Stappenplan AVG - proof werken

Het belang van privacy

Op grote schaal wordt informatie over ons vastgelegd en gebruikt. Het is belangrijk dat we zelf kunnen bepalen welke informatie met wie wordt gedeeld, en dat er op een betrouwbare manier met deze gegevens wordt omgegaan. Ook in de culturele sector wordt vaak met persoonsgegevens gewerkt. Het is belangrijk om op een gestructureerde manier om te gaan met de verwerking van deze gegevens. Dit stappenplan biedt je handreikingen hoe je als culturele organisatie AVG-proof kunt werken.

Gevolgen van slechte privacybescherming

Individuen

Houdt een organisatie zich niet aan de privacyregels? Dan krijgen mensen minder zeggenschap over hun eigen gegevens. Het kan leiden tot profilering en soms zelfs tot discriminatie of uitsluiting. Onvoldoende beveiliging vergroot ook het risico op identiteitsfraude.

Organisaties

Organisaties zijn verplicht om persoonsgegevens goed te beschermen. Dat moeten ze ook kunnen aantonen. Lukt dit niet? Dan kan de Autoriteit Persoonsgegevens (AP) sancties en boetes opleggen.

Stappenplan

Stap 1.

Vorm een privacyteam en wijs een privacycoördinator aan

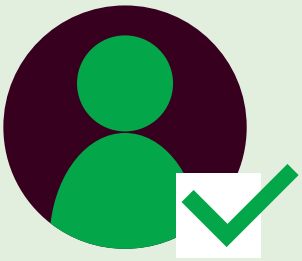
Stel een privacyteam samen met diverse expertise. Benoem een privacy-coördinator die kan begeleiden, adviseren en toezicht houden.

Stap 2.

Creëer een overzicht (per afdeling) met de PDCA-cyclus

PLAN: Wat zijn de verplichtingen uit de AVG en voldoe ik hier al aan?
DO: Voer de gesignaleerde actiepunten uit.
CHECK: Controleer of maatregelen geïmplementeerd zijn en het gewenste effect hebben. Zo niet, zet het weer op de actiepuntenlijst.
ACT: Ga weer aan de slag met de actiepunten uit de evaluatie/controle. Voer verbeteringen door.

Stap 3.



Verwerkingsregister invullen en bijhouden

Vul in het verwerkingsregister in welke verwerkingen van persoons-gegevens er binnen de organisatie plaatsvinden. Breng gegevens per afdeling en per proces in kaart.

Stap 4.

Stel een privacybeleid op

Beschrijf hierin hoe je als organisatie omgaat met de verwerking van persoonsgegevens, met betrekking tot: rechtmatigheid, doelbinding, transparantie, statistisch onderzoek, dataminimalisatie, juistheid, opslagbeperking, vertrouwelijkheid en integriteit, omgang met privacy rechten en direct marketing.

Stap 5.

Stel een privacyverklaring op

Informeer de personen van wie je de gegevens verzamelt. Wat verwerk je precies? Voor welke doeleinden? Voor hoe lang? Publiceer de privacyverklaring op je website.

Wat is een persoonsgegeven?

Alles in de Algemene Verordening Gegevensbescherming (AVG) draait om de bescherming van persoonsgegevens. Hierbij gaat het niet alleen om rechtstreekse informatie over een persoon, maar ook om informatie die te herleiden is naar een persoon.

Voorbeelden persoonsgegevens

- Voor de hand liggende persoonsgegevens zijn iemands naam, adres, telefoonnummer, BSN en pasfoto. Maar persoonsgegevens zijn bijvoorbeeld ook wat iemand op internet koopt, of die persoon allergieën heeft en beelden van een bewakingscamera waar diegene herkenbaar op staat.

- Er zijn ook persoonsgegevens die niet direct over iemand gaan, maar die wel naar die persoon te herleiden zijn. Het gaat dan om gegevens die in combinatie met andere gegevens iets zeggen over een persoon. Bijvoorbeeld het IP-adres van iemands smartphone, kenteken, geboortedatum, postcode, locatiegegevens, stem, of één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische of culturele of sociale identiteit van die persoon. Denk aan inkomen of cultureel profiel.

De AVG maakt onderscheid tussen ‘gewone’ en ‘bijzondere’ persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens die zó privacygevoelig zijn dat het grote(re) impact op iemand kan hebben als deze gegevens worden verwerkt. Daarom krijgen bijzondere persoonsgegevens extra bescherming in de AVG. Gegevens die je (in principe) niet mag verwerken zijn:

- Ras of etnische afkomst
- Politieke opvattingen
- Religieuze of levensbeschouwelijke overtuigingen
- Lidmaatschap van een vakbond
- Genetische gegevens
- Biometrische gegevens
- Gezondheidsgegevens
- Seksueel gedrag of geaardheid

Je mag deze alleen verwerken wanneer er uitdrukkelijke toestemming voor is en het een noodzakelijke verwerking is. Zie **artikel 9 AVG** voor meer informatie.

Vijf stappen om privacy binnen jouw organisatie te waarborgen

Stap 1

Vorm een privacyteam en wijs een privacycoördinator aan.

Vorm een privacyteam om ervoor te zorgen dat jouw organisatie de regels goed naleeft. Hiervoor is veel kennis en kunde nodig. Daarom is het verstandig om het privacyteam een geheel zelfstandig bedrijfsonderdeel te laten zijn, met diverse expertise. Denk hierbij aan leden van verschillende afdelingen, zoals ICT, marketing, management en directie, HR, financiën, juridisch, enz.

Wijs een privacycoördinator aan. De coördinator begeleidt, adviseert bij de invulling van alle privacydocumenten, behandelt de privacyrechten en heeft een toezichthoudende rol. Voorbeelden van taken die het privacyteam zal uitvoeren:

- Toezicht houden op de uitvoering van privacyregels.
- Bewustwording creëren bij het personeel.
- Voorlichting geven.
- Adviseren bij nieuwe ontwikkelingen.
- Opstellen en evalueren van beleid en procedures rondom privacybescherming.
- Controleren of het privacy- en informatiebeveiligingsbeleid wordt nageleefd.
- Interne audits uitvoeren.

Het is belangrijk dat de directie het voortouw neemt in het bevorderen van een privacybewuste organisatie. Bespreek met hen de kernpunten van het privacybeleid en leg vast hoe dit wordt uitgedragen. Stem samen evaluatiemomenten af en spreek af dat er jaarlijks rapportages worden opgesteld. Maak afspraken met de directie over het budget.

Stap 2

Creëer een overzicht van openstaande acties en vooruitgang (per afdeling) met de PDCA-cyclus.

Bij complexe zaken zoals de AVG komt er geen moment dat alle vinkjes gezet zijn en de organisatie 'klaar' is. Om privacy een werkend en levend onderdeel te maken van je organisatie, en om aan te tonen dat je voldoet aan je AVG-verplichtingen, is het handig om te werken volgens een cyclus waarin je continu blijft plannen, analyseren, evalueren en aanpassen: de PDCA-cyclus. De vier letters staan voor Plan, Do, Check, Act. Een methode waarmee je je organisatie continu kunt verbeteren en optimaliseren.

PLAN

Stel vast wat nodig is. Wat zijn de verplichtingen uit de AVG en voldoe ik hier al aan?
Verplichte maatregelen:

- Een verwerkingsregister bijhouden. Hierin vul je in welke verwerkingen van persoonsgegevens er binnen de organisatie plaatsvinden. Breng gegevens per afdeling en per proces in kaart.
- Een risicoanalyse uitvoeren bij gegevensverwerkingen met een hoog privacyrisico. Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen, zodat de organisatie maatregelen kan nemen om deze risico's te verkleinen.
- Een datalekregister bijhouden. Hierin neem je ook de datalekken op die je niet hoeft te melden.
- Aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer je voor deze verwerking toestemming nodig hebt. Bijvoorbeeld door de betrokkene een schriftelijke verklaring te laten ondertekenen. In een online omgeving kan dat door actief een vakje aan te laten vinken.
- Goed kunnen onderbouwen waarom je ervoor gekozen hebt om al dan niet een functionaris gegevensbescherming (FG) aan te stellen wanneer onduidelijk is of je verplicht bent om een FG aan te stellen.
- Een privacyverklaring opstellen. Ook wel privacypolicy genoemd. Deze verklaring is gericht aan degenen wiens persoonsgegevens worden verwerkt. Hierin vermeldt een organisatie welke persoonsgegevens de organisatie gebruikt en waarom.

Wat is de huidige stand van zaken? Creëer (per afdeling) een dashboard van openstaande acties en vooruitgang. Elke afdeling heeft een eigen aanspreekpunt voor de uitvoering van de privacytaken.

DO

Voer de gesignaleerde actiepunten uit. Maak een planning waar iedereen zich aan houdt.

CHECK

Controleer of maatregelen geïmplementeerd zijn en het gewenste effect hebben. Zijn er nieuwe actiepunten bijgekomen? Blijken sommige zaken toch nog niet goed genoeg geregeld? Is er een datalek geweest? Al die punten komen dankzij deze controle weer op de actiepuntenlijst.

ACT

Ga weer aan de slag met de actiepunten uit de evaluatie/controle. Voer verbeteringen door.

Datalekregister

Datalekken kunnen verschillende vormen aannemen, zoals het versturen van informatie naar het verkeerde adres, het verlies van een usb-stick of het klikken op een schadelijke link. Bij een datalek gaat het om onbedoelde toegang tot, vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie. Heb je onverhoopt met een datalek te maken, dan moet je snel in actie komen.

- **Stel een datalekprotocol op**

  Iedereen moet op de hoogte zijn van wat er moet gebeuren. Klik hier op de link voor een stappenplan van de AP.

- **Meld het bij AP**

  Dit moet binnen 72 uur om een boete te voorkomen. Je hoeft het niet te melden als het datalek geen risico voor de rechten en vrijheden van betrokkenen oplevert.

- **Registreer het datalek**

  In het datalekregister neem je ook de datalekken op die je niet hoeft te melden.

- **Meld aan betrokkene**

  Dit is alleen verplicht als het datalek een hoog risico inhoudt, bijvoorbeeld als het om bijzondere of gevoelige informatie gaat en kan leiden tot lichamelijke, materiele of immateriële schade. De melding moet duidelijk aangeven wat er met de gegevens is gebeurd, of ze in handen zijn van onbevoegden, om welke gegevens het gaat en welke maatregelen zijn genomen om het lek te dichten en toekomstige lekken te voorkomen. Het is van belang om in begrijpelijke taal te communiceren en de contactgegevens van de functionaris voor gegevensbescherming/directeur te vermelden voor eventuele vragen.

Stap 3

Vul het verwerkingsregister in en houd het bij.

In het verwerkingsregister vul je in welke verwerkingen van persoonsgegevens er binnen de organisatie plaatsvinden. Voor HR kun je bijvoorbeeld alle stappen van solliciteren, indiensttreding, functioneren, ziekte, re-integratie en uitdiensttreding doorlopen. Vul het register in per afdeling en verdeel het dan verder per proces. Dit kan het afdelingshoofd doen of de privacycoördinator. Als je het voor de eerste keer invult, kun je het zien als een nulmeting. Met een verwerkingsregister kan je laten zien dat je voldoet aan de AVG.

Het verwerkingsregister is vormvrij. Je mag zelf weten hoe je het opstelt, maar de AVG geeft wel aan welke informatie je erin moet zetten:

- Naam en contactgegevens van de verwerkingsverantwoordelijke, bijvoorbeeld de organisatie, afdelingshoofd en/of privacycoördinator.
- Waarom je de persoonsgegevens verwerkt, zoals voor relatiebeheer, personeelsmanagement of financiële administratie.
- Onderzoek de rechtmatigheid van de verwerking. Waarom mag de organisatie deze specifieke persoonsgegevens verwerken? Denk aan toestemming, uitvoering van een overeenkomst, wettelijke verplichting of noodzakelijk voor de vervulling van een taak. (Het is niet verplicht dit in het register te vermelden. Toch kan het verstandig zijn, zodat er goed over nagedacht wordt.)
- Noteer van wie je persoonsgegevens verwerkt, zoals klanten, bezoekers, werknemers, leveranciers, enz.
- Noteer welke gegevens je van hen verwerkt. Bijvoorbeeld naam, adres, e-mail.
- Check of je bijzondere persoonsgegevens verwerkt. Zo ja, heb je toestemming of een andere rechtvaardiging?
- Bekijk of er gegevens worden uitgewisseld met een derde land of internationale organisatie. Zo ja, zijn er voldoende waarborgen?
- Geef indien mogelijk aan hoelang je de gegevens bewaart.
- Leg uit welke maatregelen je hebt genomen om de persoonsgegevens te beveiligen.

Helemaal ingevuld? Evalueer het volgend jaar opnieuw en stel zo nodig bij.

Een verwerkingsregister is bijna altijd verplicht, maar er zijn uitzonderingen. Of je een verwerkingsregister moet opstellen, hangt af van de omvang van de organisatie en het type gegevens dat je verwerkt. Lees hier wanneer het verplicht is om een register op te stellen.

Organisaties schakelen vaak andere organisaties in om persoonsgegevens voor hen te verwerken. Bijvoorbeeld door de boekhouding uit te besteden. Of door gebruik te maken van een clouddienst die persoonsgegevens opslaat. Zo'n andere organisatie heet een verwerker. De organisatie die de verwerker inschakelt, is de verwerkingsverantwoordelijke. Als je gebruikmaakt van de diensten van een verwerker, dan ben je verplicht om een aantal onderwerpen vast te leggen in een schriftelijke overeenkomst. Lees hier wat in een verwerkersovereenkomst moet worden vastgelegd.

Stap 4

Stel een privacybeleid op.

Een privacybeleid is een intern document dat is bedoeld als handleiding voor medewerkers in de organisatie die met persoonsgegevens werken. Het helpt je om te zien of je voldoende maatregelen hebt genomen om de persoonsgegevens van je klanten te beschermen. In dit beleid staan alle basisregels, processen en procedures rondom het gebruik van persoonsgegevens, samen met de achtergrond, visie, principes, checks en bevoegdheden.

Je bent alleen verplicht om een privacybeleid op te stellen als dat in verhouding staat tot jouw verwerkingsactiviteiten. Of je verplicht bent om een privacybeleid op te stellen, hangt af van de concrete omstandigheden. Zoals de aard, de omvang, de context en het doel van de gegevensverwerking. Ben je niet verplicht om een privacybeleid op te stellen? Dan kan het toch nuttig zijn om dat wel te doen. Het helpt je namelijk om te zien of je voldoende maatregelen hebt genomen om de persoonsgegevens te beschermen. Het is ook een manier om aan je klanten en de AP te laten zien dat jullie voldoen aan de privacyregels.

Tips voor het opstellen van een privacybeleid

1. **Beoordeel of je het verplicht bent.**

   Of jouw organisatie een privacybeleid moet opstellen, is afhankelijk van de verwerking. Ga na welke soort gegevens jouw organisatie verwerkt en op welke schaal. Verwerk je bijvoorbeeld op grote schaal bijzondere persoonsgegevens? Dan moet je een privacybeleid opstellen en hanteren. Neem zelf het initiatief. Wacht niet tot de AP erom vraagt.

2. **Gebruik expertise.**

   Gebruik de expertise in jouw organisatie om tot een goed privacybeleid te komen. De privacycoördinator kan hier als intern toezichthouder een belangrijke rol in spelen. Je kunt ook een externe expert om advies vragen.

3. **Leg het vast in 1 document.**

   Leg het privacybeleid vast in 1 document. Voorkom versnippering van informatie in een privacyverklaring, een verwerkingsregister en een privacybeleid. De informatie is dan weliswaar beschikbaar, maar het is overzichtelijker als het privacybeleid een compleet beeld geeft.

4. **Wees concreet.**

   Een goed privacybeleid vertaalt de AVG-normen concreet naar de gegevensverwerking binnen jouw organisatie. Herhalen van de AVG-normen is niet genoeg; maak het relevant voor jouw situatie.

Een privacybeleid kent geen strikte vormvereisten. Het is echter van essentieel belang om hierin te beschrijven hoe je als organisatie omgaat met de verwerking van persoonsgegevens met betrekking tot:

Rechtmatigheid

Onder de AVG mogen organisaties alléén persoonsgegevens verwerken als ze daar een wettelijke grondslag voor hebben. De AVG kent zes grondslagen: toestemming, uitvoering van de overeenkomst, wettelijke verplichting, vitaal belang van betrokkene of andere personen, algemeen belang of gerechtvaardigd belang. Wanneer een organisatie de gegevensverwerking niet op minimaal één van deze grondslagen kan baseren, dan is het niet toegestaan om persoonsgegevens te verwerken. Zie artikel 9 AVG voor meer informatie.

Let op Verwerking van de gegevens van een kind dat jonger is dan 16 jaar is alleen rechtmatig met toestemming van de ouders.

Transparantie

Het moet voor de betrokkenen duidelijk zijn door wie, hoe en waarom hun persoonsgegevens worden verwerkt. Beschrijf van welke bezoekers je data verzamelt. Welke data? Ook de persoonlijke voorkeuren? Maak je een profiel van elke bezoeker? Koppel je dit aan een postcode? Hebben jullie daar nog wel een wettelijke grondslag voor? Hoe lang bewaar je gegevens na het kopen van een ticket of product? Koppel je dit aan de gegevens die de cookies op de website verzamelen? Gebruik je de gegevens voor social media als Instagram en Facebook? Je bent dan gegevens aan het hergebruiken. Is dit nog altijd te verenigen met het oorspronkelijke doeleinde van de verwerking? Hierover moet je allemaal transparant zijn in je privacybeleid.

Doelbinding

Beschrijf met welk doel je de persoonsgegevens verwerkt. Organisaties mogen persoonsgegevens alleen verzamelen met een gerechtvaardigd doel. Dat doel moet specifiek zijn en vooraf uitdrukkelijk zijn omschreven. De organisatie mag de gegevens niet ineens voor een heel ander doel gebruiken en ook niet zomaar doorgeven aan andere organisaties of personen. Dit mag alleen als het verenigbaar is met het doel waarvoor de gegevens zijn verzameld. Of dit zo is, kan per situatie verschillen. Lees hier meer over doelbinding.

Statistisch onderzoek

Beschrijf hoe je persoonsgegevens gebruikt voor statistisch onderzoek. Culturele organisaties willen vaak statistieken verzamelen voor subsidiegevers en interne informatie over bezoekers, kopers en dienstafnemers. Archivering, wetenschappelijk en statistisch onderzoek worden in principe beschouwd als toegestane verdere verwerking. Het doel van statistisch onderzoek moet de verwerking van geaggregeerde gegevens zijn. Met de statistiek mag je dus niet weer gericht personen gaan benaderen voor doeleinden als marketing. In dat geval ben je niet meer bezig binnen het doel van statistisch onderzoek.

Dataminimalisatie

Beschrijf hoe je de eisen van dataminimalisatie toepast. Zoals de verplichting om niet méér gegevens te verwerken dan noodzakelijk. Als organisaties persoonsgegevens verwerken, moeten ze daarbij uitgaan van het principe 'zo min mogelijk'. Dat houdt bijvoorbeeld in dat de verwerking van de gegevens moet passen bij het doel. En dat de organisatie niet méér gegevens mag verwerken dan noodzakelijk is om het doel te bereiken. Een dergelijke maatregel van dataminimalisatie kan zijn pseudonimisering of anonimisering.

Juistheid

De verwerkingsverantwoordelijke moet ervoor zorgen dat de gegevens juist zijn en de gegevens actualiseren als dat nodig is. Mensen kunnen ook aan organisaties vragen hun persoonsgegevens aan te passen als die niet kloppen.

Opslagbeperking

Organisaties moeten persoonsgegevens verwijderen zodra die niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld. Er geldt dus een beperkte bewaartermijn voor gegevens. Voor alle verwerkingen moeten de organisaties nadenken of het echt nodig is om gegevens te bewaren en, als dat het geval is, hoe lang dat moet zijn. Dit moet worden opgenomen in het privacybeleid, waarin zowel de redenen voor de bewaartermijn als de exacte duur ervan worden vastgelegd. Zodra de afgesproken bewaartermijn is verstreken, mogen de gegevens niet langer worden verwerkt, tenzij voor een ander vergelijkbaar doel.

Vertrouwelijkheid en integriteit

Persoonsgegevens moeten goed beschermd zijn tegen verlies, ongeoorloofd gebruik en cybercriminaliteit om risico's zoals datalekken en identiteitsfraude te voorkomen. Beschrijf de organisatorische en technische maatregelen die zijn genomen om de persoonsgegevens te beveiligen. Elke organisatie die persoonsgegevens verwerkt, bepaalt zelf welke beveiligingsmaatregelen nodig zijn en moet kunnen aantonen dat persoonsgegevens goed zijn beschermd. Het waarborgen van de beveiliging moet continu aandacht krijgen binnen de organisatie. De AP houdt toezicht op de beveiliging van persoonsgegevens en kan ingrijpen, bijvoorbeeld door het opleggen van boetes als de beveiliging niet goed is geregeld.

In de AVG staat dat je persoonsgegevens goed moet beveiligen. Daarom moet je eerst goed in kaart brengen welke verwerkingen je uitvoert. Daarna bepaal je welke technische en organisatorische maatregelen nodig zijn om die verwerkingen goed te beveiligen. Je kunt een zorgvuldige omgang met persoonsgegevens organisatorisch en technisch stimuleren. Dit doe je met 'privacy by design' of 'privacy by default'.

- **Privacy by design** (privacy door ontwerp) houdt in dat je er al bij het ontwerpen van producten en diensten voor zorgt dat je persoonsgegevens goed beschermt. En dat je de gegevens niet langer bewaart dan nodig is voor het doel van de verwerking.

- **Privacy by default** (privacy door standaardinstellingen) houdt in dat de standaardinstellingen van je product of dienst privacyvriendelijk zijn. Dit betekent dat je technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat je, als standaard, alleen persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat je wilt bereiken.

Voor meer informatie over privacy by design & privacy by default, zie deze publicatie van De European Data Protection Board (EDPB), een onafhankelijk orgaan waarin alle nationale privacytoezichthouders uit de Europese Unie (EU) samenwerken.

Privacy awareness

De effectiviteit van beveiligingsmaatregelen staat of valt met de privacy awareness binnen de organisatie. Begrijpen mensen het belang? Zijn zij gemotiveerd en kunnen zij op de juiste wijze omgaan met data en de systemen? Een goede voorlichting en regelmatige aandacht voor dit onderwerp zijn net zo essentieel als de maatregelen zelf. Lees **hier** meer over het beveiligen van persoonsgegevens

Omgang met privacyrechten

Hierin leg je vast hoe je omgaat met rechten van betrokkenen en hoe zij die rechten kunnen uitoefenen. Zoals het recht om een klacht in te dienen bij de AP. Maar ook het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens. Lees **hier** welke algemene regels gelden voor alle privacyrechten.

Tip

Denk na over een uniform systeem of structuur waarmee data worden opgeslagen. Op die manier kunnen persoonsgegevens ook gemakkelijk worden teruggevonden, bijvoorbeeld wanneer een betrokkene een verzoek doet of gegevens gearchiveerd/vernietigd/ overgedragen moeten worden.

Direct marketing

Direct marketing aan eigen klanten is toegestaan op basis van gerechtvaardigd belang. Voor anderen is toestemming vereist. De betrokkene mag altijd bezwaar maken tegen direct marketing, ongeacht of de gegevens gebruikt worden binnen het oorspronkelijke doeleinde of voor verdere verwerking. Dit recht van bezwaar moet duidelijk en los van de andere informatie vermeld worden. Lees **hier** aan welke eisen je moet voldoen wanneer je persoonsgegevens wil gebruiken voor direct marketing.

Door alle bovenstaande aspecten te integreren, creëer je niet alleen een AVG-conform privacybeleid, maar toon je tevens betrokkenheid bij de bescherming van privacy en gegevensbeveiliging binnen jouw organisatie.

Stap 5

Stel een privacyverklaring op.

Volgens de AVG heb je een wettelijke informatieplicht om betrokkenen te informeren wat je precies aan gegevens verwerkt, voor welke doeleinden, voor hoelang je deze bewaart, enz. De AVG vraagt hier om een prettige, leesbare samenvatting, bestemd voor je klanten/bezoekers/toekomstige medewerkers. De logische keuze is om deze op je website te publiceren. Het is dus handig om dit in begrijpelijke, heldere taal te beschrijven. Daarbij zullen bijvoorbeeld de volgende onderwerpen worden behandeld:

- Hoe en op welke wijze respecteert en waarborgt de organisatie uw privacy?
- Welke gegevens verwerkt de organisatie bij de volgende processen: bezoek website (cookies), online aankopen (ticket), een account aanmaken, het delen van gegevens met derden als de ticketverkoop via hen verloopt, beveiligingscamera's, donateur worden of andere vorm van gift, abonnement, nieuwsbrieven en andere communicatie over actualiteiten en events, sollicitatie, bewaartermijn van gegevens, rechten van betrokkenen, enz.

Klik **hier** op de link voor een voorbeeld van een privacybeleid.

Handige tips en links

In de dynamische wereld van gegevensbescherming is het essentieel om goed geïnformeerd te blijven over de AVG. Hier zijn enkele handige tips en links die kunnen helpen bij het begrijpen en naleven van de AVG.

- Autoriteit Persoonsgegevens (AP) De Autoriteit Persoonsgegevens is de Nederlandse toezichthouder op de naleving van de AVG.
- Notendop AVG Deze beknopte handleiding van de AP geeft een overzicht van de belangrijkste punten van de AVG, waardoor het een handige startgids is voor organisaties.
- Rijksoverheid.nl Algemene informatie over de AVG zoals hoe je kunt anticiperen op de AVG.
- Regelhulpen voor bedrijven – AVG Deze tool biedt praktische begeleiding en stappenplannen om organisaties te helpen bij het implementeren van de AVG in hun bedrijfsprocessen.
- Speciale website EU voor MKB De Europese Unie heeft een speciale website gemaakt om het MKB te informeren over de AVG. Eén geheel van regels voor alle bedrijven die actief zijn in de EU, ongeacht waar ze zijn gevestigd.
- Europese Commissie (EC) De uitvoerende macht van de Europese Unie. Het handelt in het belang van alle EU-landen samen. Op deze site vind je informatie over de Europese Commissie en haar beleid.
- Europees Comité voor gegevensbescherming Op deze site worden diverse thema's van de AVG uitgelegd door het Europees Comité voor gegevensbescherming. In het comité zijn alle nationale toezichthouders voor de gegevensbescherming van de lidstaten vertegenwoordigd. De informatie op de site is Engelstalig.
- General Data Protection Regulation Deze Engelstalige site koppelt de officiële artikelen van de AVG aan de overwegingen. Behulpzaam bij het verder doorgronden van de AVG.
- Nederland ICT Hier vind je nuttige algemene ICT-gerelateerde informatie en een aantal interessante factsheets.

Disclaimer

In dit stappenplan gaan we kort in op belangrijke punten van de AVG-wetgeving. Dit stuk is echter niet compleet en uitputtend.