LANDSCHAP ERFGOED UTRECHT

Is uw landschaps- of erfgoedorganisatie of vrijwilligersgroep/-organisatie al AVG bestendig?

Sinds 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). In de gehele Europese Unie geldt dezelfde privacywetgeving. De AVG zorgt onder meer voor versterking en uitbreiding van privacyrechten, meer verantwoordelijkheden voor organisaties, bevoegdheden van Europese privacy toezichthouders zoals het kunnen opleggen van boetes.
Wat dit in de praktijk betekent voor maatregelen die u inmiddels genomen dient te hebben m.b.t. de privacy van bijvoorbeeld bezoekers, klanten, eigen medewerkers en uw vrijwilligers staat hieronder.

Maak je vrijwilligersgroep of organisatie AVG bestendig
De AVG is van toepassing voor alle organisaties die gegevens van personen in een bestand bewaren, en dus ook voor vrijwilligersgroepen. Dit betekent dat zowel digitale als papieren bestanden met persoonsgegevens zo opgeborgen moeten zijn dat ze niet toegankelijk zijn voor daartoe bevoegden. Gegevens zoals mailadressen mogen alleen bewaard worden als ze een functie hebben in de uitvoering van het werk zoals bijvoorbeeld het versturen van een nieuwsbrief.

Denk na over het volgende:
welke persoonsgegevens (zie hieronder) worden verzameld en welke informatie wordt vastgelegd?
waar worden de gegevens bewaard en wie heeft toegang?
is de opgeslagen informatie functioneel voor het doel van uw organisatie?
bewaar en gebruik alleen persoonsgegevens die nodig zijn voor het doel van uw organisatie of voor het specifieke doel waarvoor ze verzameld zijn. Is het bijvoorbeeld nog nodig om de adresgegevens van uw leden te bewaren als u uitsluitend nog per mail of sociale media met ze communiceert? Hoe minder informatie er over personen wordt opgeslagen, hoe minder kans op schending van de privacy!

Wat zijn (bijzondere) persoonsgegevens?
Voor de hand liggende persoonsgegevens zijn iemands naam, adres en woonplaats. Ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras, godsdienst, gezondheid of strafrechtelijke informatie worden bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd.
Deze gegevens mogen alleen worden bewaard als er een wettelijke uitzondering is. Automatisch opslaan in een bestand is niet toegestaan. Voor activiteiten waarvoor deze gegevens van belang zijn moet iedere keer navraag gedaan worden bij de betreffende persoon.

Laat weten wat u bewaart
Laat aan uw medewerkers, vrijwilligers, klanten, relaties etc. weten wat u bewaart aan persoonsgegevens en hoe dit aansluit bij het doel van uw organisatie of project. U kunt de volgende stappen doorlopen:

- Wat voor organisatie bent u?
- Welk doel heeft uw organisatie?
- Welke persoonsgegevens wilt u vastleggen en waarom is dat nodig in relatie tot het doel?

Voorbeeld: Uw historische vereniging heeft als doel het onderzoeken en presenteren van de geschiedenis van dorp X. U bent financieel afhankelijk van leden. Bij uw vereniging is het vastleggen van persoonsgegevens noodzakelijk voor de administratie van het lidmaatschap en om deel te nemen aan de activiteiten.

Hoe lang bewaren?
Voor elk doel waarvoor u persoonsgegevens bewaart, kunt u zelf een bewaartermijn bepalen. U mag de termijnen zelf vaststellen. Maar u moet wel kunnen beargumenteren hoe lang u deze gegevens bewaart.
Is de bewaartermijn verlopen? Dan moet u de persoonsgegevens vernietigen of anonimiseren. Of eerder, als een persoon bezwaar maakt of zijn toestemming intrekt.

Is er wetgeving van toepassing die bepaalde bewaartermijnen voorschrijft? Dan moet u deze termijnen hanteren. Bijvoorbeeld: de belastingwetgeving zegt dat u uw bepaalde gegevens 7 jaar moet bewaren.

Verwerkt u persoonsgegevens voor het algemeen belang, voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden? Dan mag u persoonsgegevens langer bewaren dan noodzakelijk is voor het oorspronkelijke doel van uw verwerking.

Vastleggen van en omgaan met persoonsgegevens
Organisaties en vrijwilligersgroepen hebben een verantwoordingsplicht in de AVG. Dat betekent dat procedures moeten worden opgesteld over:

- wie is verantwoordelijk voor de opgeslagen persoonsgegevens? Er kan vrijwillig een coördinator gegevensbescherming aangewezen worden.
- soms kan een functionaris gegevensbescherming (FG) noodzakelijk zijn. Die kan intern aangewezen worden of extern ingehuurd.
- maak een zogenaamd verwerkingsregister aan waarin u aantoont wie binnen uw organisatie welke gegevens verwerkt. Op internet zijn vele voorbeelden te vinden van verwerkingsregisters.
- aan wie en voor welk doel wordt informatie in de vorm van persoonsgegevens verstrekt?
- op welke computer zijn/worden de persoonsgegevens opgeslagen, voor welk doel en hoe lang? (bij voorkeur 1 computer en in geval van een netwerk eventueel beveiligd via toegangscode/-wachtwoord)
- hoe is de automatisering beschermd tegen virussen en hacken?
- welke afspraken zijn nodig met externe gebruikers van bestanden (drukkers, verspreiders nieuwsbrieven, koepelorganisaties) en over vernietigen van gegevens na gebruik en zijn verwerkersovereenkomsten nodig? (zie hieronder)
- plaats een privacyverklaring (zie hieronder) op uw website waarin u beschrijft hoe en met welk doel u persoonsgegevens vastlegt, welke maatregelen u getroffen heeft om die te beschermen, welke bewaartermijnen u hanteert en hoe een klant/relatie/lid etc. inzage kan krijgen in de over hem/haar vastgelegde informatie.

Wat is een verwerkersovereenkomst?
Als uw organisatie persoonsgegevens uitbesteedt aan een derde partij voor specifieke doeleinden (bijv. voor een mailing of verzending van een tijdschrift die extern verwerkt wordt), dan moet er volgens de AVG een verwerkersovereenkomst worden opgesteld. In de verwerkersovereenkomst moet worden omschreven wat de exacte afspraken zijn tussen de verwerkingsverantwoordelijke (uw organisatie) en een verwerker (de derde partij). Is dit niet op een juiste manier vastgelegd, dan riskeren beide partijen een boete en is de verwerker aansprakelijk voor mogelijke schade die kan ontstaan.

Wat staat er in een verwerkersovereenkomst?
De navolgende zaken dienen o.a. te worden vastgelegd:

- het onderwerp van de verwerking
- de duur van de verwerking
- de aard van de verwerking
- het doel van de verwerking
- het soort persoonsgegevens die worden opgeslagen
- de manier waarop omgegaan moet worden met een lek van persoonsgegevens
- meer informatie over de rechten en plichten van uw organisatie als verwerkingsverantwoordelijke

- opnemen dat de verwerker de persoonsgegevens niet voor andere doeleinden gebruikt.

Wat houdt een privacyverklaring in?
Als organisatie, vereniging of als vrijwilligersgroep is het opstellen van een privacyverklaring de meest voorkomende en handige manier te voldoen aan de verplichting informatie te verschaffen over wat er gebeurt met de persoonsgegevens die worden verzameld.
Voor uw website, applicatie of webshop kunt u in een privacyverklaring informeren aan uw relaties hoe u met de persoonsgegevens omgaat.
Als u offline of online via een website of app persoonsgegevens verzamelt, bijvoorbeeld via een contactformulier, bestelformulier, bel-me-terug formulier of inschrijfformulier dan bent u verplicht om uw klanten of bezoekers van uw website te informeren over de wijze waarop u omgaat met de verkregen persoonsgegevens. Ook als bezoekers zich kunnen inschrijven voor een nieuwsbrief moet er informatie gegeven worden wat er gebeurt met de ingevulde persoonsgegevens. Een webwinkel is altijd verplicht om een privacyverklaring o.i.d. te publiceren, want deze verzamelt altijd persoonsgegevens op het moment dat een klant een bestelling plaatst.

Wat staat er in een privacyverklaring?
Het volgende kan worden opgenomen:
- bedrijfsgegevens van het bedrijf dat de gegevens verwerkt (bij uitbesteding)
- een specificatie van de gegevens die verzameld worden
- het doel van de verwerking van de gegevens
- of de gegevens wel of niet met derden worden gedeeld
- of de gegevens voor commerciële doeleinden kunnen worden gebruikt
- of gebruikt wordt gemaakt van cookies
- de wijze waarop een klant of gebruiker haar/zijn gegeven kan opvragen en kan wijzigen.

(Vrijwillig)medewerkers informeren en instrueren
Om ondanks het vastleggen van alle spelregels het lekken van persoonsgegevens te voorkomen is belangrijk dat (vrijwillig) medewerkers geïnformeerd en geïnstrueerd zijn dat niet zomaar persoonsgegevens mogen worden gedeeld. Bedenk wie er verantwoordelijk is voor de naleving van de AVG. Feitelijk zijn dat alle medewerkers: zorg dat iedereen beseft dat niet zomaar gegevens mogen worden gevraagd, opgeslagen en doorgegeven aan derden. Leg vast wie het overzicht heeft, coördineert en eindverantwoordelijk: is dat de directeur, een bestuurder, een ict-verantwoordelijke, hoofd administratie, coördinator van een vrijwilligersgroep?

Stel een procedure op voor het melden van lekken van persoonsgegevens
Elke organisatie die persoonsgegevens opslaat, is verplicht lekken te melden binnen 72 uur na ontdekking. Om dit zorgvuldig te doen is het handig vooraf procedures af te spreken.
Wat is een lek? Het in handen van derden vallen van persoonsgegevens zonder toegang tot die gegevens. Een lek van persoonsgegevens kan het gevolg van een beveiligingsprobleem zijn zoals:
- uitgelekte computerbestanden
- een gestolen geprinte ledenlijst of klantgegevens
- cyberaanvallen
- verkeerd geadresseerde/verzonden e-mail
- gestolen laptops
- afgedankte, niet-schoongemaakte computers
- verloren usb-sticks .

Bij wie in de organisatie moet een lek van persoonsgegevens gemeld worden?
- wie binnen de organisatie moet geïnformeerd worden? Stel een verantwoordelijke aan.
- wie checkt wat er gelekt is?
- hoe worden de gevolgen van de lekkage in kaart gebracht voor de personen van wie persoonsgegevens gelekt zijn?

Melding is nodig bij de Autoriteit Persoonsgegevens met de volgende gegevens:
- aard van de inbreuk
- instanties of persoon waar meer informatie over de inbreuk kan worden verkregen

- aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken
- beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens
- maatregelen die de organisatie heeft genomen of voorstelt te nemen om de gevolgen te verhelpen.

Wie controleert?
In Nederland controleert de Autoriteit Persoonsgegevens of organisaties voldoen aan de AGV. De Autoriteit Persoonsgegevens kan ook boetes opleggen wanneer na waarschuwingen een organisatie het beleid rond bescherming persoonsgegevens niet verbetert.

Het volgende is specifiek van toepassing voor musea en erfgoedorganisaties

Publicaties AVG specifiek voor musea en erfgoedinstellingen:
Voor erfgoedinstellingen is er een uit het Engels vertaalde handleiding voor de toepassing van de AVG verschenen. Met dank aan onze collega's van het Erfgoedhuis Zuid-Holland en de auteur Helen Shone van Development Partners, in samenwerking met de Association of Independent Museums (AiM) Lees hem hier:
- Succesvol beheer van privacy en informatievoorschriften in kleine musea

Daarnaast zijn er nieuwe modellen verschenen voor schenkingen, bruiklenen en bezoekvoorwaarden, aangepast aan de AVG.
Model schenkingsovereenkomst
Model bruikleenovereenkomst
Model Bezoekvoorwaarden
Toelichting op de modellen

Disclaimer: Landschap Erfgoed Utrecht is in geen geval aansprakelijk door een beroep te doen op deze tekst. Twijfelt u over hoe gevoelig de data zijn die u verzamelt, dan raden wij u aan daar een jurist voor in te schakelen. Deze informatie is puur bedoeld om u te attenderen op wat er geregeld moet worden en als inspiratie om u op weg te helpen. Er kunnen geen rechten worden ontleend aan deze tekst.