrokkenen")
- geeft de toezichthouder, de Autoriteit Persoonsgegevens, meer bevoegdheden, waaronder de bevoegdheid om hoge boetes op te leggen.

Patiënten- en cliëntenorganisaties (kortweg: organisaties) gebruiken en registreren persoonsgegevens. Bijvoorbeeld de gegevens van leden en donateurs, van relaties, personeelsleden en vrijwilligers.

Bij een patiënten- of cliëntenorganisatie bevat de administratie naast algemene persoonsgegevens meestal gezondheidsgegevens van de leden. Dit zijn bijzondere gegevens. Aan de verwerking hiervan stelt de AVG strengere eisen.

Gespecialiseerd jurist Linda Eijpe heeft deze brochure op verzoek van PGOsupport samengesteld voor patiënten- en cliëntenorganisaties.

Zij beschrijft 10 checks voor je organisatie om te voldoen aan de AVG.

Belangrijke begrippen

De AVG gebruikt specifieke begrippen. Hieronder lichten we de belangrijkste begrippen toe en geven voorbeelden voor patiënten- en cliëntenorganisaties.

Verwerkingsverantwoordelijke: de organisatie die het doel en de middelen van de verwerking van persoonsgegevens vaststelt. In deze brochure gaan we ervan uit dat de organisatie zelf de verwerkingsverantwoordelijke is.

Verwerker: een externe partij die in opdracht van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt. Voorbeelden zijn: de drukker van het ledenmagazine, het bedrijf dat de ledenadministratie voert of de website host. Maar ook de vrijwilliger die een ledenbestand krijgt om een activiteit te organiseren.

Persoonsgegevens: alle gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon. Bijvoorbeeld naam, adresgegevens, telefoonnummer, e-mailadres of IP-adres.

Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon, bijvoorbeeld de leden, patiënten, maar ook donateurs of vrijwilligers.

Gegevens over gezondheid: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een betrokkene. Gegevens over gezondheid zijn bijzondere persoonsgegevens. Aan de verwerking hiervan stelt de AVG strengere eisen.

Check 1 bewustwording en overzicht van de verwerking

Het is belangrijk dat iedereen binnen je organisatie weet dat de AVG van toepassing is en wat de gevolgen zijn. Van het bestuur (of de directie), personeelszaken tot en met alle medewerkers en vrijwilligers die persoonsgegevens verwerken (bijvoorbeeld gebruiken of kunnen inzien).

We adviseren om één persoon binnen je organisatie of binnen het bestuur aan te wijzen die verantwoordelijk is voor de correcte verwerking van de persoonsgegevens.

Onder de AVG heeft je organisatie een zogenaamde 'verantwoordingsplicht'. Dit houdt in dat jullie altijd moeten kunnen aantonen dat je organisatie handelt in overeenstemming met de AVG.

Documenteer daarom de persoonsgegevens die jullie verwerken. Zo zijn jullie je bewust van de persoonsgegevens die je organisatie verwerkt. En kun je aantonen welke gegevens jullie verwerken en waarom.

DOEN

Breng de verwerking van de persoonsgegevens in kaart door de volgende informatie te verzamelen:

- welke persoonsgegevens verwerken jullie?
  Bijvoorbeeld: naam, adres, bankgegevens, telefoonnummer, geslacht, e-mailadres

- van welke categorieën betrokkenen zijn de persoonsgegevens?
  Bijvoorbeeld: leden, patiënten, donateurs, vrijwilligers, personeelsleden

- verwerken jullie ook gegevens over gezondheid of andere bijzondere persoonsgegevens?
  Bijvoorbeeld: aandoening, medicijngebruik, godsdienst of seksuele leven

- voor welk doel gebruiken jullie de persoonsgegevens?
  Bijvoorbeeld: innen lidmaatschapsgeld, verzenden van informatie, uitnodigingen bijeenkomsten

- vragen jullie toestemming voor de verwerking? Of is er sprake van een andere wettelijke grondslag?

- gebruiken jullie een privacybeleid of hebben jullie andere informatie aan de betrokkenen verstrekt?

- wie hebben er allemaal toegang tot de persoonsgegevens?
  Bijvoorbeeld: welke personeelsleden, vrijwilligers, andere derden (verwerkers)?

- hebben jullie met deze derden/verwerkers een verwerkersovereenkomst gesloten?

- hoe worden de persoonsgegevens beveiligd / is er een beveiligingsbeleid?

- hoelang worden de persoonsgegevens bewaard?

Met deze informatie kunnen jullie inschatten welke stappen de organisatie eventueel nog moet zetten om te voldoen aan de AVG.

TIP 1
De AVG gaat uit van dataminimalisatie. Dit betekent dat organisaties zo min mogelijk persoonsgegevens moeten verwerken en uitsluitend die gegevens die nodig zijn voor het te bereiken doel. Vraag je bij alle te verwerken persoonsgegevens af of deze echt noodzakelijk zijn voor het doel dat jullie nastreven.

TIP 2
De AVG legt extra verplichtingen op aan organisaties die gegevens verwerken over de gezondheid of andere bijzondere persoonsgegevens, zoals over de godsdienst of het seksuele leven. Het onrechtmatig gebruik van dergelijke bijzondere persoonsgegevens kan namelijk een zeer grote impact hebben op de privacy. Het kan er bijvoorbeeld toe leiden dat de betrokkenen gestigmatiseerd worden, geen hypotheek of levensverzekering meer kunnen krijgen of niet worden aangenomen bij een sollicitatie. Indien het niet nodig is om deze bijzondere gegevens te verwerken dan moet een organisatie dat ook niet doen.

Check 2 Functionaris Gegevensbescherming

Onder de AVG is het voor patiënten- en cliëntenorganisaties verplicht om een functionaris voor de gegevensbescherming (FG) te benoemen als de organisatie bijzondere persoonsgegevens verwerkt van meer dan 10.000 mensen.

Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over de gezondheid, godsdienst of het seksuele leven.

Een FG is nodig als de verwerking een kernactiviteit van de organisatie is.

Dat zijn activiteiten die nodig zijn om de doelen van de organisatie te bereiken, of die tot de hoofdtaken van de organisatie horen. Zo is de verwerking van gegevens over de gezondheid van patiënten een kernactiviteit van een ziekenhuis. Datzelfde geldt waarschijnlijk voor de verwerking van de persoonsgegevens en de gegevens over de gezondheid van de leden van patiënten- en cliëntenorganisaties. Deze organisaties moeten deze (persoons)gegevens immers verwerken voor de uitvoering van hun kerntaak: het bieden van diensten en informatie aan de leden/donateurs.

De verwerking van persoonsgegevens die ondersteunend zijn aan de bedrijfsvoering, zoals voor de salarisadministratie, vallen buiten de kernactiviteiten.

Zie voor meer informatie over de richtlijnen voor functionarissen voor de gegevensbescherming de website van de Autoriteit Persoonsgegevens.

Organisatie kunnen ook vrijwillig kiezen voor het aanstellen van een FG. Dit heeft als voordeel dat de FG de organisatie kan adviseren over de verplichtingen uit de AVG en de gevolgen daarvan binnen de eigen organisatie.

DOEN

Maak een interne analyse om te bepalen of je organisatie een Functionaris voor de Gegevensbescherming moet aanstellen. Leg deze analyse vast om aan te kunnen tonen dat jullie rekening hebben gehouden met alle relevante factoren. De Autoriteit Persoonsgegevens kan deze analyse opvragen.

Taken van de functionaris voor de gegevensbescherming (FG)

De FG is een interne toezichthouder. De FG informeert en adviseert over de verplichtingen uit de AVG en ziet toe op de naleving. De FG kan advies verstrekken bijvoorbeeld over de DPIA (zie check 5). De FG is contactpersoon voor de Autoriteit Persoonsgegevens en werkt met de autoriteit samen.

De FG kan iemand van de eigen organisatie zijn, maar mag ook een externe functionaris zijn.
Zie voor meer informatie over de taken van de FG de website van de Autoriteit Persoonsgegevens.

Check 3 rechten van betrokkenen

De AVG geeft betrokkenen meer (privacy)rechten en versterkt deze. Hieronder volgt een opsomming van een aantal rechten van de betrokkenen:

- Het recht op informatie over en inzage in de verwerking van de gegevens van de betrokkene;
- Het recht op correctie of beperking van de persoonsgegevens;
- Het recht om vergeten te worden ('vergetelheid'); de betrokkene heeft het recht om jullie te vragen zijn/haar persoonsgegevens te verwijderen (inclusief het laten verwijderen bij eventuele andere organisaties waaraan jullie de gegevens hebben verstrekt);
- Het recht op dataportabiliteit; betrokkenen kunnen jullie vragen om hun persoonsgegevens in een standaard format te ontvangen en/of door te sturen aan een nieuwe organisatie;
- Het recht om bezwaar te maken tegen profilering en geautomatiseerde besluitvorming.

Een betrokkene kan een klacht indienen bij de Autoriteit Persoonsgegevens over de wijze waarop jouw organisatie met persoonsgegevens omgaat. De Autoriteit Persoonsgegevens is verplicht om deze klacht te behandelen.

DOEN

Check of jouw organisatie kan voldoen aan de rechten van de betrokkenen en richt hiervoor interne processen in. Alle relevante medewerkers moeten zich bewust zijn van de rechten die de betrokkenen hebben en de wijze waarop je organisatie met verzoeken moet omgaan.

Informeer betrokkenen over de rechten die zij hebben en hoe zij daarvan gebruik kunnen maken. Deze informatie moet duidelijk, transparant en toegankelijk zijn. De informatie kan worden opgenomen in het privacybeleid van je organisatie

Pas jullie privacybeleid eventueel aan, met daarin de rechten van de betrokkenen, zodat het voldoet aan de AVG.

Voordat een betrokkene toestemming geeft, moet hij/zij het privacybeleid hebben ontvangen of kunnen inzien en opslaan.

In bijlage 1 vind je een model privacybeleid.

Check 4 aanleggen van register van de gegevensverwerking

De AVG verplicht organisaties om verantwoording af te leggen over de verwerking van persoonsgegevens en aan te tonen dat de organisatie voldoet aan de verplichtingen.

Onderdeel hiervan is de verplichting om een register van de verwerkingsactiviteiten bij te houden indien:

- er meer dan 250 medewerkers werkzaam zijn; of
- er minder dan 250 medewerkers werkzaam zijn, maar er gegevens over gezondheid, godsdienst of seksuele leven worden verwerkt.

Als je organisatie gegevens over de gezondheid verwerkt, zul je een register van de verwerkingsactiviteiten moeten bijhouden. Hoe het register wordt opgezet is vrijgelaten. Wel schrijft de AVG voor welke informatie in het register moet worden opgenomen. Het betreft de volgende informatie:

1. de naam en contactgegevens van:
- de organisatie en de vertegenwoordiger van de organisatie;
- eventuele andere organisaties waarmee gezamenlijk de doelen en middelen van de verwerking zijn vastgesteld;
- de Functionaris voor de gegevensbescherming (FG), als die is aangesteld;
- eventuele andere internationale organisaties waar persoonsgegevens mee worden gedeeld;
2. de doelen waarvoor de persoonsgegevens worden verwerkt. Bijvoorbeeld voor het lidmaatschap, de betaling, het bezorgen van producten of diensten of direct marketing;
3. een beschrijving van de categorieën van personen van wie gegevens worden verwerkt. Bijvoorbeeld leden, vrijwilligers, donateurs;
4. een beschrijving van de categorieën van persoonsgegevens. Zoals de NAW-gegevens, telefoonnummers, e-mailadressen, bankrekeningnummers;
5. de datum waarop de gegevens gewist moeten worden (als dat bekend is) en/of de bewaartermijnen;
6. de categorieën van ontvangers aan wie persoonsgegevens worden verstrekt;
7. als de gegevens met een land of internationale organisatie buiten de EU worden gedeeld, dan moet dit worden aangegeven in het register;
8. een algemene beschrijving van de technische en organisatorische maatregelen die worden genomen om persoonsgegevens die worden verwerkt te beveiligen.

DOEN

Stel een register op met hierboven opgesomde informatie. De Autoriteit Persoonsgegevens kan inzage verlangen in het register. Houd dit register bij en pas het aan indien er veranderingen optreden.

In bijlage 2 vind je een template voor een register gegevensverwerking.

Check 5 Data Protection Impact Assessment (DPIA)

Onder de AVG kan een patiënten- of cliëntenorganisatie verplicht zijn om een DPIA uit te voeren. Met een DPIA breng je vooraf de privacyrisico's van gegevensverwerking in kaart, waarna je maatregelen kunt nemen om de risico's te verkleinen. De DPIA is eigenlijk een instrument om de risico's van schending van de privacyrechten van betrokkenen te beheren.

Een DPIA is verplicht voor gegevensverwerkingen die 'waarschijnlijk een hoog risico' voor de privacyrechten van de betrokkenen hebben. Hiervan is sprake bij verwerking van bijzondere persoonsgegevens, zoals gegevens over gezondheid, godsdienst of seksuele leven van meer dan 10.000 mensen.

De Autoriteit Persoonsgegevens heeft een lijst van verwerkingen gepubliceerd waarvoor een DPIA verplicht is.

Meer informatie hierover is te vinden in de richtsnoeren opgenomen op de website van de Autoriteit Persoonsgegevens:

DOEN

Check of jullie een DPIA moeten uitvoeren. Verwerken jullie bijzondere persoonsgegevens (bijvoorbeeld gegevens over de gezondheid) en is deze verwerking grootschalig? Dan is waarschijnlijk een DPIA nodig.

Besluiten jullie dat de gegevensverwerking waarschijnlijk geen "hoog risico" inhoudt, dan moeten jullie dat goed motiveren en schriftelijk vastleggen, bijvoorbeeld in het onder stap 4 genoemde register.

Uitvoering van een DPIA

De DPIA moet steeds voorafgaand aan de start van de verwerking van de persoonsgegevens worden uitgevoerd. Ook voor bestaande gegevensverwerkingen (gestart voor introductie van de AVG) is het nodig te onderzoeken of een DPIA nodig is.

Verwerkt je organisatie nu al persoonsgegevens of start de organisatie een nieuwe verwerking? Maak dan de afweging of een DPIA nodig is. Is het antwoord ja, dan moet je daarmee starten.

De DPIA moet minimaal aan de volgende kenmerken voldoen:

1. een systematische beschrijving van de beoogde gegevensverwerkingen, de doeleinden en wettelijke grondslagen;
2. een beoordeling van de noodzaak en de evenredigheid van de verwerkingen; Dat houdt in: is het verwerken van persoonsgegevens op deze manier noodzakelijk om het doel van je organisatie te bereiken? Is de inbreuk op de privacy van de betrokkenen niet onevenredig in verhouding tot dit doel?
3. een beoordeling van de privacyrisico's voor de rechten en vrijheden van betrokkenen;

4. de beoogde maatregelen om: (I) de risico's aan te pakken/te verkleinen en (II) aan te tonen dat je organisatie aan de AVG voldoet;
5. De DPIA moet worden vastgelegd in een verslag.

In bijlage 3 vind je een voorbeeld DPIA.

Check 6 toestemming van betrokkenen

Voor sommige gegevensverwerkingen heb je toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Van een rechtsgeldige toestemming is pas sprake indien:

- deze vrijelijk is gegeven,
- gegeven is voor een specifiek doel en bovendien
- gebaseerd is op duidelijke informatie.

Van 'vrijelijk' is sprake als de betrokkene een keuze heeft. Er is bijvoorbeeld geen sprake van 'vrijelijk' als de betrokkene verplicht is om gegevens over zijn gezondheid in te vullen, terwijl hij alleen maar een mailing van je organisatie wil ontvangen.
De gegevens over de gezondheid zijn niet noodzakelijk om de mailing te ontvangen, daarom moet de betrokkene de keuze hebben om deze gegevens te verstrekken.

In alle gevallen moet je kunnen aantonen dat de betrokkene toestemming heeft gegeven.

Indien jullie bijzondere persoonsgegevens verwerken, bijvoorbeeld over de gezondheid, dan geldt bovendien dat de toestemming 'uitdrukkelijk' moet zijn. Dit betekent dat de betrokkene expliciet zijn wil moet hebben geuit in woord, geschrift of gedrag. Een stilzwijgende of impliciete toestemming is daarvoor niet voldoende.

DOEN

Check of de wijze waarop je organisatie toestemming vraagt, krijgt en registreert voldoet aan de AVG. Pas deze desnoods aan.

Zorg ervoor dat de betrokkenen hun toestemming vervolgens ook op een makkelijke manier kunnen intrekken.

Check 7 privacy by design & privacy by default

Organisaties zijn volgens de AVG verplicht om technische en organisatorische maatregelen te nemen om de persoonsgegevens te beveiligen tegen bijvoorbeeld verlies of onrechtmatig gebruik. In de AVG zijn 2 nieuwe verplichtingen geïntroduceerd: privacy by design en privacy by default.

Privacy by design houdt in dat de organisatie bij het ontwerpen van haar producten en diensten zorgt dat de persoonsgegevens goed worden beschermd en dat er zo min mogelijk gegevens worden verwerkt. Dat laatste wil zeggen alleen die gegevens die nodig zijn voor het doel van de verwerking.

Privacy by default houdt in dat de organisatie technische en organisatorische maatregelen moet nemen om te zorgen dat zij in de standaard privacy-instelling (van websites, apps, elektronische formulieren e.d.) alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat zij wil bereiken. Hieronder volgen twee voorbeelden:

1. Indien jullie een online forum aanbieden, dan moet de meest privacyvriendelijke instelling de standaardinstelling zijn. Dat is bijvoorbeeld de instelling waarbij het forumlid anoniem is, zodat andere forumleden niet kunnen zien wie de berichten plaatst. Het forumlid moet dan zelf (bewust) kiezen voor het openbaar maken van zijn of haar persoonsgegevens.

2. Als iemand zich wil aanmelden voor een activiteit of de nieuwsbrief, of geld wil doneren, dan mogen jullie niet méér gegevens vragen dan nodig is voor de uitvoering van aanmelding of de donatie.

DOEN

Check per verwerking welke technische maatregelen jullie kunnen nemen om zo min mogelijk persoonsgegevens te verwerken. Bekijk of er persoonsgegevens vernietigd, geanonimiseerd of versleuteld kunnen worden of beter moeten worden beschermd. Implementeer de maatregelen.

Breng verder per verwerking in kaart of jullie in de standaard privacy-instelling (van bijvoorbeeld jullie website, webtoepassingen of formulieren) alleen die gegevens vragen die echt noodzakelijk zijn voor het specifieke doel. Verwijder de velden voor de niet-noodzakelijke gegevens.

Check 8 meldplicht datalekken

De AVG verplicht datalekken te melden. Alle datalekken moeten in een register worden gedocumenteerd. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of aan de meldplicht is voldaan.

Er is sprake van een datalek als er een beveiligingsincident heeft plaatsgevonden, waarbij persoonsgegevens verloren zijn gegaan en/of waarbij het onrechtmatig gebruik daarvan niet kan worden uitgesloten. Voorbeelden hiervan zijn: kwijtraken van een USB -stick, diefstal van een laptop, inbraak door een hacker.

Het datalek moet direct, binnen 72 uur, gemeld worden aan de autoriteit persoonsgegevens, tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Hierbij is van belang wat voor persoonsgegevens er gelekt zijn. Als er bijzondere persoonsgegevens, zoals gegevens over gezondheid, gelekt zijn, dan is melding meestal noodzakelijk.

Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkene gemeld worden.

DOEN

Het is belangrijk dat de juiste personen binnen je organisatie direct op de hoogte raken van een eventueel datalek en vervolgens de juiste handelingen verrichten. We adviseren hiervoor een protocol op te stellen en in te voeren in de organisatie.

In bijlage 4 vind je een voorbeeldprotocol datalekken.

Leg daarnaast een register aan, waarin eventuele datalekken worden opgenomen. In het register moet je ook vermelden of het datalek is gemeld bij de Autoriteit Persoonsgegevens en de betrokkene(n). Als dit niet gemeld is, moet je aangeven waarom jullie dat niet noodzakelijk vinden. Als het wel gemeld is, moet je dat ook opnemen in het register.

In bijlage 5 vind je een formulier melden datalek.

Check 9 verwerkersovereenkomst

Bijna alle patiënten- en cliëntenorganisaties maken gebruik van zogeheten 'verwerkers'. Dit zijn derden die namens de organisatie persoonsgegevens verwerken. Bijvoorbeeld hostingpartijen, salaris- of ledenadministratie en bedrijven die mailings verzorgen.

Op grond van de AVG is de organisatie verplicht om met deze verwerkers een verwerkersovereenkomst te sluiten waarin de verplichtingen uit de AVG zijn opgenomen.

In bijlage 6 vind je een model verwerkersovereenkomst.

Ook vrijwilligers van de organisatie verwerken soms gegevens van bijvoorbeeld leden/donateurs. Het is daarom belangrijk de vrijwilligersovereenkomst aan te vullen met een bijlage over het verwerken van persoonsgegevens.

In bijlage 7 vind je zo'n vrijwilligersovereenkomst in verband met het verwerken van persoonsgegevens.

Lees ook ons artikel met 9 veelgestelde vragen over de verwerkersovereenkomst.

DOEN

Check met welke verwerkers jullie samenwerken en beoordeel of de huidige overeenkomsten voldoen aan de AVG.

Sluit met deze verwerkers een verwerkersovereenkomst.

Bijlage 6 model verwerkersovereenkomst.

Check 10 toezichthouder

De AVG stelt dat een organisatie maar met één toezichthouder te maken heeft, de 'leidende toezichthouder'. Dit is van belang voor organisaties die meerdere vestigingen in Europa hebben.

De leidende toezichthouder is in principe de toezichthouder van de EU-lidstaat waar de hoofdvestiging van een organisatie zich bevindt. Deze is als eerste verantwoordelijk voor het toezicht op organisaties met grensoverschrijdende gegevensverwerkingen.

Als de hoofdvestiging in Nederland is, dan is de Nederlandse Autoriteit Persoonsgegevens de 'leidende toezichthouder'.

DOEN

Bevindt je organisatie zich in Nederland? Dan treedt de Nederlandse Autoriteit Persoonsgegevens op als privacy-toezichthouder.

Meer weten over de AVG?

Heb je na het lezen van deze brochure nog vragen over AVG in het algemeen? Of over de acties die jullie moeten ondernemen om aan de privacywetgeving te blijven voldoen? Neem gerust contact op. Martine Versluijs helpt je graag verder.