

INTERN PRIVACY BELEID

STICHTING OUD SOEST (MUSEUM SOEST)

VOOR DE VERWERKING VAN PERSOONSgegevens

Versie 2.0 – september 2020

1. INTRODUCTIE

Dit is het privacy beleid (hierna: het "Privacy beleid") van **de Stichting Oud Soest** (hierna: "**het Museum**"). Dit privacy beleid ziet op het verzamelen en verwerken van persoonsgegevens die van vrijwilligers, donateurs en leden van de club van 100 worden verwerkt, als op gegevens van exposanten en andere derden die binnen het Museum worden gebruikt. Het privacy beleid beschrijft op welke wijze het Museum met deze gegevens omgaat en welke protocollen en processen zij binnen het Museum heeft geïmplementeerd om ervoor te zorgen dat de veiligheid van de gegevens gewaarborgd is en dat aan de vereisten van de Algemene verordening gegevensbescherming ("AVG") wordt voldaan.

In dit privacy beleid komen de volgende onderwerpen aan bod:

- ◆ Verwerkingsregister
- ◆ Type persoonsgegevens en doelen
- ◆ Informatieplicht
- ◆ Rechten van betrokkenen
- ◆ Derde partijen
- ◆ Beveiliging
- ◆ Datalekken

- ◆ Bewaartermijnen

- ◆ Doorgifte van persoonsgegevens

Om ervoor te zorgen dat dit Privacy beleid blijft aansluiten bij de verwerking van persoonsgegevens binnen het Museum, zal het Privacy beleid minimaal eens in de vijf jaar worden geëvalueerd. Aan de hand van die evaluatie zal, indien vereist, het Privacy beleid en de hieraan gehechte documenten worden aangepast. Indien op een moment voor de evaluatie duidelijk wordt dat het Privacy beleid aanpassing behoeft, zal het Museum de vereiste aanpassingen op dat moment al doorvoeren.

2. PRIVACY BELEID

2.1. Verwerkingsregister

Het Museum houdt een verwerkingsregister bij. Dit register bevat onder meer een beschrijving van de (categorieën) persoonsgegevens die binnen het Museum worden verwerkt, de doelen waarvoor ze worden verwerkt, de derden aan wie de gegevens worden verstrekt, de bewaartermijn van de gegevens en de technische

en organisatorische maatregelen die zijn genomen om de gegevens te beschermen.

Binnen het Museum hebben alleen de **bestuursleden van de Stichting Oud Soest** toegang tot het register.

Het register wordt door het Museum continue en actief bijgehouden. Wijzigingen in de verwerking van persoonsgegevens worden direct in het register doorgevoerd.

2.2. Type persoonsgegevens en doeleinden

Binnen het Museum worden persoonsgegevens van verschillende categorieën personen verwerkt:

1. Vrijwilligers
2. Vrienden (donateurs)
3. Leden van de Club van 100
4. Mensen die items in bruikleen geven of willen schenken
5. Exposanten
6. Mensen die aan een bedrijf of organisatie verbonden zijn, waar het museum een relatie mee heeft
7. Persoonsgegevens in het kader van bijzondere wet en/of regelgeving.

Vrijwilligers

Indien een vrijwilliger zich aanmeldt bij het Museum, worden allereerst de persoonsgegevens vereist voor inschrijving verstrekt. Het betreft hier NAW gegevens (naam adres woonplaats), telefoonnummer en emailadres en, indien hiertoe nadrukkelijk toestemming is verkregen, geboortedatum. Dit laatste in verband met de traditie de betrokkene een felicitatie te sturen op de verjaardag.

Alle gegevens die het Museum verkrijgt in het kader van het inschrijven van een vrijwilliger, worden beveiligd opgeslagen in 1 computer in het Museum, in Word en Excelbestanden en Buildix (hierna: het "Systeem"). Tevens worden de

gegevens fysiek opgeslagen in een kast die slechts toegankelijk is voor degenen die verantwoordelijk zijn voor het privacy beleid binnen het Museum.

Alle gegevens die over de vrijwilligers worden verzameld, worden gebruikt met als doel de communicatie met de vrijwilliger mogelijk te maken.

Vrienden (donateurs), leden Club van 100

Indien een vriend (donateur) of lid van de Club van 100 zich aanmeldt bij het Museum, worden allereerst de persoonsgegevens vereist voor inschrijving verstrekt. Het betreft hier NAW gegevens (naam adres woonplaats), telefoonnummer en emailadres.

Alle gegevens die het Museum verkrijgt in het kader van het inschrijven, worden beveiligd opgeslagen in 1 computer in het Museum, in Word en Excelbestanden en Buildix (hierna: het "Systeem"). Tevens worden de gegevens fysiek opgeslagen in een kast die slechts toegankelijk is voor degenen die verantwoordelijk zijn voor het privacy beleid binnen het Museum.

Alle gegevens die worden verzameld, worden gebruikt met als doel de communicatie en financiële afwikkeling met de betrokkene mogelijk te maken

Bruikleengevers, exposanten, andere relaties

Indien een bruikleengever, exposant of andere relatie zich aanmeldt bij het Museum, worden allereerst de persoonsgegevens vereist voor inschrijving verstrekt. Het betreft hier NAW gegevens (naam adres woonplaats), telefoonnummer en emailadres.

Indien men zich telefonisch of via de website van het Museum aanmeldt, wordt de betrokkene verzocht de gegevens te verstrekken die vereist zijn voor registratie.

Alle gegevens die het Museum verkrijgt in het kader van het inschrijven, worden beveiligd opgeslagen in 1 computer in het Museum, in Word en Excelbestanden

en Buildix (hierna: het "Systeem"). Tevens worden de gegevens fysiek opgeslagen in een kast die slechts toegankelijk is voor degenen die verantwoordelijk zijn voor het privacy beleid binnen het Museum.

Alle gegevens die worden verzameld, worden gebruikt met als doel de communicatie en financiële afwikkeling met de betrokkene mogelijk te maken

Persoonsgegevens in het kader van bijzondere wet en/of regelgeving

In het kader van bijzondere wetten en/of andere regelgeving kunnen door het Museum persoonsgegevens worden verzameld.

In verband met de Corona-crisis worden door museum Soest met ingang van de maand juni 2020 persoonsgegevens van bezoekers genoteerd. Het betreft hier NAW gegevens (naam adres woonplaats), telefoonnummer en emailadres.

Tevens wordt verwerkt op welke dag en tijd een bezoeker in het museum aanwezig was. Op verzoek van de GGD, het RIVM of andere overheidsorganisaties belast met bestrijding van de Corona-pandemie kunnen de voornoemde persoonsgegevens worden overgedragen. De registratie en eventuele overdracht van deze gegevens zal op een beveiligde wijze geschieden. De bewaartermijn van deze gegevens, ten behoeve van het voldoen aan een mogelijk verzoek voornoemd, is beperkt tot de duur die de GGD of het RIVM noodzakelijk acht

2.3. Informatieplicht

Het Museum stelt de betrokkene bij inschrijving op de hoogte van de persoonsgegevens die zij over deze persoon verzamelt en voor welke doeleinden deze persoonsgegevens vervolgens worden gebruikt.

Bij de inschrijving van de gegevens wordt de betrokkene gewezen op het **privacy statement** van het Museum zoals vermeld op de website.

Rechten van betrokkenen

Alle verzoeken, op welke wijze ook binnengekomen (telefonisch, per e-mail, per brief), van een bij het Museum betrokkene waarin rechten ten aanzien van persoonsgegevens worden ingeroepen, worden verzonden aan het Museum ter attentie van de voorzitter van het bestuur. Verzoeken en alle overige afhandeling worden opgeslagen in de map AVG in het museum Soest.

Na ontvangst van een verzoek zal het Museum eerst de identiteit van de verzoeker verifiëren. Het Museum kan de verzoeker vragen een kopie van een identiteitskaart mee te zenden. Het Museum zal daarbij aan de verzoeker aangegeven dat het BSN niet mag worden verstrekt en dus van de kopie van de identiteitskaart verwijderd moet worden.

Indien de identiteit van de betrokkene is vastgesteld, zal het Museum de verzoeker laten weten dat er binnen één maand op het verzoek zal worden gereageerd. Indien het verzoek complex is, kan deze termijn met maximaal twee maanden worden verlengd. Indien dit het geval is, zal het Museum dit binnen de initiële maand aan de verzoeker laten weten.

Het bestuur van het Museum zal vervolgens vaststellen welk recht precies wordt ingeroepen en verzamelt de in dat kader vereiste informatie. Op basis van deze informatie wordt een verslag opgesteld. Op basis van dit verslag wordt besloten of, en zo ja, op welke wijze aan het verzoek van de verzoeker kan worden voldaan.

Voor de communicatie richting de verzoeker en het treffen van maatregelen naar aanleiding van een verzoek zullen in beginsel geen kosten in rekening worden gebracht bij de verzoeker. Slechts in bepaalde gevallen zal het Museum kosten in rekening brengen (een redelijke vergoeding in het licht van de administratieve kosten). Bijvoorbeeld wanneer verzoeker meerdere inzageverzoeken of herhaaldelijk ongegronde verzoeken indient. Het Museum mag in uitzonderingsgevallen ook weigeren om gevolg te geven aan het verzoek.

Indien gevolg wordt gegeven aan het verzoek van een verzoeker, dienen in bepaalde gevallen ook derde partijen op de hoogte te worden gesteld. Het verslag dient daarom ook de derde partijen te beschrijven die betrokken zijn bij het honoreren van een verzoek van de verzoeker. Dergelijke kennisgevingen laat het

Museum achterwege als dit onmogelijk blijkt of onevenredig veel inspanning vergt.

Het Museum heeft zodanige technische maatregelen genomen dat aan verzoeken van verzoekers kan worden voldaan. Zo kan het Museum een verzoeker inzage verlenen in de gegevens die over hem/haar worden verzameld, kunnen gegevens worden verwijderd of verbeterd, kan de verwerking van gegevens tijdelijk worden gestaakt, kunnen deze gegevens makkelijk overgezet worden naar een nieuwe aanbieder en wordt er bij de intrekking van toestemming zorg voor gedragen dat de gegevens vanaf dat moment niet weer voor dat doel worden gebruikt.

Derde partijen

Het Museum maakt voor het verwerken van persoonsgegevens gebruik van (een) derde partij(en). Het gaat daarbij om partijen die louter ten behoeve van het Museum gegevens verwerken (hierna: "Verwerkers").

Met deze Verwerker(s) heeft het Museum een verwerkersovereenkomst afgesloten waarin onder meer de mate van beveiliging van de persoonsgegevens die de Verwerker voor het Museum verwerkt wordt beschreven. Ook bevat de verwerkersovereenkomst bepalingen omtrent het uitvoeren van een audit bij de Verwerker en de procedure die moet worden gevolgd als van een incident omtrent persoonsgegevens sprake is.

In het Museum wordt van de volgende Verwerker gebruikgemaakt :

- ◆ **RETO**, in het kader van onderhoud en support van het computersysteem

Persoonsgegevens worden niet aan andere verwerkingsverantwoordelijken verstrekt zonder voorafgaande uitdrukkelijke toestemming van de betrokkene. Dat is alleen anders indien er een wettelijke verplichting tot verstrekking bestaat. Daarbij geldt dat alleen de strikt noodzakelijk geachte gegevens worden verstrekt.

2.4. Beveiliging

Het Museum hecht veel waarde aan de beveiliging van de aan haar verstrekte persoonsgegevens. Het Museum heeft daarom passende technische en organisatorische maatregelen genomen om deze persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.

Voor zover het Museum gebruikmaakt van Verwerkers zijn met deze Verwerkers afspraken gemaakt over de te nemen technische en organisatorische maatregelen. Hierbij wordt een risicoanalyse gemaakt. Op grond van de risico's die de persoonsgegevens en de aard van de verwerking met zich meebrengen, wordt het gewenste beveiligingsniveau bepaald.

Het Museum heeft op grond van de verwerkersovereenkomst het recht de door de Verwerker getroffen maatregelen periodiek te auditen, testen, beoordelen en evalueren om zo te bepalen of de overeengekomen maatregelen worden nageleefd en of deze nog doeltreffend zijn en om deze zo nodig aan te laten passen.

Het Museum hanteert in aanvulling op het bovenstaande ook interne beveiligingsmaatregelen. Het gaat daarbij onder meer om de volgende maatregelen:

- ◆ Persoonsgegevens worden op een beveiligde wijze uitgewisseld
- ◆ Persoonsgegevens worden niet op USB sticks of andere mobiele dragers gekopieerd tenzij de persoonsgegevens versleuteld worden
- ◆ Alleen de in dit beleidsstuk benoemde bestuursleden hebben toegang tot de persoonsgegevens
- ◆ Wachtwoorden zijn voldoende sterk en worden periodiek vervangen
- ◆ Binnen het Museum zijn processen ingericht die aangeven wat er moet gebeuren indien een incident inzake persoonsgegevens zich voordoet of indien betrokkenen een beroep op hun rechten doen
- ◆ Devices als laptops en mobiele telefoons worden niet onbeheerd achtergelaten, worden versleuteld opgeslagen en verlies/diefstal dient direct te worden gemeld bij het Museum
- ◆ Toegang tot het pand is alleen mogelijk met aan medewerkers verstrekte sleutels. Er wordt nauwkeurig bijgehouden wie de

beschikking heeft over een sleutel. Verlies/diefstal van een sleutel dient direct te worden gemeld bij het Museum

Binnen het Museum worden maandelijks back-ups gemaakt. Hiermee realiseert het Museum dat in het geval van een incident met persoonsgegevens (bijvoorbeeld in het geval van ransomware) een recente back-up teruggezet kan worden zodat persoonsgegevens niet blijvend verloren gaan.

De interne beveiligingsmaatregelen kunnen door het Museum steekproefsgewijs worden gecontroleerd. Controle zal altijd zo kort en zo beperkt mogelijk uitgevoerd worden. Indien er een gerichte verdenking bestaat tegen een medewerker kan tot gerichte controle worden overgegaan. Aan de hand van de uitkomst van steekproeven kunnen door het Museum disciplinaire maatregelen genomen worden.

Uitgangspunt binnen het Museum is dat niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld. Zo vraagt het Museum niet meer informatie uit bij de betrokkene dan noodzakelijk is voor de communicatie en financiële afwikkeling. Ook bij het inschakelen van derde partijen, beoordeelt het Museum of de door die derde partij aangeboden dienst aansluit bij het doel dat het Museum voor ogen heeft en er niet meer persoonsgegevens worden verzameld dan daarvoor nodig is.

2.5. Datalekken

Het Museum heeft passende technische en organisatorische maatregelen genomen die tot doel hebben de kans op verlies of onrechtmatige verwerking van persoonsgegevens zo veel mogelijk te beperken. Ondanks deze maatregelen bestaat de kans dat zich toch een incident met betrekking tot persoonsgegevens voordoet.

Elk incident met betrekking tot persoonsgegevens moet **schriftelijk** worden gemeld aan het bestuur van het Museum, waarna deze vervolgens zal bepalen of:

- ◆ er inderdaad sprake is van een incident dat betrekking heeft op persoonsgegevens

- ◆ welke maatregelen genomen moeten worden om het incident te stoppen en de gevolgen te beperken
- ◆ er een externe partij moet worden ingeschakeld om bij de oplossing van het incident te assisteren
- ◆ het incident aan de Autoriteit Persoonsgegevens moet worden gemeld. De melding aan de Autoriteit Persoonsgegevens zal vervolgens binnen 72 uur nadat het Museum op de hoogte is geraakt van het incident plaatsvinden
- ◆ degenen op wie de persoonsgegevens betrekking hebben, moeten worden geïnformeerd over het incident
- ◆ welke maatregelen er genomen moeten worden om herhaling van het incident te voorkomen

Aangezien de kans bestaat dat een Verwerker als eerste op de hoogte raakt van een (potentieel) incident, is in de Verwerkersovereenkomst afgesproken dat de Verwerker het Museum zo snel mogelijk op de hoogte stelt van een incident. Ook zijn er afspraken gemaakt over het oplossen van het incident en het verstrekken van nadere gegevens.

Het Museum documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Dit logboek wordt opgeslagen in Excel.

2.6. Bewaartermijnen

Het Museum hanteert een beleid voor het bewaren van persoonsgegevens. Persoonsgegevens die niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld en tevens niet op grond van andere wetgeving bewaard moeten worden, worden door het Museum verwijderd. De persoonsgegevens dienen in dat geval ook uit eventuele back-ups, archieven en andere systemen te worden verwijderd.

Vrijwilligers gegevens

Vrijwilliger gegevens worden bewaard zolang de betrokkene vrijwilliger is en met toestemming van de vrijwilliger voor een periode daarna, in verband met mogelijke reünies en het verzenden van uitnodigingen voor bijvoorbeeld openingen van exposities.

Overige betrokkenen

Het Museum bewaart gegevens van de overige betrokkenen zolang deze betrokken zijn bij het museum en daarna, voor zover vereist op basis van fiscale boekhoud- en administratieplicht, gedurende een periode van 7 jaar.