AVG E-book

Titel: Alles wat je moet weten over de AVG

fgonline.nl

Inhoudsopgave

1. Inleiding

Welkom bij deze handleiding over de Algemene Verordening Gegevensbescherming (AVG). Het boek is gratis en bedoeld om je op weg te helpen.

2. Wat is de AVG?

De AVG is een Europese wetgeving die is ontworpen om de privacy en bescherming van persoonsgegevens te waarborgen. Het is van toepassing op alle organisaties die persoonsgegevens van Europese burgers verzamelen, verwerken of opslaan. De AVG legt verplichtingen op aan deze organisaties en geeft individuen meer controle over hun eigen gegevens.

3. Belangrijke begrippen

- Persoonsgegevens: In de Algemene Verordening Gegevensbescherming (AVG) wordt persoonsgegevens gedefinieerd als ‘alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon’. Dit betekent dat informatie direct over iemand kan gaan of informatie die, alleen of in combinatie met andere gegevens, naar die persoon te herleiden is.
- Verwerking: Elke handeling of reeks handelingen met betrekking tot persoonsgegevens, zoals verzamelen, opslaan, gebruiken, etc.
- Verwerkingsverantwoordelijke: De persoon of organisatie die bepaalt hoe en waarom persoonsgegevens worden verwerkt.
- Verwerker: De persoon of organisatie die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke.

4. Welke organisaties moeten voldoen aan de AVG?

Iedere organisatie die persoonsgegevens van EU-burgers verwerkt, moet voldoen aan de AVG. Dit geldt zowel voor bedrijven als voor non-profitorganisaties en overheidsinstellingen.

5. Rechten van betrokkenen

De AVG verleent individuen verschillende rechten met betrekking tot hun persoonsgegevens:

- Recht op informatie: personen hebben het recht om te weten wat je met hun persoonsgegevens doet en waarom.
- Recht op inzage: personen hebben het recht om te weten welke gegevens over hen worden verzameld en verwerkt.
- Recht op rectificatie: personen kunnen onjuiste gegevens laten corrigeren.
- Recht op wissen: personen kunnen verzoeken om verwijdering van hun gegevens.
- Recht op beperking van verwerking: personen kunnen vragen om de verwerking van hun gegevens te beperken.
- Recht op dataportabiliteit: personen kunnen hun gegevens in een gestructureerd, gangbaar formaat ontvangen.

- Recht van bezwaar: personen kunnen bezwaar maken tegen de verwerking van hun gegevens.
- Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming: personen hebben volgens artikel 22 lid 1 AVG het recht om niet te worden onderworpen aan besluiten van gegevensverwerkende organisaties die uitsluitend berusten op geautomatiseerde verwerking (waaronder profilering).

6. Verantwoordelijkheden van organisaties

Organisaties moeten zorgen voor:

- Juridische basis voor verwerking: zorg ervoor dat je gegevens verwerkt op basis van een geldige juridische grondslag, zoals toestemming, contractuele noodzaak of wettelijke verplichting.
- Privacyverklaring: sinds de invoering van de AVG is iedere ondernemer verplicht informatie te delen over hoe hij omgaat met persoonsgegevens. Een privacyverklaring moet aan een aantal regels voldoen. Zo moet het helder en begrijpelijk zijn opgeschreven. Op die manier is het voor betrokkenen duidelijk wat er met hun persoonsgegevens gebeurt. Ook moet de privacyverklaring altijd makkelijk te vinden zijn op de website van de organisatie. Een link naar de verklaring moet bijvoorbeeld in de footer van de website staan. Verder moet je als organisatie de verklaring regelmatig updaten.
- Data protection by design and by default: zorg ervoor dat gegevensbescherming is ingebouwd in de processen en systemen van je organisatie.

7. Hoe maak je je organisatie AVG-klaar?

Om je organisatie AVG-klaar te maken, doorloop je de volgende stappen:

- Gegevensinventarisatie: begin met het identificeren en in kaart brengen van alle persoonsgegevens die je verzamelt, verwerkt en opslaat. Dit omvat het begrijpen van waar de gegevens vandaan komen, hoe ze worden gebruikt en wie toegang heeft tot deze gegevens.
- Juridische basis: zorg ervoor dat je voor elke verwerking van persoonsgegevens een geldige juridische basis hebt. Dit kan toestemming zijn, een contractuele noodzaak, een wettelijke verplichting, of gerechtvaardigd belang.
- Verwerkingsregister: stel een verwerkingsregister op waarin je alle verwerkingen van persoonsgegevens documenteert. Dit register moet informatie bevatten over de verwerkingsdoeleinden, de categorieën van persoonsgegevens, de ontvangers, de bewaartermijnen en de technische en organisatorische maatregelen ter bescherming van de gegevens.
- Privacyverklaring: ontwikkel en publiceer een duidelijke privacyverklaring waarin je uitlegt hoe je persoonsgegevens verzamelt, gebruikt en beschermt. De privacyverklaring moet makkelijk te vinden zijn op de website van je organisatie.
- Beoordeel of je verplicht bent een Functionaris Gegevensbescherming (FG) aan te stellen.

- Verwerkingsovereenkomsten: zorg ervoor dat je verwerkingsovereenkomsten hebt met alle derden die persoonsgegevens verwerken namens jouw organisatie. Deze overeenkomsten moeten specificeren hoe de gegevens moeten worden beschermd en de verantwoordelijkheden van beide partijen vastleggen.
- Data Protection Impact Assessments (DPIA): voer DPIA's uit voor verwerkingen die een hoog risico kunnen inhouden voor de rechten en vrijheden van betrokkenen. Dit helpt bij het identificeren en mitigeren van mogelijke privacyrisico's.
- Medewerkerstraining: zorg ervoor dat je medewerkers goed zijn opgeleid over de AVG en hun verantwoordelijkheden bij de verwerking van persoonsgegevens. Regelmatige training helpt bij het voorkomen van fouten en het bevorderen van een cultuur van gegevensbescherming binnen je organisatie.
- Procedures en beleid: ontwikkel en implementeer procedures voor het omgaan met verzoeken van betrokkenen, datalekken en andere AVG-gerelateerde kwesties. Dit omvat processen voor het bijhouden van datalekken en het beantwoorden van verzoeken om inzage of verwijdering van persoonsgegevens.
- Beveiligingsmaatregelen: implementeer technische en organisatorische maatregelen om persoonsgegevens te beschermen. Dit kan encryptie, toegangspolicies, en fysieke beveiligingsmaatregelen omvatten.

8. Verwerkingsregisters

Elke organisatie die structureel persoonsgegevens verwerkt, is verplicht een verwerkingsregister bij te houden. Slechts zelden is een organisatie vrijgesteld van deze verplichting, aangezien vrijwel iedere organisatie op regelmatige basis persoonsgegevens verwerkt. Het verwerken van personeels- of klantgegevens wordt bijvoorbeeld al beschouwd als een structurele verwerking.

Wat staat er in een verwerkingsregister?

Zowel een verwerkingsverantwoordelijke als een verwerker moet een verwerkingsregister bijhouden. Wat er in het register staat is afhankelijk van de rol die een organisatie heeft.

Bij de verwerkingsverantwoordelijke bevat het verwerkingsregister de volgende informatie:

- naam en contactgegevens van de verwerkingsverantwoordelijke, en van de functionaris gegevensbescherming (indien aanwezig)
- verwerkingsdoeleinden
- categorieën betrokkenen (bijvoorbeeld klanten, websitebezoekers en medewerkers)
- categorieën persoonsgegevens (bijvoorbeeld NAW-gegevens, contactgegevens, financiële gegevens)
- categorieën ontvangers (bijvoorbeeld ICT-dienstverleners)
- informatie over eventuele doorgifte van persoonsgegevens naar een derde land
- bewaartermijnen
- beveiligingsmaatregelen

Bij de verwerker is het register georganiseerd per verwerkingsverantwoordelijke. Verwerkers nemen de volgende informatie op in het verwerkingsregister:

- naam en contactgegevens van de verwerker en de verwerkingsverantwoordelijke, en de functionaris gegevensbescherming (indien aanwezig)
- categorieën verwerkingen
- informatie over eventuele doorgifte van persoonsgegevens naar een derde land
- beveiligingsmaatregelen

9. Verwerkingsovereenkomsten

In een verwerkersovereenkomst maken partijen afspraken over de omgang met persoonsgegevens. Het uitgangspunt is dat de verwerkingsverantwoordelijke bepaalt wat er met de persoonsgegevens gebeurt. De verwerker mag de gegevens alleen in opdracht van de verwerkingsverantwoordelijke verwerken. Beide partijen zijn wettelijk verplicht om hier afspraken over te maken. Een verwerkingsovereenkomst moet afspraken bevatten over:

- Persoonsgegevens en doeleinden
- Subverwerkers
- Doorgifte van persoonsgegevens
- Beveiligingsmaatregelen
- Datalekken
- Audits
- Verzoeken van betrokkenen
- Verwijdering of vernietiging van persoonsgegevens

10. Wanneer is een Functionaris Gegevensbescherming (FG) verplicht?

Een Functionaris Gegevensbescherming (FG) is verplicht in de volgende gevallen:

- Overheidsinstanties en publieke organisaties. Voor deze organisaties is een FG altijd verplicht, ongeacht het type persoonsgegevens dat ze verwerken. Het kan gaan om de rijksoverheid, gemeenten en provincies, maar ook om bijvoorbeeld zorg- en onderwijsinstellingen.
- Organisaties die op grote schaal individuen volgen of hun activiteiten in kaart brengen. Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen, cameratoezicht, personeelsvolgsystemen en monitoring van iemands gezondheid via wearables.
- Organisaties die op grote schaal bijzondere persoonsgegevens verwerken. Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands gezondheid, ras/etniciteit, politieke opvatting of geloofsovertuiging.
- Organisaties die strafrechtelijke persoonsgegevens verwerken.

In andere gevallen is het niet verplicht om een FG aan te stellen, maar kan het toch nuttig zijn, afhankelijk van de aard en omvang van de gegevensverwerkingen binnen de organisatie.

11. Data Protection Impact Assessments (DPIA)

De AVG geeft aan dat je in ieder geval een DPIA moet uitvoeren als je als organisatie:

- Systematisch en uitgebreid persoonlijke aspecten van mensen beoordeelt. Dit doet u op basis van geautomatiseerde verwerking van persoonsgegevens.
- Op grote schaal bijzondere persoonsgegevens verwerkt.
- Strafrechtelijke gegevens verwerkt.
- Op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied. Bijvoorbeeld met cameratoezicht.

12. Hoe ga je om met datalekken?

Volgens de AVG ben je verplicht een datalekregister op te stellen en bij te houden. Hierin houd je bij welke datalekken er in je organisatie zijn geweest. In het register moet je alle datalekken vastleggen die zich binnen je organisatie hebben afgespeeld. Ook de datalekken die je niet aan de AP hebt gemeld.

Het doel van het datalekregister is dat je als organisatie:

- Leert van eerdere datalekken en bewust bent van datalekken die in het verleden hebben plaatsgevonden.
- Effectieve maatregelen neemt om de kans op nieuwe, soortgelijke datalekken te verminderen.
- Met een datalekregister aan de AP kunt laten zien dat je voldoet aan de meldplicht datalekken.

<u>Het melden van datalekken:</u>

- De Autoriteit Persoonsgegevens: informeer de AP over het datalek als het waarschijnlijk een risico voor de rechten en vrijheden van betrokkenen met zich meebrengt. De melding aan de Autoriteit Persoonsgegevens moet plaatsvinden binnen 72 uur na ontdekking.
- De betrokkenen waarvan de data is gelekt: informeer de betrokkenen als het datalek waarschijnlijk een hoog risico voor hun rechten en vrijheden met zich meebrengt.

13. Handhaving en boetes

De AVG kent strikte handhavingsmechanismen en kan aanzienlijke boetes opleggen voor niet-naleving. Boetes kunnen oplopen tot 20 miljoen euro of 4% van de jaarlijkse wereldwijde omzet, afhankelijk van wat het hoogste is.

14. Wat zijn normale, gevoelige en bijzondere persoonsgegevens?

In de context van de AVG worden persoonsgegevens ingedeeld in drie categorieën: normale persoonsgegevens, gevoelige persoonsgegevens, en bijzondere persoonsgegevens.

15. Normale persoonsgegevens

Normale persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon, maar die niet als bijzonder gevoelig worden beschouwd.

- Naam
- Adres
- Telefoonnummer
- E-mailadres
- Geboortedatum
- Geslacht

Bescherming: Hoewel normale persoonsgegevens een lager risico voor de privacy van betrokkenen met zich meebrengen dan bijzondere persoonsgegevens, moeten ze nog steeds adequaat worden beschermd tegen ongeoorloofde toegang, verlies of verwerking. Organisaties moeten zorgen voor een goede beveiliging en zorgvuldig omgaan met deze gegevens, volgens de vereisten van de AVG.

16.Gevoelige persoonsgegevens

Voor het verwerken van deze persoonsgegevens is het belangrijk dat er extra waarborgen worden getroffen omdat er misbruik van kan worden gemaakt.

- Financiële gegevens, zoals je inkomen
- Locatiegegevens
- Informatie over kinderen of andere kwetsbare groepen
- Strafrechtelijke gegevens (Zie hoofdstuk 20)
- BSN (Zie hoofdstuk 21)

17. Bijzondere persoonsgegevens

Bijzondere persoonsgegevens omvatten de meest gevoelige categorieën van gegevens en vereisen de hoogste mate van bescherming. De AVG stelt strenge voorwaarden aan de verwerking van deze gegevens om de privacy van betrokkenen te waarborgen.

- Gezondheidsgegevens
- Gegevens over ras of etnische afkomst
- Politieke opvattingen
- Religieuze of levensbeschouwelijke overtuigingen
- Lidmaatschap van een vakbond
- Genetische gegevens
- Seksuele geaardheid

Organisaties moeten de hoogste beveiligingsmaatregelen en zorgvuldigheid hanteren bij het verwerken van deze gegevens.

18. Verwerkingsgrondslagen voor normale en gevoelige persoonsgegevens

De AVG vereist dat je een geldige grondslag hebt voor het verwerken van normale en gevoelige persoonsgegevens. Deze grondslagen zijn de basis waarop je gegevensverwerkingen kunt rechtvaardigen. Hier zijn de zes hoofdgrondslagen:

1. Je hebt toestemming van de persoon om wie het gaat.
2. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
3. Het is noodzakelijk om gegevens te verwerken omdat je dit wettelijk verplicht bent.
4. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
5. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang uit te voeren / openbaar gezag uit te oefenen.
6. Het is noodzakelijk om gegevens te verwerken om een gerechtvaardigde belang te behartigen.

19. Verwerken van bijzondere persoonsgegevens

De verwerking van bijzondere persoonsgegevens is verboden. Tenzij er een beroep kan worden gedaan op een uitzondering. In de AVG staan 10 uitzonderingen. Daarnaast moet je een van de 6 grondslagen voor het verwerken van 'gewone' persoonsgegevens hebben.

In de praktijk vallen sommige van die uitzonderingen en grondslagen samen. Bijvoorbeeld als je uitdrukkelijke toestemming hebt gekregen van de betrokkene.

Van de 10 uitzonderingen uit de AVG zijn er 5 die alleen van toepassing zijn als hiervoor in de nationale wet een rechtsbasis is gecreëerd. Dat betekent dat er alleen op zo'n uitzondering beroep mag worden gedaan als er in een Nederlandse wet staat dat dit mag.

De 10 uitzonderingen zijn:

1. Iemand heeft uitdrukkelijke toestemming gegeven voor de verwerking van de eigen persoonsgegevens.
2. Alleen als het in een wet staat: De verwerking is noodzakelijk om verplichtingen uit te voeren of specifieke rechten uit te oefenen van u of de betrokken persoon. Dit op het gebied van het arbeidsrecht, het socialezekerheidsrecht of het socialebeschermingsrecht.
3. De verwerking is noodzakelijk om de vitale belangen van de betrokken persoon of van een andere natuurlijke persoon te beschermen. Dit geldt alleen wanneer diegene fysiek of juridisch niet in staat is om toestemming te geven.
4. Je verwerkt de persoonsgegevens als stichting, vereniging of andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is. Het gaat om persoonsgegevens van uw (oud-)leden of personen met wie je regelmatig contact heeft, gerelateerd aan de doelstelling. En je verwerkt de gegevens voor gerechtvaardigde activiteiten en met passende waarborgen.
5. Je verwerkt persoonsgegevens die de betrokken persoon zelf doelbewust openbaar heeft gemaakt.

6. De verwerking is noodzakelijk om een rechtsvordering in te stellen, uit te oefenen of te onderbouwen.
7. Alleen als het in een wet staat: De verwerking is noodzakelijk voor een zwaarwegend algemeen belang.
8. Alleen als het in een wet staat: De verwerking is noodzakelijk voor doeleinden van preventieve of (arbeids)geneeskundige aard. Zoals het beoordelen van arbeidsgeschiktheid en/of het verstrekken van gezondheidszorg.
9. Alleen als het in een wet staat: De verwerking is noodzakelijk voor de volksgezondheid.
10. Alleen als het in een wet staat: De verwerking is noodzakelijk voor archivering in het algemeen belang, wetenschappelijk/historisch onderzoek of statistische doeleinden.

20. Speciale regels voor strafrechtelijke gegevens

De verwerking van strafrechtelijke gegevens (AVG: 'persoonsgegevens van strafrechtelijke aard') is verboden. Tenzij je kunt beroepen op een specifieke wettelijke uitzondering én op een van de grondslagen voor het verwerken van 'gewone' persoonsgegevens.

Dit zijn de 2 belangrijkste wettelijke uitzonderingen voor het verwerken van strafrechtelijke persoonsgegevens:

- De verwerking geschiedt onder verantwoordelijkheid van de overheid.
- De verwerking is toegestaan bij wetgeving die ook passende waarborgen biedt voor de rechten en vrijheden van de betrokken personen.

21. Speciale regels voor het burgerservicenummer (BSN)

Het BSN is een uniek persoonsnummer dat in de eerste plaats bedoeld is voor het contact tussen burgers en de overheid. Organisaties buiten de overheid mogen het BSN alleen gebruiken als dat wettelijk is bepaald. Dit geldt bijvoorbeeld voor organisaties in de zorg en het onderwijs. Staat het niet in de wet, dan mag het niet. Ook niet met toestemming.

Deze handleiding biedt een uitgebreid overzicht van de AVG en praktische stappen om je organisatie AVG-klaar te maken. Door deze richtlijnen te volgen, kun je zorgen voor een effectieve naleving van de AVG en bijdragen aan de bescherming van persoonsgegevens. Als je verder hulp nodig hebt, aarzel dan niet om contact op te nemen.
