DMCC

STAPPENPLAN

In 10 stappen naar AVG compliance

2023

De AVG

In mei 2018 is de huidige Europese privacywetgeving (Algemene Verordening Gegevensbescherming oftewel de AVG) in werking getreden.

Heeft uw organisatie een database met gegevens van klanten, donateurs, leden, prospects of frequente bezoekers? Gebruikt u deze gegevens in uw bestand om hen op de hoogte te houden van uw activiteiten, acties of voorstellingen? Verstuurt u een e-mailnieuwsbrief of heeft uw organisatie een Facebookpagina of Twitteraccount? Dan verwerkt u persoonsgegevens en moet u zich aan de wet- en regelgeving houden met betrekking tot de bescherming van persoonsgegevens.

Het concept van verantwoording vormt de basis van de AVG. Organisaties moeten kunnen aantonen dat zij begrijpen hoe de vereisten van de AVG impact hebben op hun verwerkingen van persoonsgegevens. Ook moeten zij de juiste beheersmaatregelen treffen om compliance te waarborgen. Vergelijkbaar met de handelingen die we kennen bij financiële verslaglegging van organisaties.

Dit stappenplan geeft een overzicht van de belangrijkste privacy compliance vereisten en vertelt stapsgewijs hoe organisaties deze op een praktische manier kunnen implementeren.

Heeft u nog andere vragen over de AVG? Raadpleeg dan de kennisbank op onze website of stel uw vraag via info@dmcc.nl

Stap 1. Inventariseer welke gegevens u verzamelt (heeft u deze ook echt nodig?)

Organisaties willen (potentiële) klanten kennen om hen beter van dienst te zijn. Dus mogen zij van de nieuwe privacywet klant- en contacthistorie bijhouden. Dit betekent niet dat u vrijuit data mag verzamelen. Organisaties mogen data verzamelen, maar alleen op proportionele wijze voor het doel waarmee ze die gegevens verzamelen. Daarom mogen hotels bijvoorbeeld in principe geen kopie van het paspoort opslaan en moet een goed doel zich afvragen wanneer een donateur vertelt over zijn zieke moeder of dit gegeven bijdraagt aan het verbeteren van de dienstverlening.

Dit geldt in grote mate voor het vastleggen van aandoeningen, ziektes, pijntjes en psychische problemen. Legt uw organisatie bij telemarketing vast dat iemand doof is of handelingsonbekwaam? Realiseert u zich dan dat dit bijzondere persoonsgegevens zijn, die een organisatie eigenlijk niet mag verzamelen zonder expliciete toestemming. Als zonder bepaalde gegevens dezelfde dienst kan worden verleend, mogen ze niet vastgelegd worden. Het is duidelijk dat in allerlei gevallen verschillende interpretaties mogelijk zijn. Het is daarom zaak om de medewerkers in kwestie goede instructies te geven en te zorgen dat hun kennis bijvoorbeeld door cursussen en trainingen op niveau blijven. Dergelijk beleid laat ook zien dat een bedrijf proactief streeft naar compliance.

AVG: artikel 6 t/m 10
Rechtmatige verwerkingsgronden en toestemming

> **In het kort:** de AVG vereist dat organisaties een rechtmatige grondslag hebben voor de verwerking, zoals bijvoorbeeld het uitvoeren van een overeenkomst, het bijhouden van een (leden)administratie of het uitvoeren van marketingactiviteiten. Voor sommige verwerkingen, denk aan online marketing, mogen gegevens alleen verzameld worden met toestemming.

Organisaties moeten voor iedere verwerking nagaan:
- Wat de grondslag voor de gegevensverwerking is (uitvoering overeenkomst/ marketing/analyse);
- Of de gegevensverzameling proportioneel is voor het doel;
- Hoe lang de gegevens bewaard moeten worden;
- Of toestemming nodig is voor de verwerking en of die duidelijk gevraagd wordt op registratiepagina's;
- Of toestemming aangetoond kan worden (d.m.v. bijvoorbeeld een timestamp en versiebeheer van privacy statements en/of algemene voorwaarden).

Stap 2. Documenteer uw verwerkingen

De AVG verplicht organisaties tot het bijhouden van een zogenaamd verwerkingenregister. Dit is in feite een privacy administratie vergelijkbaar met een financiële administratie. Er moet een overzicht komen van welke data, via welke bronnen, in welke systemen worden verzameld, wie hierbij kan en hoe de beveiliging is ingericht. Daarnaast moeten organisaties aangeven welke leveranciers in opdracht data verwerken. Denk hierbij bijvoorbeeld aan een administratiekantoor of de externe IT leverancier. Deze documentatieplicht blijkt in de praktijk een van de moeilijkste vereisten om in te vullen.

Data is de rode draad binnen organisaties waardoor organisaties in toenemende mate gebruik maken van gespecialiseerde leveranciers, die allemaal data vastleggen, verwerken en opslaan. Iedere organisatie met een klant of ledenbestand heeft bijvoorbeeld een CRM systeem, een emailsysteem, een order management systeem, een CMS systeem, actiepagina's en petitiesites, fora, WhatsApp en Messengerdiensten. Vaak corresponderen de systemen niet met elkaar en wordt gewerkt met import en exports, die worden uitgevoerd of verwerkt door verschillende afdelingen of verwerkers. Het kan snel veranderen in een data spaghetti van verwerkingen waardoor er een actueel en compleet overzicht van systemen moet zijn, oftewel een systeem architectuur plaat.

AVG: artikel 30
Verwerkingenregister

In het kort: de verantwoordelijke (database eigenaar) moet een verwerkingenregister bijhouden. Ook de verwerkers (bijvoorbeeld een IT leverancier) moet bijhouden in opdracht van welke organisaties hij welke gegevens verwerkt. Voor het opzetten van dit register is geen vormvereiste gesteld. Dat betekent dat uw organisatie zelf het format mag bepalen van het register. Uiteraard moet het wel goed opgezet worden, overzichtelijk zijn voor interne gebruikers en actueel worden bijgehouden.

Organisaties moeten:

- Identificeren waar en door wie binnen en buiten de organisatie persoonsgegevens worden verwerkt;
- Bepalen op welke wijze (welk type register) zij de details van de verwerkingen in kaart gaat brengen en wat hierin staat opgenomen. Hierbij kunt u denken aan:
  - Naam en adresgegevens van de verantwoordelijken en de eventuele privacy of Functionaris Gegevensbescherming (FG);
  - Doeleinden van de verwerking;
  - Omschrijving van de (categorieën) persoonsgegevens en betrokkenen;
  - Omschrijving van de (categorieën) ontvangers;
  - Omschrijving en naam van verwerkers eventueel met link naar de verwerkersovereenkomst;

    - Het systeem of de applicatie waarin de persoonsgegevens opgeslagen zijn;
    - Of gegevens buiten de EU worden verwerkt;
    - Bewaartermijnen;
    - Generieke omschrijving van technische en organisatorische maatregelen die zijn genomen om data te beveiligen.
- Nagaan op welke wijze het register actueel wordt gehouden. Wordt de verantwoordelijkheid decentraal belegd bij de proceseigenaren of juist centraal bij een privacy officer of FG.

Stap 3. Beheer en controleer uw verwerkingen

In de privacywet staat dat organisaties die op grote schaal mensen monitoren of die bijzondere persoonsgegevens verwerken verplicht een Functionaris Gegevensbescherming (FG) moeten aanstellen. Bijzondere persoonsgegevens zijn gegevens die kunnen leiden tot discriminatie of uitsluiting, zoals informatie over levensovertuiging, seksuele voorkeur, ras of gezondheid. De FG heeft een onafhankelijke advies functie.

Ook als bovenstaande niet op de verwerking van toepassing is, moet een organisatie privacy bij een afdeling of persoon zoals de privacy officer beleggen. Het principe van accountability betekent dat organisaties grip moeten hebben op hun verwerkingen. En als privacy ieders verantwoordelijkheid is, blijkt in de praktijk vaak dat niemand zich verantwoordelijk voelt. Het kan goed zijn dat met de wijze waarop uw organisatie persoonsgegevens verwerkt een fulltime FG of privacy oficer niet vereist is, maar dat u wel privacy expertise nodig heeft. U mag deze dan ook extern betrekken.

AVG: artikel 24, 37, 38 & 39
Verantwoordelijkheid van de verwerkingsverantwoordelijke

> **In het kort:** organisaties moeten een Functionaris Gegevensbescherming (FG) aanstellen indien zij op grote schaal mensen monitoren of bijzondere persoonsgegevens verwerken. De FG rapporteert aan de directie en moet een mandaat hebben om zijn functie onafhankelijk uit te kunnen voeren. Zijn contactgegevens worden doorgegeven aan de Autoriteit Persoonsgegevens (AP) en de FG treedt op als vertegenwoordiger van de organisatie bij eventuele verzoeken.

Organisaties moeten:
- Bepalen of zij voor hun verwerkingen verplicht zijn een FG aan te stellen;
- Bepalen welke mandaat deze persoon heeft en welke middelen tot zijn beschikking moeten staan bij het uitoefenen van zijn taak;
- De contactdetails doorgeven aan de Autoriteit Persoonsgegevens.

Stap 4. Delegeer bewust aan verwerkers

Grip op verwerkingen betekent ook zicht en controle op eventuele verwerkers die uw organisatie inschakelt. Allereerst door het sluiten van een verwerkersovereenkomst. Dat is allang niet zomaar een paragraaf in de opdrachtovereenkomst, maar een volwaardig document met informatie over de opdracht, het type gegevens, bewaartermijnen en beveiligingsmaatregelen.

Ten tweede, controleer de verwerking bij de verwerkers door bijvoorbeeld periodiek beveiligingsrapporten op te vragen of door een derde partij te vragen om de afspraken in de verwerkersovereenkomst op locatie te controleren. Het zal duidelijk zijn dat dit een grotere klus gaat worden naarmate er meer verwerkers zijn.

AVG: artikel 28, 37, 82 & 83
Verwerkers

In het kort: verwerkers (leveranciers) hebben ook een aantal zelfstandige verplichtingen op basis van de AVG. Zo moeten zij data adequaat beveiligen, mogen zij niet zonder meer sub-verwerkers inschakelen zonder toestemming van de verantwoordelijke en moeten zij een datalek zo snel mogelijk melden aan de verantwoordelijke. Daarnaast hebben zij ook de plicht om zelfstandig mee te werken aan verzoeken van de privacy toezichthouder. Deze afspraken over de verwerkingen moeten worden vastgelegd in een verwerkersovereenkomst.

Organisaties moeten:

- Verwerkersovereenkomsten afsluiten met hun leveranciers met daarin:
  - Een duidelijke opdrachtomschrijving;
  - De doeleinden van de verwerking;
  - Een omschrijving van de (categorieën) data die verwerkt worden;
  - Geheimhouding;
  - Inschakelen van derden en onderaannemers;
  - Locatie van de data;
  - Afhandeling van verzoeken van de betrokkene (recht op inzage, correctie en verzet en het recht om vergeten te worden);
  - Duur van de overeenkomst en wijze van beëindiging;
  - De termijnen waarbinnen de verwerker de data mag bewaren;
  - Dat persoonsgegevens moeten worden vernietigd;
  - Een omschrijving van de door de verwerker te hanteren beveiligingsmaatregelen;
  - Instructie met betrekking tot datalekken;
  - Een mogelijkheid tot controle (audit) van naleving van de overeenkomst door de verantwoordelijke;
  - Aansprakelijkheid;
  - Recht op heronderhandeling van de overeenkomst;
  - Toepasselijk recht.

Stap 5. Informeer de personen in uw bestand

Het uitgangspunt van de privacywet is dat organisaties gegevens van personen mogen verzamelen mits er aan voorwaarden wordt voldaan. De belangrijkste voorwaarde is dat mensen van wie de gegevens worden verzameld hier begrijpelijk over worden geïnformeerd en dat hen een keuze wordt geboden over wat er met die gegevens mag worden gedaan. Het volstaat niet om die informatie te geven met een linkje naar uw algemene voorwaarden of uw privacy statement. Organisaties moeten op de registratiepagina's in een bij- of onderschrift melden waarvoor zij gegevens verzamelen om te voldoen aan de informatieplicht.

Kijk bijvoorbeeld eens naar de informatie onderaan de donatieknop op de donatiepagina van WNF "hoe gaat WWF om met je gegevens". De aanvullende informatie over de verwerking staat vervolgens in een privacy statement. Het is belangrijk dat het statement eenvoudig toegankelijk is via de website zoals via de footer en op alle formulieren waar gegevens worden gevraagd. Het taalgebruik moet ook begrijpelijk zijn en aansluiten bij de gemiddelde doelgroep. Ooit gezien hoe Coolblue dit doet?

AVG: artikel 12 t/m 14
Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene

In het kort: organisaties moeten de mensen wiens gegevens zij verwerken (betrokkenen) ten tijde van de registratie zo volledig mogelijk informeren over de verwerking. Dus welke gegevens slaan zij voor welke doeleinden op. De AVG verplicht ook dat organisaties vertellen hoe lang zij data opslaan en op basis van welke grondslag zij gegevens verwerken. Indien gegevens verrijkt worden moet uw organisatie vertellen met welke informatie dan wordt verrijkt. Verder moet de betrokkene geïnformeerd worden over zijn recht op inzage, correctie en verzet. Al deze informatie moet eenvoudig toegankelijk en begrijpelijk zijn.

Organisaties moeten:
- Beoordelen of een privacy statement leesbaar is en de informatie geeft die de AVG vereist.
- Beoordelen of het privacy statement voldoende toegankelijk is. Staat er bijvoorbeeld een link naar het privacy statement bij alle online registratiepagina's en is privacy apart benoemd in de webpagina footer.

Stap 6. Bescherm en beveilig uw gegevens

Organisaties verzamelen veel gegevens waardoor het ook enorm van belang is om deze gegevens goed te beschermen tegen kwaadwillende personen. Cyberaanvallen komen steeds vaker voor. Deze cyberaanvallen zorgen voor een flinke impact op de bedrijfsvoering met het risico op imagoschade, data verlies, financiële kosten en boetes. Een goede beveiliging is essentieel om criminelen buiten de deur te houden en het vertrouwen van het publiek en personeel te waarborgen. Volgens de AVG dienen bedrijven passende technische en organisatorische maatregelen te nemen zoals encryptie, monitoring, toegangsbeveiliging en twee-factorauthenticatie.

Mocht het toch zover komen, dan dient u binnen 72 uur na het ontdekken van een datalek hiervan melding te doen. Deze wordt gemeld bij de Autoriteit Persoonsgegevens als het lek (kans op) ernstige nadelige gevolgen heeft voor de privacy van de betrokkenen en wordt ook gemeld aan de betrokkenen zelf. Naast een meldplicht is er ook een protocolplicht. De protocolplicht houdt in dat organisaties een overzicht moeten bijhouden van alle data incidenten die zijn ontdekt, met daarbij de overweging of deze wel of niet gemeld zijn bij de AP en/of bij de betrokkenen. Dit wordt ook wel een incidentregister genoemd. Met dit incidentregister kunt u monitoren en passende maatregelen nemen met als doel datalekken te voorkomen.

AVG: artikel 25, 32, 33 & 34
Technische en organisatorische maatregelen. Meldings- en protocolplicht.

In het kort: de AVG verplicht organisaties hun gegevens (digitaal) te beschermen. Denk hierbij aan IT beveiliging, autorisatiebeheer en periodieke controles om risico's te minimaliseren. Zorg ervoor dat het bekend is welke acties personeelsleden dienen te ondernemen wanneer informatie wordt gelekt, gestolen en wordt kwijtgeraakt. Dit is terug te vinden in een datalek protocol. Zorg ervoor dat ieder incident dat inbreuk heeft op de privacy ook wordt geregistreerd in een incidentregister. Twee-factorauthenticatie is een sterk middel om datalekken te beperken.

Organisaties moeten:
- Evalueren of gegevens fatsoenlijk worden beschermd tegen cyberaanvallen, ongeautoriseerde toegang en datalekken.
- Een datalek protocol en incidentregister actief in gebruik hebben.
- Gebruik twee-factorauthenticatie waar het mogelijk.

Stap 7. Het juiste gebruik van cookies

Organisaties gebruiken vele cookies en soortgelijke technieken om websites gebruikersvriendelijker te maken en om informatie te verzamelen over de webbezoekers. Dit is natuurlijk begrijpelijk, alleen de AVG verplicht organisaties om webbezoekers te informeren en ook om toestemming te vragen. Organisaties mogen webbezoekers dus niet weren, omdat zij geen toestemming willen geven voor alle cookies.

Via een cookie statement kunt u in eenvoudig taalgebruik toelichten welke cookies worden gebruikt. Waarom deze worden geplaatst, welke informatie met welk doel wordt verzameld en of de informatie aan derden wordt verstrekt. Stel daarnaast procesbeschrijvingen op, zodat het duidelijk is welke cookies precies wanneer actief zijn. Stel uzelf ook de vraag als organisatie, of deze cookies wel bij uw organisatiecultuur en visie passen.

Toon een passende cookiebanner met een directe verwijzing in de vorm van een link naar het cookie statement. Onderscheid hierin de verschillende cookies, zoals: functionele, analytische, tracking en social media cookies. De functionele cookies zijn vereist voor het goed functioneren van de website waardoor toestemming niet is vereist. De andere cookies vereisen wel toestemming van de webbezoeker. Zorg dat de cookiebanner op een later tijdstip kan worden bezocht, zodat de webbezoeker de eerder gegeven toestemming kan wijzigen. Bijvoorbeeld via een link in het cookie statement. De gegeven toestemming dient opgeslagen te worden en jaarlijks te worden hernieuwd.

AVG: artikel 6, 7, 12, 13 & 14

In het kort: zorg ervoor dat cookies zijn beschreven in een cookie statement en in procesbeschrijvingen. Stel automatisch de meest privacy vriendelijke instellingen in dus alleen functionele cookies. Gebruik adequaat een cookiebanner die onderscheid maakt in de cookies en later eenvoudig te wijzigen is. Verwijs naar een cookie statement in eenvoudig taalgebruik die makkelijk te vinden is op de website.

Organisaties moeten:

- Beoordelen of een cookie statement leesbaar is en de informatie geeft die de AVG vereist.
- Een cookiebanner adequaat gebruiken en een link naar het cookie statement bieden.
- Automatisch privacy vriendelijke instellingen hebben op de website en dus privacy by default hanteren.
- Cookie procesbeschrijvingen hebben, zodat het gebruik juist en aantoonbaar is (vooral bij third party cookies).

Stap 8. Maak medewerkers bekend met privacy

De AP noemt het creëren van awareness als een van de belangrijkste instrumenten om AVG compliant te worden. Belangrijk is hierbij ‘walk the talk’ en toegankelijk te zijn om privacy ‘levend’ te houden. Het is afhankelijk van de grootte van de organisatie om eventueel ook privacy advocates in te schakelen. Dit zijn medewerkers met een andere functie dan privacy officer, maar wel het privacy enthousiasme hebben en willen overdragen. Het bestuur speelt hierin ook een grote rol. Zij dienen ook hun steun te laten zien en privacy bewustzijn te promoten door onder andere zelf privacy bewust te werk te gaan.

Daarbij kunt u verschillende trainingen aanbieden op verschillende momenten. Natuurlijk is het belangrijk om nieuwe medewerkers bij indiensttreding een AVG training te geven, echter hierna stopt het niet. Biedt periodiek trainingen aan om privacy actueel te houden. Biedt daarbij ook de mogelijkheid om meer te lezen over privacy door middel van een kennisbank, waar onder andere het privacy beleid, webinars en e-learnings te vinden zijn.

De praktijk laat zien dat het simuleren van datalekken een sterke manier is om het interactief te maken en het privacy gesprek gaande houden. Voorbeelden zijn het versturen van phishing mails, workshops geven met actuele voorbeelden of een privacy escaperoom.

AVG: artikel 24
Awareness

In het kort: zorg ervoor dat er binnen de organisatie een sterke privacy bewustzijn heerst. Dat zijn de belangrijkste organisatorische beveiligingsmaatregel die u kunt nemen. Train uw personeelsleden regelmatig op het gebied van AVG en zorg dat privacy als een positieve toevoeging wordt gezien. Denk hierbij aan een jaarlijkse privacy bewustzijn campagne, maar ook aan periodieke trainingen met praktijk voorbeelden en simuleer een datalek (stuur een phishing mail uit en bespreek de reacties).

Organisaties moeten:
- Privacy bewustzijn promoten.
- Periodiek verschillende privacy trainingen verzorgen aan het personeel en aansturende medewerkers.
- Online eenvoudig het privacy beleid, webinars, e-learnings en artikelen over privacy aanbieden.
- Privacy documentatie actueel en volledig houden.

Stap 9. Bundel alles samen in een privacy beleid

De Autoriteit Persoonsgegevens vindt het belangrijk dat een organisatie definieert wie welke verantwoordelijkheden draagt voor privacy compliance, zowel op sturend als op uitvoerend niveau. Een organisatie dient het onderwerp dus te beleggen bij één persoon met voldoende mandaat of binnen een bedrijfsonderdeel. En dit ook te documenteren in het privacy beleid, zodat er een bepaalde accountability ontstaat en privacy continu wordt gewaarborgd.

Daarbij is het cruciaal dat privacy meegaat in de organisatie breed PDCA-cyclus, zodat privacy processen adequaat en frequent worden gecheckt. We hebben eerder gesproken over grondslagen, verwerkers, organisatorische en technische maatregelen, datalekken en cookies. Wanneer er een gezamenlijk document is met alle privacy processen gebundeld dan is het beleid omtrent privacy duidelijk, aantoonbaar en eenvoudig te raadplegen.

AVG: artikel 24
Privacy beleid

In het kort: bundel alle privacy processen en protocollen in een document genaamd privacy beleid, zodat het beleid duidelijk, aantoonbaar en eenvoudig te raadplegen is. De privacy verantwoordelijke kan aan toezichthouders aantonen dat uw bedrijfsvoering continu privacy compliant is.

Organisaties moeten:
- Een privacy verantwoordelijke hebben met voldoende mandaat.
- Privacy als continu proces zien organisatie breed waarbij het privacy beleid structuur geeft.

Stap 10. Tot slot; gooi ook eens wat weg

Organisaties weten de delete knop maar mondjesmaat te vinden, terwijl de wet zegt dat zij alleen persoonsgegevens mogen gebruiken als dat noodzakelijk is voor het afgesproken doel. In AVG termen heet dit dataminimalisatie. Na verloop van bijvoorbeeld een klantrelatie is het onvoldoende om een account op 'inactief' te zetten. Persoonsgegevens moeten na verloop van tijd verwijderd of geanonimiseerd worden. In praktijk worstelen organisaties met het vaststellen van bewaartermijnen voor gegevens.

Toch zijn er wel een paar handvatten:

Klantrelatie e-mail en TM
U moet bepaalde gegevens van klanten uit uw marketingdatabase verwijderen als de klantrelatie voorbij is en u deze gegevens hebt verkregen in het kader van die klantrelatie. Veel organisaties zetten de termijn voor het benaderen van een (ex)klant op twee jaar na de laatste financiële transactie.

Direct Mail
Er is geen klantrelatie nodig om iemand een geadresseerd poststuk te sturen. Het gebruik van adresdata voor direct mail blijft opt-out. Zo lang een adresbestand nog redelijk converteert kunnen de gegevens voor direct mail gebruikt worden.

Financiële administratie
U mag persoonsgegevens ook langer bewaren, maar daar moet dan een ander doeleinde voor zijn dan marketing (het terugwinnen van een klant). Bijvoorbeeld omdat dit moet vanwege een *wettelijke verplichting* (de fiscus kent een bewaartermijn van 7 jaar). Of als *bewijsmateriaal bij klachten*. De onrechtmatige daad verjaart immers pas na 5 jaar.

Benieuwd hoe wij u kunnen ondersteunen?

De wijze waarop organisaties klantgegevens gebruiken en met klanten omgaan kan reputaties maken of breken. Daarom is het zo belangrijk dat het volgens de regels gebeurt. DMCC helpt daarbij!

Zo ondersteunen wij onze opdrachtgevers als privacy officer, adviseren wij bij ingewikkelde juridische vraagstukken of controleren wij de naleving van wet- en regelgeving als Functionaris Gegevensbescherming. Ook kunnen wij u adviseren over het creëren van de optimale klantbeleving of datastrategie. Benieuwd hoe wij u kunnen ondersteunen? Neem eens een kijkje op onze website: www.dmcc.nl of bel 088 777 93 11.

Prangende vraag?

Onze experts beantwoorden uw vraag binnen één werkdag

088 777 93 11

info@dmcc.nl

www.dmcc.nl