Algemene Verordening Gegevensbescherming (AVG): Stappenplan voor ontwikkeling privacy beleid voor musea en andere erfgoedinstellingen

Inhoud

Inleiding 3
Hoe dit stappenplan te gebruiken? 3
Stap 1: verwerking van persoonsgegevens 5
Stap 2: leg een verwerkingenregister aan 5
Stap 3: waarom verzamelt u gegevens en wat gaat u hier mee doen? 6
Stap 4: stel de wettelijke grondslag vast 6
Stap 5: stel een privacyverklaring op 8
Stap 6: rechten van betrokkenen 8
Stap 7: beveiliging 9
Stap 8: datalekken 9
Stap 9: verwerkersovereenkomsten 10

Inleiding

Sinds 25 mei 2018 is de Wet bescherming persoonsgegevens vervallen en daarvoor in de plaats is de Algemene Verordening Gegevensbescherming (AVG) in de plaats gekomen. De AVG verschilt op een aantal punten van de oude wetgeving. Het omgaan met persoonsgegevens, het zogenaamde verwerken, moet niet alleen rechtmatig gebeuren, maar ook aantoonbaar rechtmatig. Die aantoonbaarheid heeft gevolgen voor uw organisatie. U moet meer vastleggen over de verwerking van persoonsgegevens, en u moet zich daarover kunnen verantwoorden. In de eerste plaats tegenover de personen van wie u de gegevens verwerkt, de betrokkene, zoals die in de AVG heet. In de tweede plaats tegenover de Autoriteit Persoonsgegevens (AP), die onder de AVG uitgebreidere bevoegdheden heeft gekregen, waaronder het opleggen van hoge boetes. Maar voordat we ons hierover druk maken moeten we niet vergeten stil te staan wat de achtergrond van deze Europese wet is, namelijk de bescherming van de privacy, en dat het bewust bezig zijn met de persoonsgegevens die u verwerkt en de wijze waarop u dat doet daar een bijdrage aan levert. Daarnaast heeft het ook voordelen voor uw organisatie: persoonsgegevens die u kunt verwijderen hoeft u ook niet te beveiligen en als het met minder kan ruimt het ook op.

Het is belangrijk dat alle medewerkers van de organisatie bekend zijn met de uitgangspunten van de AVG omdat iedereen er mee te maken heeft. Voor de mensen die toegang hebben tot de persoonsgegevens is het belangrijk dat er afspraken worden gemaakt over bijvoorbeeld de beveiliging, zoals het op slot zetten van de computer. Voor de mensen die niet direct met de persoonsgegevens werken gelden deze afspraken ook, maar ook hoe de toegang tot uw museum is geregeld, of hoe in overleg beveiligingscamera's worden geplaatst zonder dat men teveel wordt opgenomen. Als laatste moet het bestuur, of de leidinggevende, weten waar men nou precies verantwoordelijk voor is en wat die verantwoordelijkheid onder de AVG met zich meebrengt.

Dit stappenplan is behandeld tijdens de informatiesessie d.d. 11 juni 2018.
Het beperkt zich tot de toepassing van de AVG in de organisatie van uw instelling.
De AVG kan ook gevolgen hebben voor uw collecties en archieven. In de AVG worden een aantal uitzonderingen gemaakt voor instellingen die onder de archiefwet vallen, vooralsnog is hier veel onduidelijkheid over. Wij zullen de ontwikkelingen volgen. .

Heeft u tijdens de uitwerking van uw privacybeleid nog vragen: wij organiseren in 2018 spreekuren waarvoor u vooraf uw vragen per mail indient. De data van de spreekuren vindt u binnenkort op de website en worden aangekondigd in de nieuwsbrief De Erfgoedloper.

Hoe dit stappenplan te gebruiken?

In dit plan staan de onderwerpen waar u iets mee moet. Voordat u denkt: "moeten we dit allemaal regelen?", hoe minder u verwerkt, of hoe minder gevoelige gegevens, hoe relatief makkelijker het is. Gebruik vooral uw gezonde verstand, en hou het belang voor ogen van de mensen waarvan u de gegevens verwerkt. Als u het allemaal niet in één keer klaar heeft, scheelt het al als u een plan heeft waarmee u kunt laten zien er serieus werk van te maken.

Wie de volledige regelgeving wil inzien, kan deze vinden op:
www.autoriteitpersoonsgegevens.nl

Voordat we beginnen met de stappen is het goed om de hoofdlijn van de AVG in het achterhoofd te houden:

1. Het doel van de verwerking: waarom verwerkt u bepaalde persoonsgegevens. Belangrijk hierbij is de zogenaamde doelbinding, wat bepaalt dat u persoonsgegevens niet voor een ander doel mag gebruiken dan waarvoor u ze heeft verzameld.
2. Mag dat volgens de wet? Dat noemen we de grondslag; al uw verwerkingen moeten op één van de zes grondslagen gebaseerd zijn die in de AVG worden genoemd.
3. Als u doel en grondslag heeft bepaald moet u de gegevens zorgvuldig en netjes verwerken. Hoe zijn ze beveiligd en is het voor iedereen duidelijk hoe u het heeft geregeld?

Stap 1: verwerking van persoonsgegevens

We hebben het over de toepassing van de AVG, en dus over de verwerking van persoonsgegevens. Persoonsgegevens zijn gegevens waarmee een natuurlijk persoon kan worden geïdentificeerd, zoals een visitekaartje, een rijbewijs, telefoonnummer, e-mailadres etc. Het is van belang om eerst te bepalen òf er persoonsgegevens in uw organisatie worden verwerkt. Het gaat niet alleen om klant- of bezoekersgegevens, maar bijvoorbeeld ook om personeels- of vrijwilligersadministratie, cameratoezicht en de persoonsgegevens van bedrijven en instellingen waarmee u contact onderhoudt. Denk ook aan verwerkingen die wat minder zichtbaar zijn, zoals de bezoekersgegevens op uw website en e-mail.

Actie:

- Inventariseer welke persoonsgegevens worden verzameld. Het is verleidelijk om meteen “de diepte” in te gaan, maar het is belangrijker om eerst een volledig beeld te hebben over wat u nou precies aan verwerkingen van persoonsgegevens in huis hebt. Wat kan helpen is om na te denken van welke soort betrokkenen u gegevens verwerkt (“bezoekers”, “donateurs” of “sollicitanten”) en dan vast te stellen waar deze gegevens zich bevinden: welke computer, netwerklocatie, in de archiefkast, of bijvoorbeeld bij een externe partij.

Voorbeeld:

Persoonsgegevens	Locatie
Vrijwilligers	Excelsheet op PC in kantoor
Aanmeldformulieren evenementen	Melkbus naast de ingang
Contactgegevens donateurs	PC/Gmail

Stap 2: leg een verwerkingenregister aan

Hoewel het voor kleine organisaties geen verplichting is, kan het aanleggen van een overzicht van uw verwerkingen erg handig zijn. Met een up-to-date verwerkingenregister heeft u beter zicht op uw verwerkingen, wat helpt om goed na te denken over de voorwaarden waaronder u persoonsgegevens verwerkt. Met een actueel overzicht kunt u daarnaast beter voldoen aan de transparantievereisten van de AVG, bijvoorbeeld als iemand wil weten welke gegevens u van hem of haar verwerkt en hoe u dat allemaal geregeld heeft.

- Actie: Maak een verwerkingenregister (zie voorbeeld) waarin staat:
    - Naam en contactgegevens van de verantwoordelijke, bv uw stichting en degene die over de verwerkingen gaat;
    - De naam van de verwerking, bijvoorbeeld “Personeel” of “Verzendlijst”;
    - Locatie van de verwerking: waar zijn de gegevens opgeslagen? Denk ook aan papier!
    - Omschrijving van de betrokkenen, zoals nieuwsbriefabonnees, vrienden, personeel, zakelijke relaties etc.
    - De persoonsgegevens: wat legt u vast? Mailadres, NAW-gegevens, telefoonnummer etc.
    - Het doel van de verwerking: waarom verzamelt u deze gegevens (zie stap 3)?

- Grondslag bv toestemming of gerechtvaardigd belang, inclusief onderbouwing (zie ook stap 4);
- Hoe lang u de persoonsgegevens bewaart en waarop deze termijn is gebaseerd;
- Beveiliging: zit er een antivirus programma op de computer, gaat de computer buiten openingstijden achter slot en grendel of staat alles op een draagbare schijf of usb-stick die op een andere plek wordt bewaard;
- Omschrijving van de ontvangers. Dat zijn eventuele partijen met wie u gegevens deelt, bijvoorbeeld een ander museum of als de gegevens "in de cloud" staan. Als er ontvangers buiten de EU zijn moeten deze apart worden genoemd, inclusief het land;

Stap 3: waarom verzamelt u gegevens en wat gaat u hier mee doen?

Een vereiste van de AVG is dat u documenteert waarom u bepaalde persoonsgegevens verzamelt en wat u er mee wilt doen. Door dit te vermelden in het verwerkingenregister voldoet u aan de onder de AVG vereiste duidelijkheid richting betrokkenen en de toezichthouder. De AVG bepaalt dat persoonsgegevens alleen mogen worden verwerkt voor het doel waarvoor u ze verzamelt. Het is daarom belangrijk dat u zich aan het oorspronkelijke doel van de verwerking houdt. Verwerk daarnaast zo min mogelijk persoonsgegevens; denk steeds goed na welke gegevens u vraagt en beperk u tot de hoogst noodzakelijke. Voor een elektronische nieuwsbrief heeft u genoeg aan een e-mailadres, vraag dan niet naar allerlei personalia of geslacht. Als de verwerking buiten het oorspronkelijke doel valt zijn er nog wel mogelijkheden, en dat is als dat andere doel verenigbaar is met het oorspronkelijke doel. Zo is het houden van een enquête over de kwaliteit van de nieuwsbrief verenigbaar met het oorspronkelijke doel van het versturen van de nieuwsbrief. Zorg in dat geval voor terughoudend gebruik van de gegevens en laat de mogelijkheid dat betrokkenen zich er voor kunnen afmelden. Bepaal ook hoe lang u de gegevens wilt bewaren. Voor wat betreft Mailchimp: kijk goed welke instellingen je kan aanpassen zodat zo min mogelijk gegevens met andere partijen wordt gedeeld. Kijk ook naar goedkope alternatieven zoals Enormail, wat in het Nederlands wordt aangeboden.

Actie:

- Leg van de verwerkingen die u heeft verzameld vast waarom u dat doet, bv "verzenden nieuwsbrief", of "vrijwilligersadministratie". Kijk of u met minder gegevens af kan en hoe lang u ze wilt bewaren. Als u een doel heeft wat volgens u verenigbaar is met het oorspronkelijke doel, legt u vast waarom u dat vindt. Kijk ook of er privacyvriendelijker alternatieven zijn voor software die u nu gebruikt

Stap 4: stel de wettelijke grondslag vast

Onder de AVG moet u voor de verwerking van persoonsgegevens kunnen terugvallen op één van de zogenaamde wettelijke grondslagen. Voor kleine musea zijn de relevante grondslagen:

1. Toestemming van de betrokkene
2. Overeenkomst met de betrokkene
3. Wettelijke verplichting die vereist dat u persoonsgegevens verwerkt
4. Een eigen gerechtvaardigd belang

Ad 1: Toestemming van de betrokkene.
Deze moet vrijwillig zijn gegeven. Bij het vragen van toestemming, geeft u duidelijk en in eenvoudige taal aan waarvoor de toestemming wordt gegeven. Verstop de toestemming niet in een lange tekst, maar wees helder, bijvoorbeeld door bij de toestemming een vraag te stellen ("Wilt u…) of in duidelijke bewoordingen een ja/nee vraag te stellen. De betrokkene moet daarnaast goed geïnformeerd worden. Dat kan met een specifieke toestemming en bijvoorbeeld een heldere privacyverklaring worden geregeld . Voor een sterk bewijs voor de toestemming is het advies is om te werken met een "dubbele opt-in", waarbij na inschrijving de betrokkene een e-mail ontvangt waarin de keuze nogmaals bevestigd wordt. De toestemming moet te allen tijde in te trekken zijn. Dat vergt wel enige administratie, maar daarmee kunt u na intrekking dit ook meteen regelen door na de intrekking de betreffende persoonsgegevens per omgaande de gegevens te vernietigen. Die toestemmingadministratie kunt u bijvoorbeeld regelen door de email waarin de toestemming is gegeven als bestand op te slaan in een map met de naam van de ontvanger. Let er op dat bij het nemen van foto's, wat ook een vorm van verwerken van persoonsgegevens is, ook soms toestemming gevraagd moet worden. Als u een evenement organiseert, zet dan op de uitnodiging dat er foto's gemaakt kunnen worden en wat u daarmee gaat doen. Laat mensen dat weten en stel ze in de gelegenheid om er ofwel niet op te komen, dan wel dat ze hun toestemming geven. Neem dit op in uw privacyverklaring. Als er een journalist een foto maakt van uw evenement dan vallen die foto's onder de journalistieke exceptie waardoor u daar geen zorgen over hoeft te hebben. Het moet echt

Ad 2: Overeenkomst met de betrokkene.
Voor het verwerken van persoonsgegevens die redelijkerwijs nodig zijn voor de uitvoering van een overeenkomst is geen aparte toestemming nodig. Dit kan een koopovereenkomst zijn, maar ook iemand die een kaartje koopt, een arbeidsovereenkomst of een overeenkomst met vrijwilligers. Onderbouw wel wat "redelijkerwijs noodzakelijk" is in het geval van uw verwerkingen.

Ad 3: Wettelijke verplichting die vereist dat u persoonsgegevens verwerkt.
Deze grondslag is van toepassing als de wet u opdraagt om persoonsgegevens te verwerken, bijvoorbeeld het bewaren van een kopie ID-bewijs op grond van de wet op de loonbelasting. Let op dat verwerking van BSN alleen mag als daar een wettelijke verplichting voor is.

Ad 4: Een eigen gerechtvaardigd belang.
Deze "restcategorie" lijkt eenvoudig: u vindt dat u een belang heeft, en daarom gaat u persoonsgegevens verwerken. Echter zo eenvoudig ligt het niet. U moet voor deze grondslag kunnen aantonen welke belangenafweging u heeft gemaakt, op grond waarvan uw belang zwaarder weegt dan het privacybelang van de betrokkene. Denk aan leden, donateurs of "Vrienden van…". Deze mag u, op basis van gerechtvaardigd belang vanwege hun kennelijke betrokkenheid met uw instelling, per post of telefonisch berichten sturen die te maken hebben met het belang en/of doelstelling van uw organisatie (NB e-mail en SMS hebben altijd toestemming nodig). De regels rondom ongevraagd mailen van relaties en klanten zijn vastgelegd in de Telecommunicatiewet. Let er wel op dat u kunt aantonen dat er een relatie is met de geadresseerden en zorg altijd voor een link in het bericht waarmee direct uitschrijven mogelijk wordt gemaakt. Dit legt u vast in het verwerkingenregister en meldt

het in uw privacyverklaring. Deze direct marketing wordt onder de AVG gezien als een gerechtvaardigd belang, maar dat ontslaat u niet van het maken van een belangenafweging.

Actie:

- Bepaal per verwerking op basis van welke wettelijke grondslag u dat doet. Leg dit vast in het verwerkingenregister en onderbouw dat waar nodig.

Stap 5: stel een privacyverklaring op

Omdat het voor iedereen duidelijk moet zijn wat er met hun gegevens gebeurt verplicht de AVG tot het beschikbaar stellen van een privacyverklaring. Met deze privacyverklaring laat u zien waarom u bepaalde persoonsgegevens verwerkt, hoe ze worden beveiligd en hoe betrokkenen hun rechten kunnen uitoefenen, bijvoorbeeld het recht op inzage. In een privacyverklaring moet in elk geval staan:

- Naam van de verantwoordelijke en contactpersoon;
- Of u gegevens van minderjarigen (jonger dan 16) verwerkt, daar is toestemming van de ouders voor nodig.
- Beknopt omschreven doelen van de verwerking(-en) en bewaartermijn;
- Gebruik van cookies op de website. Leg uit wat het is en waarvoor u ze gebruikt (vraag ook uw provider of websitebouwer);
- Beveiliging. Beschrijf op hoofdlijnen hoe u de persoonsgegevens heeft beveiligd.
- Met welke partijen u persoonsgegevens deelt;
- Hoe betrokkenen hun rechten kunnen uitoefenen (zie stap 6).
- Verwijzing naar de Autoriteit Persoonsgegevens voor het uitoefenen van het klachtrecht

Let op dat de privacyverklaring in begrijpelijk Nederlands wordt opgesteld. Dus geen lange juridische verhandelingen, maar korte zinnen die de lezer meteen duidelijk maken wat er wordt bedoeld. Het beschikbaar stellen kan op uw website, maar als u een papieren inschrijfformulier gebruikt voor de nieuwsbrief, leg daar dan ook een privacyverklaring bij die eventueel kan worden meegenomen. Breng uw relaties op de hoogte van uw (nieuwe) privacyverklaring.

Actie:

- Stel een privacyverklaring op die voldoet aan bovenstaande en stel deze waar nodig makkelijk beschikbaar.

Stap 6: rechten van betrokkenen

Betrokkenen hebben een aantal rechten, en om aan die rechten tegemoet te komen is het nodig dat u in uw organisatie daarover afspraken maakt.

Het inzagerecht betekent dat u op verzoek van de betrokkene een overzicht en kopieën moet geven van de gegevens die u verwerkt, inclusief de doelen, bewaartermijn, de ontvangers (wie mogen erbij of met wie deelt u de gegevens?) en hoe u aan de gegevens bent gekomen. Voor zo'n overzicht mogen geen kosten in rekening worden gebracht. Om een datalek te voorkomen moet u wel zeker weten dat u de persoonsgegevens aan de juiste persoon verstrekt. Zorg dat u binnen vier weken aan het verzoek voldoet.

Er zijn nog een aantal rechten. Het recht op correctie, op grond waarvan betrokkenen hun gegevens kunnen laten wijzigen, bijvoorbeeld bij een naamsverandering bij huwelijk. Daarnaast het recht op verwijdering, waar een betrokkene een beroep op kan doen als de bewaartermijn van de persoonsgegevens is verstreken of als er geen grondslag meer is voor de verwerking. Het recht op bezwaar houdt verband met de verwerking van persoonsgegevens op een eigen gerechtvaardigd belang (zie onder stap 4). Denk aan een gepubliceerde lijst van donateurs, waar iemand die daar op staat bezwaar maakt tegen de vermelding van zijn naam, of een beveiligingscamera die onnodig veel personeel vastlegt. Als laatste het recht op overdracht van gegevens, wat zoveel betekent dat de gegevens van de betrokkene in een elektronisch formaat kunnen worden overgedragen aan een organisatie die een vergelijkbare dienst als de uwe aanbiedt. Van de laatste is de kans zeer klein dat u daarmee te maken krijgt. Het voldoen aan een inzageverzoek zal vaak de aanleiding zijn voor de uitoefening van de andere rechten.

Actie:

- Leg afspraken vast over hoe u binnen de termijn kunt voldoen aan inzageverzoeken. Zorg dat in de privacyverklaring op uw website vermeld staat hoe betrokkenen zo'n verzoek kunnen indienen.

Stap 7: beveiliging

Voor het zorgvuldig omgaan met persoonsgegevens is het van belang dat deze worden beveiligd. Beveiliging wordt opgedeeld in technische en organisatorische maatregelen. De maatregelen moeten passend zijn gezien de soort gegevens die u verwerkt en de risico's die daarmee kunnen worden gelopen, en u moet zich erover kunnen verantwoorden. Voor de technische beveiliging kijkt u bijvoorbeeld naar wachtwoorden op de pc’s (lengte, heeft en gebruikt iedereen een eigen wachtwoord) en of de gegevens zijn versleuteld (ook de backup!). Dit soort regels werkt alleen als ook worden uitgevoerd in de organisatie. Maak en hou dit bespreekbaar. Denk bij organisatorische maatregelen bijvoorbeeld aan het niet laten slingeren van inschrijfformulieren (clean desk) en het verwijderen van accounts als personeel uit dienst treedt, of vrijwilligers die niet meer voor uw museum werken.

Actie:

- Sta stil bij de wijze waarop u nu werkt (hoe komen gegevens binnen, waar worden ze bewaard, wie kan erbij etc.) en neem maatregelen als daar reden voor is. Documenteer dit en houd de medewerkers op de hoogte. Controleer regelmatig of de beveiliging nog werkt en zet beveiliging regelmatig op de agenda.

Stap 8: datalekken

Ondanks de beveiliging kan het voorkomen dat de persoonsgegevens die u verwerkt bij onbevoegden onder ogen kunnen komen. Dat kan hele vervelende gevolgen hebben voor de betrokkene(-n). Denk aan een verloren USB-stick met de donateursadministratie, een e-mail in de CC in plaats van de BCC of als de administratie verloren gaat door een virus. Als dat gebeurt is sprake van een datalek, en, afhankelijk van de ernst en de te verwachten gevolgen voor de betrokkenen, moet deze worden gemeld bij de Autoriteit Persoonsgegevens.
Bepaal eerst of er sprake is van een datalek: gaat het om persoonsgegevens, is daarmee iets gebeurt wat niet de bedoeling was en is één van uw technische of organisatorische maatregelen (al dan niet per ongeluk) omzeild? De AVG vereist dat elk datalek, hoe klein

ook, intern wordt geregistreerd. Daar kan je van leren. Als het lek naar verwachting risico's oplevert voor de betrokkenen moet het lek ook worden gemeld bij de Autoriteit Persoonsgegevens (dat kan hier). De AP kan contact met u opnemen voor nader onderzoek. Als het een ernstig lek is kan de AP een waarschuwing of zelfs een boete uitdelen. Als de risico's groot zijn voor betrokkenen moeten deze ook op de hoogte worden gesteld. Denk aan de verloren donateursadministratie: als daar naast NAW-gegevens ook geboortedatum en bankrekening bij zit is een kwaadwillende al een heel eind op weg voor een geslaagde poging tot identiteitsfraude. Mocht je beslissen om betrokkenen niet op de hoogte te brengen en het datalek komt alsnog uit, bedenk dan dat imagoschade vervelender kan uitpakken dan het ontvangen van een berisping of boete in het geval dat je wel de juiste acties hebt ondernomen.

Actie:

- Stel een procedure op voor het omgaan met datalekken. Win advies in van een deskundige om te bepalen of het lek serieus genoeg is om te melden. Registreer in elk geval alle incidenten. Zorg voor een klimaat waarin het maken van dergelijke fouten bespreekbaar is, vaak gebeuren dit soort zaken per ongeluk. Hou voor ogen dat het bij de meldplicht gaat om de bescherming van de privacy van de betrokkene.

Stap 9: verwerkersovereenkomsten

Als u persoonsgegevens onderbrengt bij een andere partij, bijvoorbeeld als u de administratie "in de cloud" heeft staan, of bij gebruik van Mailchimp of Google Analytics op uw website, moet u een verwerkersovereenkomst sluiten met die partij. Voor Googledrive en Gmail voorziet Google in een standaard overeenkomst (https://cloud.google.com/terms/data-processing-terms), en daarmee wordt aan de eis van een verwerkersovereenkomst. Een ander voorbeeld is dat u een website heeft uitbesteed en deze partij de gegevens die binnenkomen via het contactformulier voor u administreert en aan u doorstuurt, of aan een dienstverlener waar u uw administratie hebt uitbesteed. In een verwerkersovereenkomst regelt u hoe deze partijen omgaan met de persoonsgegevens waarvoor u verantwoordelijk bent. De ervaring leert dat aanbieders van dergelijke diensten zelf het initiatief nemen om een verwerkersovereenkomst af te sluiten, zij hebben er waarschijnlijk meer dan u. Omdat het een overeenkomst is moet deze namens uw organisatie worden getekend door iemand die daartoe bevoegd is. Het verdient de aanbeveling om u door een deskundige te laten voorlichten over de inhoud van de overeenkomst zodat u begrijpt wat wordt overeengekomen en dat u weet aan welke verplichtingen u moet voldoen. Wat in elk geval in een verwerkersovereenkomst moet zijn geregeld:

- De wederpartij wordt benoemd als verwerker
- Beschrijving van wat precies aan persoonsgegevens wordt verwerkt
- Geheimhouding en garanties
- Eventueel gebruik van sub-verwerkers
- Verbod op verwerking voor andere doeleinden door verwerker
- (Verbod op) doorgifte naar derde landen
- Hoe beveiligt de verwerker de gegevens
- Recht om audits te laten uitvoeren
- Hoe wordt omgegaan met datalekken
- Afhandeling inzageverzoeken

- Aansprakelijkheid en vrijwaring
- Duur en opzegging

Actie:

- Bij de inventarisatie van de verwerkingen geeft u aan waar de gegevens zich bevinden. Als dat een locatie is bij een andere partij moet u met deze partij een verwerkersovereenkomst afsluiten. Zorg ervoor dat u begrijpt wat deze overeenkomst inhoudt, en dat het contract wordt getekend door iemand die namens uw organisatie daartoe bevoegd is. Leg in het verwerkingenregister vast dat u een dergelijke overeenkomst heeft afgesloten.

Bijlagen:

Voorbeeld verwerkingsregister (elektronisch beschikbaar)
Voorbeeld privacyverklaring

Bronnen:
Website Autoriteit Persoonsgegevens
Handboek AVG Compliance in de Praktijk, ICTRecht, 2018
De Algemene Verordening Gegevensbescherming, ICTRecht, 2018