ERFGOEDHUIS
ZUID·HOLLAND

Succesvol beheer van privacy-en informatievoorschriften in kleine musea

De toepassing van de Algemene Verordening Gegevensbescherming (AVG) voor erfgoedinstellingen

Erfgoedhuis Zuid-Holland
Tamara van Zwol, Saskia Boom (red.)
15 maart 2018

Inhoud

Deze gids is de Nederlandse uitgave van *Succes Guide. Successfully managing privacy and data regulations in small museums*, door Helen Shone van Development Partners, in samenwerking met de Association of Independent Museums (AiM).
Deze publicaties is vanuit het Engels naar het Nederlands vertaald en zoveel mogelijk aangepast aan de voor Nederland geldende situatie. Erfgoedhuis Zuid-Holland is niet aansprakelijk voor eventuele onvolkomenheden.

De informatie die hier wordt gegeven is gebaseerd op richtlijnen die momenteel beschikbaar zijn. Lezers moeten zich ervan bewust zijn dat verdere updates zullen worden gepubliceerd.

De voorschriften voor gegevensbescherming reiken veel verder dan hier wordt besproken en we bevelen aan om kennis te nemen van de volledige regelgeving via

www.autoriteitpersoonsgegevens.nl

Voor wie is deze gids bedoeld?

Deze gids is bedoeld voor musea en andere culturele organisaties die willen begrijpen hoe zij moeten reageren op de huidige en toekomstige regelgeving voor gegevensbescherming. Dit in aanloop naar de nieuwe Europese privacywetgeving "General Data Protection Regulation" (GDPR), in Nederland de "Algemene Verordening Gegevensbescherming" (AVG), die in werking treedt op 25 mei 2018.

Deze gids richt zich tot medewerkers en vrijwilligers die zich bezighouden met ledenwerving en –administratie, fondsenwerving en/of marketing. Het wordt daarbij aangeraden om de belangrijkste punten met alle personeelsleden en vrijwilligers in de organisatie te delen, omdat veel van hen in contact komen met het verzamelen en verwerken van gegevens. Vergeet niet dat gegevensbescherming niet alleen een kwestie van inkomstenwerving is, maar ook draait om gegevens die de organisatie verzamelt en gebruikt, van verklaringen tot mailinglijsten en vrijwilligersinformatie.

In deze gids worden de belangrijkste gegevensbeschermingskwesties beschreven om u te helpen bij het controleren van uw huidige positie en het opstellen van een actieplan. Het is bedoeld als een praktische gids die u op het juiste pad zet voor naleving van de gegevensbeschermingsvoorschriften. Er is achterin een "checklist actiepunten" opgenomen, waarin de aandachtspunten en te ondernemen maatregelen worden samengevat.

Hoe zit het met onze collecties en archieven?
Veel erfgoedorganisaties bewaren persoonlijke gegevens in hun verzameling en archieven. Voor het verwerken van persoonsgegevens zijn er een aantal uitzonderingen gemaakt in de Uitvoeringswet AVG voor instellingen die onder de Archiefwet vallen. Maar het is voor de archiefbranche nog niet helemaal duidelijk wat de precieze impact is van de AVG. Er worden daarom risicoanalyses uitgevoerd bij drie soorten archiefinstellingen, voor meer duidelijkheid. Op het moment van schrijven zijn hier nog geen resultaten van bekend.

Zie voor de Nederlandse situatie Wbg en Archiefwet:

https://www.erfgoedinspectie.nl/toezichtvelden/archieven/wet--en-regelgeving/overige-informatiewetgeving/wet-bescherming-persoonsgegevens

Waarom praten we hier nu over?

De Wet Bescherming Persoonsgegevens is sinds 2001 van kracht. Deze heeft organisaties altijd verplicht om gegevens eerlijk en verantwoordelijk te beheren. Deze verordening moet per 25 mei 2018 worden geactualiseerd en aangescherpt volgens de Algemene Verordening Gegevensbescherming (AVG), een nieuwe wet van de EU.

Recente, strengere handhavingsacties, in combinatie met een algemene verschuiving in de houding ten opzichte van persoonlijke gegevens, laten een verschuiving zien van het laissez-faire naar een tijd van grotere persoonlijke controle en organisatorische verantwoordelijkheid.

Het is belangrijk dat deze veranderingen aan de top van uw organisatie worden begrepen, maar ook stafmedewerkers en vrijwilligers moeten hierin worden meegenomen, omdat zij verantwoordelijk zijn voor de genomen beslissingen.

Organisaties moeten zich voorbereiden op de wijzigingen in de wetgeving inzake gegevensbescherming voordat de nieuwe voorschriften van kracht worden op 25 mei 2018.

Waarom verzamelt u gegevens?

In het verleden verzamelden veel organisaties gegevens gewoon omdat het mogelijk was, niet omdat ze wisten hoe en waarvoor ze deze zouden gebruiken. Een eenvoudig advies is om bewust en strategisch te zijn over de gegevens die worden verzameld. Kortom, wees duidelijk waarom u gegevens verzamelt en wat u ermee wilt doen. Maar ook; documenteer uw beslissingen. Het verantwoordingsprincipe van de AVG vereist dat organisaties kunnen aantonen hoe zij voldoen aan de regelgeving voor gegevensbescherming, wat kortweg betekent dat u uw besluitvorming moet documenteren.

Het is mogelijk dat u persoonlijke gegevens wilt verzamelen voor een breed scala aan doeleinden, met enkele van de meest voorkomende:

- Nieuwsbriefmailings
- Fondsenwervingsverzoeken
- Vrijwilligersbeheer
- Evenementen
- Gift Aid (giften aan goede doelen)

Documenteer uw beslissingen

Verzamel alleen de informatie die u nodig heeft

Volgens de nieuwe wetgeving mag u alleen gegevens verzamelen die nuttig zijn en externe informatie die niet relevant is voor uw doeleinden moet vermijden. Dit leidt ook tot minder werk voor het opschonen en beheren van gegevens.

Documenteer uw beslissingen: het verantwoordingsprincipe van de AVG vereist dat organisaties kunnen aantonen hoe zij voldoen aan de regelgeving inzake gegevensbescherming.

Gegevens die als 'gevoelig' worden geclassificeerd, mogen alleen onder strikt gecontroleerde omstandigheden worden bewaard – dit heeft betrekking op raciale of etnische afkomst, politieke opvattingen, religieuze overtuigingen, vakbondsactiviteiten, lichamelijke of geestelijke gezondheid, seksleven of bijzonderheden over strafbare feiten.

Voor het verzamelen van gevoelige gegevens moet aan een van de volgende criteria zijn voldaan:

- De persoon heeft expliciete toestemming gegeven (bijv. ze hebben u misschien verteld over een handicap en hoe dit van invloed kan zijn op een evenement)
- De persoon heeft de informatie opzettelijk openbaar gemaakt
- Om te voldoen aan de wet
- Voor medische doeleinden

- Voor het bewaken van gelijkheid van kansen

Onthoud dat iedereen het recht heeft om toegang te vragen tot de gegevens in uw bezit, dus houd het objectief en sla niets op dat uw reputatie in gevaar kan brengen. Het kan handig zijn om u voor te stellen dat de betrokkene achter u staat bij het invoeren van zijn of haar gegevens in de database.

Onthoud dat iedereen het recht heeft om toegang te vragen tot de gegevens in uw bezit

Bewaar gegevens alleen als u ze nodig heeft

Sta niet toe dat persoonlijke gegevens oneindig worden bewaard. Het is verleidelijk om de gegevens vast te houden 'voor het geval dat' het nuttig is, maar naarmate de informatie ouder wordt, wordt het minder een voordeel en meer een risico. Naarmate de tijd verstrijkt, wordt het moeilijker om ervoor te zorgen dat de informatie juist is, waardoor het risico dat verouderde informatie ten onrechte wordt gebruikt, groter wordt. Het vasthouden aan oude gegevens verhoogt ook de datadruk: het moet nog steeds veilig worden bewaard, ondanks het feit dat het niet nuttig is, en de organisatie moet reageren op verzoeken om inzage van de betrokkene, ook al is de informatie niet gebruikt.

Er is geen absoluut tijdschema, maar gezegd wordt dat 'persoonsgegevens niet langer worden bewaard dan nodig is'. U moet dus uw eigen interne regels opstellen over hoe lang dit zou moeten zijn. Het heeft waarschijnlijk weinig zin om gegevens te bewaren die al vele jaren niet gebruikt zijn.

Houd er rekening mee dat er mogelijk informatie is die voor een lange periode nodig is om wettelijke of rapportageredenen. In voorkomende gevallen is het volledig acceptabel om een basisdossier aan te leggen dat bepaalde datavelden langer actief houdt dan andere overtollige details.

Nadat u uw interne regels hebt opgesteld, moet dit worden gedocumenteerd in een eenvoudig beleid voor gegevensopslag en een systeem dat is ingesteld om te zorgen dat het wordt geïmplementeerd. In eerste instantie kan het een uitdaging zijn om oude gegevens (die zich in papieren bestanden bevinden, evenals spreadsheets en databases) te identificeren en te verwijderen, maar een eenmalige inspanning om de organisatie tot een verstandige positie voor gegevensbehoud te brengen, zal op langere termijn vruchten afwerpen.

Vergeet niet dat iedereen het recht heeft om toegang te vragen tot de gegevens in uw bezit.

Hoe verzamelt en bewaart u gegevens?

De volgende stap in uw data-audit is om te bepalen hoe u uw gegevens verzamelt en hoe u deze opslaat.

Waar zijn uw inzamelpunten?

De meeste organisaties verzamelen gegevens uit een aantal verschillende bronnen. Deze contactmomenten kunnen zijn:

- Bezoekersontvangst
- Online schenkingen
- Vriendengroep
- Aanmelden voor nieuwsbrief
- Giftengegevens
- Evenementen
- Commerciële verhuur
- Retail
- Vrijwilligersbeheersystemen

Organisaties moeten consistent zijn in hun benadering van het verkrijgen van toestemming, waar deze ook wordt verzameld. Dit is belangrijk voor de ervaring van uw achterban, maar nog meer voor backofficesystemen die uw activiteiten ondersteunen – het is erg moeilijk om goede gegevens betreffende toestemmingen te onderhouden als u verschillende vragen op verschillende plaatsen stelt.

Denk goed na over de verschillende plaatsen waar u gegevens verzamelt en overweeg of de aanpak om toestemming te krijgen gestroomlijnd is. Het maakt niet uit of de systemen op papier zijn gebaseerd op een gedeelte van de site en elektronisch in een ander deel, maar de belangrijkste toestemmingsverklaring en opties moeten op elkaar worden afgestemd.

Meer informatie over toestemming vindt u in de onderstaande secties.

Organisaties moeten consistent zijn in hun benadering van het verkrijgen van toestemming, waar deze ook wordt verzameld

Hoe bewaart u uw gegevens?

Belangrijk bij het bewaren van gegevens is in de eerste plaats dat de gegevens goed beveiligd zijn. Kortom: de gegevensopslag en de verwerkingsprocedures moeten veilig zijn.

Databases hebben de neiging om veiliger te zijn dan papieren systemen en spreadsheets. Ze zijn onafhankelijk van de belangrijkste gedeelde documenten van een computernetwerk en vereisen wachtwoorden om in te loggen. Gewoonlijk is de toegang tot een database beperkt tot degenen die het nodig hebben.

Risicogebieden van werken met een database zijn (maar zijn niet beperkt tot):

- een groot aantal mensen die toegang hebben tot de database;
- een gebrek aan een geschikt back-upproces;
- gegevensrapporten worden gedownload naar een gedeelde schijf van de hoofdcomputer, waar iedereen er toegang toe heeft.

Verdere aandachtspunten van een database zijn:

- De beveiliging moet periodiek worden herzien om het risico van een datalek te verminderen.
- Organisaties moeten consistent zijn in hun benadering voor het verkrijgen van toestemming, waar deze ook wordt verzameld,

Het is geen vereiste om een database te hebben om uw gegevens te beheren – een op papier of spreadsheet gebaseerd systeem is prima als dit in verhouding staat tot de hoeveelheid gegevens die u bewaart en verwerkt. Maar de veiligheid van deze systemen moet ook regelmatig worden herzien en er moeten procedures worden opgesteld om elk beveiligingsrisico te beperken. U moet uw besluitvorming en acties documenteren.

Als onderdeel van uw gegevensbeveiligingsaudit moet u kijken naar de reis die uw gegevens afleggen. Als u rechtstreeks in een database invoert, dan is het een zeer korte afstand, maar niet alle systemen zijn zo geavanceerd. Een voorbeeldscenario in een klein museum kan als volgt zijn:

Bezoekers dienen bij aankomst een papieren formulier in te vullen bij de receptie. Het formulier wordt doorgegeven aan een administratief personeelslid of vrijwilliger die de gegevens in een spreadsheet plaatst.

Als onderdeel van uw gegevensbeveiligingsaudit moet u kijken naar de reis die uw gegevens afleggen

Risicopunten van deze procedure kunnen zijn:

- Het formulier wordt onbeheerd achtergelaten bij de receptie.
- Het formulier wordt niet vernietigd of op de juiste wijze opgeslagen nadat de informatie in de gegevensspreadsheet is geplaatst.
- De gegevensspreadsheet is toegankelijk voor alle medewerkers en vrijwilligers die toegang hebben tot het gedeelde computernetwerk.

Alle bovenstaande situaties kunnen ertoe leiden dat informatie in handen komt van mensen binnen of buiten de organisatie die geen recht op toegang te hebben.

Deze risico's kunnen worden verminderd door:

- Een afsluitbare lade bij de receptie om formulieren in te bewaren wanneer de receptie niet wordt bemand.
- Er wordt een versnippersysteem geïmplementeerd voor formulieren die zijn verwerkt.
- De gegevensspreadsheet of het relevante gedeelte van het computernetwerk is beveiligd met een wachtwoord, en alleen de juiste mensen hebben toegang.

Het opslaan van toestemmingsgegevens

Naast een goede beveiliging van de gegevens, vereist de AVG ook de mogelijkheid om toestemmingsinformatie op te slaan op de manier die de AVG voorschrijft.

De nieuwe regels voor gegevensbescherming vertegenwoordigd door de AVG vereisen dat organisaties meer informatie verzamelen en opnemen met betrekking tot toestemming. Aangezien de nieuwe regels stellen dat niet mag worden aangenomen dat de toestemming voor altijd kan worden verleend, vereisen ze dat organisaties de datum vastleggen waarop toestemming is gegeven. Als iemand uit uw achterban vervolgens voor 'opt-out' kiest, zal het ook noodzakelijk zijn om de datum hiervan te registreren. De regels vereisen ook dat organisaties hun achterban de mogelijkheid biedt om zich aan te melden voor verschillende communicatiekanalen, zoals post, e-mail, telefoon en sms.

Zoals u zich kunt voorstellen, vereist de combinatie van deze voorschriften een groot aantal nieuwe velden in uw databases of kolommen in de spreadsheets. Tot op heden zijn de meeste databases niet automatisch geconfigureerd om deze nieuwe vereisten te ondersteunen en dus moet er een alternatief worden gevonden, met behulp van velden die u kunt 'bevragen' of zo nodig kunt doorzoeken. Dit systeem moet uiterlijk in mei 2018 klaar zijn voor gebruik wanneer de AVG van kracht wordt.

Wanneer heeft u toestemming nodig?

Gegevensverwerking heeft niet alleen betrekking op de communicatie die u verzendt, maar ook op het scala aan manieren waarop u persoonlijke gegevens kunt gebruiken, van analyse van bezoekersstatistieken tot vermogensscreening. Sommige van deze activiteiten worden als 'opdringeriger' beschouwd, daarom is er een grotere instemmingsverplichting nodig om ze uit te voeren. Andere activiteiten kunnen worden uitgevoerd op basis van 'gerechtvaardigd belang', zoals hieronder beschreven.

Gerechtvaardigd belang: Wat is dit precies?

Gerechtvaardigd belang is de alternatieve wettelijke basis voor instellingen om bepaalde soorten gegevensverwerking uit te voeren. Organisaties moeten hun belangen om persoonsgegevens te verwerken om hun doelstellingen te bereiken afwegen tegen de rechten van het individu. De uitkomst van deze afwegingstest bepaalt of persoonlijke gegevens kunnen worden verwerkt zonder toestemming nodig te hebben.

Met betrekking tot direct marketing per post en telefoon (e-mail en sms vereisen altijd toestemming), vereist de verordening dat organisaties rekening houden met de 'redelijke verwachtingen' van individuen op basis van hun relatie met u. Als de personen in kwestie geen relatie met u hebben en verrast zouden zijn als ze een mailing ontvangen, dan is het waarschijnlijk dat de evenwichtsoefening niet in uw voordeel is. Daarnaast moet u rekening houden met de frequentie van de mailings die u verzendt – de betrokken personen vinden bijvoorbeeld dat maandelijkse mailings onredelijk zijn, maar zullen graag een jaarlijkse update ontvangen.

Wanneer u op gerechtvaardigd belang vertrouwt als basis voor een mailing, moet u altijd een duidelijke en eenvoudige stap voor het afmelden voor toekomstige directe mailings aangeven. En vergeet niet dat als iemand zich heeft afgemeld, de regel van het gerechtvaardigde belang niet kan worden gebruikt, zodat u dus een manier moet vinden om ze uit te sluiten van uw toekomstige mailings.

In het kader van de AVG kunnen overheidsinstanties (waaronder musea van lokale overheden) niet meer op gerechtvaardigd belang vertrouwen als rechtsgrond voor gegevensverwerking zonder toestemming. In plaats daarvan moeten zij kunnen aantonen dat 'de verwerking noodzakelijk is voor de uitvoering van een taak die wordt uitgevoerd in het openbaar belang' of 'voor de uitvoering van een contract met de betrokkene'.

Gegevensverwerkingswerkzaamheden: Toestemming versus Gerechtvaardigd Belang

Uitvoering van een contract/ servicecommunicatie[1]

Wanneer iemand evenementtickets koopt of iets uit uw online winkel bestelt, verwachten zij een bevestiging te ontvangen op dezelfde manier als waarop zij de transactie hebben gedaan, dat wil zeggen per e-mail indien verzonden per e-mail of online ingediend, of per post indien verzonden per post. Dit type bevestiging wordt niet als een directe marketingactiviteit aangemerkt en kan zonder toestemming plaatsvinden.

Direct marketing

Alle mailings die de doelstellingen van een organisatie bevorderen, worden als direct marketing beschouwd. Dit omvat ook op maat gemaakte brieven, wat verrassend kan zijn, omdat we denken dat direct marketing iets is dat naar grote aantallen mensen wordt gestuurd. Het betekent dat in bijna alle vormen van communicatie met de achterban er toestemming nodig is of (voor mailings per post) de regel van het gerechtvaardigd belang.

Vermogensscreening en onderzoek

Vermogensscreening (de praktijk van het analyseren van gegevens om de capaciteit van een persoon om te doneren in te schatten) en individuele onderzoeksprofielen worden door het ICO[2] beschouwd als indringende gegevensverwerkingsactiviteiten. Ze zijn niet illegaal, maar vereisen toestemming. Het is belangrijk dat deze activiteiten niet verborgen zijn in het privacybeleid onder onduidelijke termen zoals 'onderzoek', wat een aantal verschillende activiteiten zou kunnen betekenen.

[1] Dit geldt alleen voor bestaande klanten. Iemand is een bestaande klant als deze persoon een product of dienst van u heeft gekocht. Er moet sprake zijn van een koopovereenkomst, waarin u verplicht bent of was om iets te leveren en de klant om daarvoor te betalen. Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg?qa=marketing&scrollto=1

[2] De ICO in het Verenigd Koninkrijk is vergelijkbaar met de Autoriteit Persoonsgegevens in Nederland

Het delen van gegevens

U heeft toestemming nodig om gegevens extern te delen – dit kan met een postvoorbereider zijn, een vermogensscreeningbureau of (hoewel af te raden) een andere organisatie voor eigen gebruik. De manieren van delen moeten duidelijk worden omschreven in het privacybeleid. Het delen van gegevens moet altijd worden uitgevoerd met een contract omdat u de verantwoordelijkheid behoudt voor wat de externe organisatie met de gegevens doet. U moet hun gegevensbeschermingsreferenties controleren en ervoor zorgen dat ze op het vereiste niveau zijn voordat u gegevens met hen deelt.

Uw gegevens aan een andere instelling geven voor hun eigen gebruik moet worden vermeden. Een voorbeeld hiervan is een lokale organisatie die uw mailinglijst wil gebruiken om informatie over hun activiteiten rechtstreeks naar uw achterban te sturen.

Uw gegevens aan een andere instelling geven voor hun eigen gebruik moet worden vermeden

De Autoriteit Persoonsgegevens geeft aan:

Wilt u de persoonsgegevens aan derde partijen verstrekken ? Dan moet u mensen goed informeren over welke categorieën derde partijen dat zijn. Ook moet u apart toestemming vragen voor deze verstrekking aan genoemde soorten derde partijen. Dit geldt ook als u reclame van derde partijen aan uw klanten wilt sturen.

Als deze activiteit iets is dat u niet kunt vermijden, moet de manier van delen expliciet en ondubbelzinnig worden beschreven in het privacybeleid, bij voorkeur met de naam van de ontvangende organisatie. Maar waar mogelijk, vermijd dit gewoon helemaal.

Werknemersbestanden

Deze gegevens kunnen worden verwerkt onder de gerechtvaardigde belangenregel[3]. Dit belang moet rechtmatig, voldoende duidelijk verwoord en ook echt aanwezig zijn. Dat is zo wanneer een verwerking aantoonbaar noodzakelijk is om uw bedrijfsactiviteiten te verrichten. Bijvoorbeeld het voeren van een personeelsadministratie.

Uw gegevens aan een andere instelling geven voor hun eigen gebruik moet worden vermeden.

[3] Meer informatie over het gerechtvaardigd belang vindt u op de website van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-gerechtvaardigd-belang-6330

Lidmaatschap/Vrienden

Wanneer mensen zich aanmelden voor een lidmaatschap of een Vriendenvereniging, geven zij automatisch hun contactgegevens. Als hun gegevens uitsluitend voor het lidmaatschapsplan zijn vastgelegd, zonder een algemene opt-in-aanvraag, beperkt u uw gegevensverwerkingsactiviteiten waarvoor u toestemming hebt tot de welke verenigbaar zijn met het lidmaatschap. Omdat deze mensen echter duidelijk betrokken zijn bij het museum, kunt u mogelijk het gerechtvaardigd belang gebruiken voor nietlidmaatschapsgerelateerde communicatie per post.

Een van de genoemde voordelen van een lidmaatschap of vriendenvereniging is meestal een tijdschrift of nieuwsbrief, en dit valt onder 'uitvoering van een contract'. Dit kan per e-mail worden verzonden (als ze u hun e-mailadres hebben gegeven als onderdeel van de aanmelding) of per post. De inhoud van deze nieuwsbrief is echter een grijs gebied. Zou de ontvanger redelijkerwijs verwachten dat dit ook inzamelingsacties voor fondsenwerving omvat? Als leden zich hebben aangemeld voor een brede toestemmingsverklaring met een link naar het privacybeleid, dan hoeft dit geen reden tot bezorgdheid te geven.

Als uw Vriendenvereniging wordt beheerd door een afzonderlijke instelling, kunnen zij de gegevens niet zonder toestemming delen met het (hoofd)museum. Deze afzonderlijke instelling moet zich houden aan de voorschriften voor gegevensbescherming en een eigen privacybeleid hebben.

Activiteit	Toestemming nodig		Gerechtvaardigd belang
	Nee	Ja	
Uitvoering van een contract – dwz. bevestiging van een bestelling of evenemententicket	V		V
Analyse van samengevoegde gegevens, bijvoorbeeld bezoekersstatistieken, bezoekers van evenementen of fondsenwerving	V		V
Werknemers- en vrijwilligersbestanden	V		V
Direct marketing per post of telefoon	V		V
Schenking bedankbrief	V	V	V
Direct marketing via e-mail, sms, geautomatiseerde telefoongesprekken		V	
Gedetailleerde onderzoeksprofielen, intern gecreëerd of extern geproduceerd		V	
Vermogensscreening		V	
Gegevens delen		V	

Een voorbeeld
Voor een Vrienden- of lidmaatschapsplan dat deel uitmaakt van het museum of de erfgoedorganisatie: het is aan te raden om een algemene toestemmingsverklaring te hebben die andere mailings van het museum omvat, en een link naar het privacybeleid. Toestemming voor post/e-mail moet in deze verklaring opgenomen zijn zodat u vervolgens de contactvoorkeuren van de leden dienovereenkomstig kunt vastleggen.

Als u mensen vraagt zich af te melden in plaats van zich aan te melden, heeft u geen toestemming zoals gedefinieerd door de AVG en moet elke gegevensverwerking op basis van 'gerechtvaardigd belang' plaatsvinden. U zult niet kunnen e-mailen behalve om aan de verwachtingen van de lidmaatschapsvoordelen te voldoen, bijvoorbeeld als uw ledennieuwsbrief per e-mail wordt verzonden.

Als de Vriendenvereniging een afzonderlijke instelling is, moet de Vriendenorganisatie duidelijk maken dat ze apart staat van het museum wanneer ze nieuwe leden inschrijven. Als zij de gegevens met het museum willen delen, moet dit expliciet worden vermeld in een opt-in-toestemmingsverklaring; u mag geen gegevens delen via een opt-out of gerechtvaardigde belangen.

Als de Vriendenvereniging bij aanmelding niet duidelijk heeft gemaakt dat ze de gegevens met het museum zullen delen, kunnen ze dit niet doen. Om gegevens met het museum te delen, moeten ze ofwel toestemming krijgen van elk individu, ofwel een mail sturen waarmee mensen kunnen doorklikken naar een rechtstreekse aanmelding bij het museum.

Voor bestaande Vrienden moet u de toestemming die u al hebt herzien en beslissen of deze voldoende is om aan de AVG-vereisten te voldoen – zie het gedeelte over historische gegevens hieronder.

Op welk moment moet toestemming verkregen worden?

Het ICO en de Fundraising Regulator[4] adviseren dat toestemming om gegevens te bewaren en te verwerken wordt verkregen wanneer de gegevens voor het eerst worden verzameld. Dit wordt normaal bereikt door de combinatie van een toestemmingsverklaring (die de hoofdpunten geeft) en een privacyverklaring (die de details geeft). Samen moeten deze twee verklaringen betrekking hebben op al uw gegevensverwerkingsactiviteiten.

De Autoriteit Persoongegevens geeft aan:

Verwerkt u persoonsgegevens die gebaseerd is op toestemming van de betrokken personen? Dan moet u onder de (AVG) kunnen laten zien dat u die toestemming daadwerkelijk heeft. Twee van de eisen die de AVG stelt aan 'toestemming' zijn dat deze 'geïnformeerd' en 'specifiek' gegeven is. Om geldige toestemming aan te tonen is het dan ook essentieel dat u kunt laten zien op basis van welke informatie de betrokken personen de toestemming hebben gegeven. Het is dus onvoldoende om alleen de toestemming zelf vast te leggen.

Wanneer het niet mogelijk is om toestemming te verkrijgen op het punt van gegevensverzameling, dan moet dit bij de eerste beschikbare gelegenheid gebeuren, zoals de eerste keer dat u contact met hen opneemt. Het wordt onaanvaardbaar geacht om zonder toestemming namen en adressen te bewaren, alleen omdat u ze niet gebruikt.

Opt-in versus opt-out

In het kader van de DPA[5] was het acceptabel om van de achterban te verlangen dat ze zich afmelden ('opt-out') voor verschillende vormen van gegevensverwerking, zoals aan een mailinglijst toegevoegd te worden, in plaats van zich aan te melden ('opt-in'). Gewoonlijk zou er een verklaring zijn die iets zegt in de trant van het volgende: 'Als u niet wilt dat wij u verdere informatie over onze activiteiten sturen, vink dan het vakje aan.''

De regels voor e-mail, sms en geautomatiseerde telefoontjes zijn sinds 2003 anders dan die van andere vormen van communicatie, toen afzonderlijke wetgeving (PECR[6]) toestemming vereiste om op een opt-in basis te mogen gebeuren. Sinds 2003 hebben we dus 'opt-outs' voor post, normale telefoontjes en andere gebieden voor gegevensverwerking en 'opt-ins' voor e-mail, sms en geautomatiseerde telefoontjes.

Onder de AVG moet toestemming worden verleend voor alle vormen van gegevensverwerking en communicatie.

[4] https://www.fundraisingregulator.org.uk/
[5] Data Protection Act. Dit is de huidige privacywet (tot 25 mei 2018) in het Verenigd Koninkrijk.
[6] Privacy and Electronic Communications Regulations

De nieuwe vereiste is dat toestemming vrijelijk, specifiek, geïnformeerd en ondubbelzinnig moet zijn. Individuen moeten een proactieve keuze laten zien; toestemming kan niet worden aangenomen uit vooraf aangevinkte vakjes of inactiviteit. Informatie over gegevensverwerking moet op een dusdanige manier worden uitgelegd die mensen gemakkelijk kunnen begrijpen, en niet verborgen in jargon of ambiguïteit. Individuen moeten de mogelijkheid hebben om zich aan te melden ('opt-in') voor verschillende communicatiekanalen (post, e-mail, enz.), in plaats van van hen te verwachten dat ze zich in één keer voor alles aanmelden.[7]

Hoe moet een toestemmingsverklaring eruitzien?

De toestemmingsverklaring moet mensen de basis vertellen over wat u met hun gegevens gaat doen en een link bevatten naar het meer gedetailleerde privacybeleid. Het moet zo kort zijn dat mensen het kunnen lezen en begrijpen, maar lang genoeg om zinvol te zijn. Gebruik niet meer formele taal dan gewoonlijk – het is veel beter om dezelfde toon te gebruiken als in uw andere communicatie. En aangezien u mensen vraagt om zich pro-actief aan te melden ('opt-in'), is het een idee om innemend over te komen zodat ze zich willen aanmelden. Gebruik iets inspirends en unieks. Het is een goede gewoonte om mensen eraan te herinneren dat ze zich op elk gewenst moment kunnen afmelden ('opt-out').

- Gebruik uw huisstijl
- Wees interessant, innemend
- Bied verschillende communicatiekanalen aan, niet alleen een enkele JA/NEE keuze
- Wees consistent in alle gegevensverzamelinglocaties en -mediums
- Zorg ervoor dat uw tekst niet dubbelzinnig is
- Herinner mensen eraan dat ze zich later kunnen afmelden ('opt-out')
- Geef een link naar uw privacybeleid

[7] Zie ook Handleiding Algemene Verordening gegevensbescherming, hoofdstuk 4.3.1.: Toestemming kan blijken uit een ondubbelzinnige wilsuiting of uit een ondubbelzinnige, actieve handeling van de betrokkene. Vaak wordt hiervoor de term *opt in* gehanteerd. *Opt out* – het gebruik maken van de optie om je van toestemming te onthouden – is geen toestemming. Wanneer de betrokkene bijvoorbeeld een vinkje zet in een vakje om zijn akkoord aan te geven, dan is er sprake van ondubbelzinnige toestemming (*opt in*). Wanneer echter hetzelfde vakje al aangekruist is en de betrokkene vinkt het niet uit (*opt out*), dan is er geen ondubbelzinnige toestemming tot stand gekomen.

Toestemmingsverklaring: een basisvoorbeeld
We houden u graag op de hoogte van het laatste nieuws, activiteiten en acties voor fondsenwerving. U kunt u op elk gewenst moment daarvoor afmelden. Als u ermee akkoord gaat om gecontacteerd te worden, vink dan de volgende vakjes aan:

- Post
- E-mail
- Telefoon
- Sms

Volledige details over hoe we op de gegevens van onze achterban letten, zijn beschikbaar in ons privacybeleid.

Toestemming hoeft niet te worden gegeven via een selectievakje of een schriftelijke verklaring. Het kan mondeling zijn of via een andere handeling waaruit de wens van een individu blijkt om zich aan te melden ('opt-in') – bijvoorbeeld een visitekaartje dat in een doos wordt gedaan wanneer heel duidelijk wordt gemaakt waarvoor het kaartje zal worden gebruikt. Maar als de toestemming niet geschreven is, kunt u dit het beste schriftelijk bevestigen en een link naar het privacybeleid geven.

Wat is een privacystatement of privacyverklaring?

Het privacybeleid (soms een privacyverklaring of privacystatement genoemd) is waarschijnlijk uw belangrijkste document met betrekking tot gegevensbescherming. Ondanks het feit dat het een langetermijnvereiste is onder de dataregelgeving, hebben veel kleine organisaties er nog steeds geen. Dit kan snel en eenvoudig worden verholpen en moet zo snel mogelijk worden gedaan door organisaties die zich in deze positie bevinden.

Het privacybeleid moet een duidelijke uitleg zijn van wie u bent en wat u gaat doen met de persoonsgegevens. Het moet al uw huidige gegevensverwerkingsactiviteiten omvatten en pogen om uw toekomstige gegevensverwerkingsbehoeften toekomstbestendig te doen zijn, anders bestaat het risico dat u ergens in de toekomst niet in staat zult zijn iets belangrijks te doen.

Een voorbeeld van een privacyverklaring is die van Scouting Nederland[8]:

https://www.scouting.nl/privacy

Het is acceptabel om het privacybeleid te updaten zolang dit gemakkelijk toegankelijk is, maar als er een grote verandering is, is het noodzakelijk om dit actief onder de aandacht van uw achterban te brengen.

Het is acceptabel om het privacybeleid te updaten zolang dit gemakkelijk toegankelijk is, maar als er een grote verandering is, is het noodzakelijk om dit actief onder de aandacht van uw achterban te brengen.

[8] Op het moment van publicatie van deze handleiding zijn deze uitspraken mogelijk niet bijgewerkt om aan alle nieuwe AVG-vereisten te voldoen.

Wat moet onder een privacyverklaring vallen?

In zekere zin zou dit een samenvatting moeten zijn van alles wat we in dit document hebben besproken. Vergeet niet dat u specifiek, duidelijk en ondubbelzinnig moet zijn in het beschrijven van uw gegevensverwerkingsactiviteiten. Het moet voor niet-gespecialiseerde doelgroepen gemakkelijk zijn om te begrijpen wat u met hun gegevens gaat doen. Het is algemeen gebruikelijk om waar nodig in gewone taal te schrijven, waarbij een hele alinea wordt gebruikt om een gebied van gegevensverwerking uit te leggen als dit de beste manier is om dubbelzinnigheid te voorkomen. U kunt ook een lijst met opsommingspunten hebben als dit de beste manier lijkt om uw informatie over te brengen, maar vergeet niet dat duidelijkheid belangrijker is dan bondigheid. Te gebruiken koppen, waar relevant, zijn:

- Wie u bent, inclusief het adres en registratienummer van de instelling
- Welke persoonlijke gegevens u verzamelt
- Wat u gaat doen met de gegevens, bijvoorbeelden:
    - ✓ Mailings met betrekking tot nieuws en evenementen
    - ✓ Fondsenwervingsverzoeken
    - ✓ Onderzoek (wees specifiek over het type onderzoek dat u zult uitvoeren)
    - ✓ Vermogensscreening (leg uit wat dit is en hoe u dat gaat doen)
    - ✓ Samengevoegde data-analyse, waaronder monitoring van bezoekersstatistieken of de effectiviteit van communicatie, inclusief het volgen van e-mails
    - ✓ Gegevens delen - met wie u deze deelt en voor welke doeleinden
- Cookies op uw website
- Hoe u de gegevens opslaat en veilig houdt
- Hoe mensen een 'Subject Access Request' (inzageverzoek van de betrokkene) kunnen indienen'
- Een verklaring met betrekking tot updates van uw privacybeleid: 'We
- evalueren regelmatig ons privacybeleid en kunnen van tijd tot tijd wijzigingen aanbrengen.''
- De datum van de laatste update van het privacybeleid.
- Hoe contact te leggen met uw organisatie.

Het inzageverzoek van de betrokkene is een wettelijke vereiste waaraan alle organisaties moeten voldoen als daarom wordt gevraagd. Dit verwijst naar het recht van een persoon om een kopie te zien van de informatie die een organisatie over hen bewaart.

Dit omvat een recht om:

- te worden verteld of er persoonlijke gegevens worden verwerkt
- een beschrijving van de gegevens te krijgen, de redenen waarom het wordt verwerkt en of het zal worden gedeeld
- de bron van de gegevens te verkrijgen

Onder de AVG kunt u geen vergoeding meer vragen tenzij het verzoek 'kennelijk ongegrond of buitensporig' is of als de persoon meerdere verzoeken doet.

Publicatie van de privacy verklaring

Schrijf niet alleen een privacyverklaring om deze vervolgens ergens onderin een la terecht te laten komen. U moet het delen met uw achterban en het gemakkelijk maken om het te vinden.

Het is gebruikelijk om een aparte webpagina te hebben voor het privacybeleid. Koppelingen ernaar kunnen dan als een voettekst op uw website worden geplaatst (zodat u vanaf elke pagina ernaar kunt linken) en als voettekst in uw e-mails.

Schrijf niet alleen een privacyverklaring om deze vervolgens ergens onderin een la terecht te laten komen. U moet het delen met uw achterban en het gemakkelijk maken om het te vinden.

Als u voor de eerste keer een privacyverklaring maakt, moet u dit aan uw achterban melden, bijvoorbeeld via uw nieuwsbrief, tijdschrift of andere reguliere mailing. Het lijkt misschien niet het interessantste onderwerp om reclame voor te maken, maar het is belangrijk dat u kunt aantonen dat u inspanningen hebt gedaan om deze informatie te delen.

Wees voorbereid op het beheren van afmeldingen voor verschillende elementen van uw privacyverklaring. Ze zeggen misschien dat ze graag nieuwsbrieven ontvangen, maar bijvoorbeeld geen mailings met verzoeken willen ontvangen. Of ze kunnen zeggen dat ze niet willen dat u onderzoek naar hen of hun vermogen doet.

Wat betekent dit voor uw eerder opgeslagen gegevens?

De meeste organisaties hebben gegevens met betrekking tot het oude 'opt-out' systeem en sommige hebben helemaal geen toestemmingsgegevens. Kunnen deze gegevens worden ontsloten?

Sommige grote instellingen hebben besloten om iedereen in hun database aan te schrijven en hen te vragen om zich proactief aan te melden, wetende dat ze een groot percentage van hun database zullen verliezen. Het 'voordeel' van deze beslissing is dat ze aan het eind van het proces een veel actievere database zullen hebben, wetende dat iedereen bij de zaak is betrokken, en dat ze de uitgaven voor direct mailing omlaag hebben gebracht.

Als u ervoor kiest om deze aanpak te volgen, weet u dat u volledig gedekt bent, maar het zou waarschijnlijk ook flink wat geld kosten voor het onderhoud van uw database. Als u uw gegevens wilt blijven gebruiken zoals die zijn, moet u deze nauwkeurig bekijken, de bestaande toestemmingen en de gevoeligheid van de gegevens bekijken en de risico's beoordelen.

Een belangrijke overweging is of u van plan bent contact op te nemen via e-mail of per post:

E-mailcontact – u kunt alleen contact opnemen met mensen die zich actief hebben aangemeld ('opt-in'). Het bewijs kan bestaan uit een aanmelding voor een toestemmingsverklaring of een inschrijving op een e-mailnieuwsbrief of andere emailspecifieke communicatie (hoewel de laatste gevallen specifiek zijn voor die specifieke communicatie tenzij ze op dat moment werden gevraagd om zich aan te melden voor alle e-mailcommunicatie). U kunt geen (oude) e-mailadressen gebruiken waarvoor u geen toestemming hebt.

Postcontact – u kunt ervoor kiezen om te vertrouwen op de regel van het gerechtvaardigd belang om contact te blijven maken via de post. Er is een bijzonder sterke zaak voor die mensen aan wie een 'opt-out'-toestemmingsverklaring is aangeboden en die zich niet hebben afgemeld, omdat u kunt stellen dat ze waarschijnlijk verwachten dat ze uw mailings zullen ontvangen. U kunt ervoor kiezen om mensen per post te contacteren om hen te vragen hun toestemmingsstatus te upgraden naar 'aanmelden'. Maar houd er rekening mee dat iedereen die niet reageert op een dergelijk verzoek, nadat de nieuwe wet van kracht is, moet worden geacht zich te hebben afgemeld en dat hun gegevens dienovereenkomstig zijn gewijzigd.

Checklist actiepunten

Al uw besluitvorming op het gebied van gegevensbescherming moet worden gedocumenteerd door middel van de notulen van de trustee of interne vergaderingen of in beleidsdocumenten, zodat u kunt laten zien welke acties u heeft ondernomen om ervoor te zorgen dat u zich aan de regels houdt als er klachten worden ingediend of als u wordt gecontroleerd door de Autoriteit Persoonsgegevens.

Actiepunten:

- Beoordeel uw behoeften inzake gegevensverzameling in relatie tot de gegevens die u verzamelt. Verzamelt u meer dan nodig is? Kunt u gegevens verwijderen die niet nodig zijn?
- Hoe lang moet u uw gegevens bewaren? Maak een gegevensopslagbeleid en voer het uit.
- Waar en hoe verzamelt u gegevens? Bent u consistent?
- Beveiliging: zijn uw gegevensverzamelings- en opslagsystemen beveiligd?
- Welke wijzigingen moet u aanbrengen in uw database of andere systemen om toestemmingsgegevens vast te leggen, zoals vereist wanneer de AVG van kracht wordt?
- Welke gegevensverwerkingsactiviteiten voert u uit?
- Welke toestemming heeft u om deze uit te voeren?
- Vertrouwt u voor bepaalde activiteiten op de gerechtvaardigd belangregel? Zo ja, documenteer dan waarom u dit redelijk vindt.
- Hoe gaat u uw toestemmingsverklaring bijwerken?
- Heeft u een privacyverklaring? Zo niet, maak er dan een. Als u dit doet, kijk er dan zorgvuldig naar.
- Nieuw aangemaakte privacyverklaringen moeten bekend worden gemaakt – hoe gaat u dit doen?
- Wat zijn uw plannen voor uw oudere, al opgeslagen, gegevens?

Verdere informatie

- Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacy wetgeving

- Uitvoeringswet AVG:

  https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/wetsvoorstel-uitvoeringswet-algemene-verordening-gegevensbescherming
- Handleiding AVG: https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming

- Informatie over de AVG voor erfgoedinstellingen: https://www.zelfdoeninerfgoedengroen.nl/info-tips/wetgeving/avg/

Contact

Voor vragen, neem contact met ons op.
Erfgoedhuis Zuid-Holland,
Tamara van Zwol
vanzwol@erfgoedhuis-zh.nl
015-215 43 50

Met dank aan:

Helen Shone Development Partners Ltd September 2017

Association of Independent Museums (AIM)
3 Chestnut Grove Ludlow Shropshire SY8 1TJ
AIM Editor – Sassy Hicks www.aim-museums.co.uk

Oude Delft 116
2611CG Delft

info@erfgoedhuis-zh.nl
www.erfgoedhuis-zh.nl