PALEIS HET LOO

VERWERKERS-OVEREENKOMST

Verwerkersovereenkomst [NAAM BEDRIJF]

Datum: DATUM

Contractpartijen:

1. Stichting Paleis Het Loo, nationaal museum gevestigd aan het Koninklijk Park 1 te Apeldoorn, rechtsgeldig vertegenwoordigd door mevrouw P. Harms, Zakelijk Directeur.

Hierna te noemen: **'Verwerkingsverantwoordelijke'**,

en

2. Verwerker te weten [STATUTAIRE NAAM], statutair gevestigd te [PLAATS], vertegenwoordigd door [NAAM EN/OF NAAM BESTUURDER].

Hierna te noemen: **'Verwerker'**,

Gezamenlijk aan te duiden als: **'Partijen'** en afzonderlijk als **'Partij'**

Overwegende dat:

- Partijen op DATUM een Overeenkomst met betrekking tot [OMSCHRIJVING] hebben gesloten.
- Ter uitvoering van deze overeenkomst Persoonsgegevens worden verwerkt.
- Partijen gelet op het bepaalde in de privacywetgeving, waaronder de Algemene verordening gegevensbescherming nadere afspraken wensen te maken over de voorwaarden waaronder Verwerker de Persoonsgegevens zal verwerken;
- Partijen in dit kader in deze overeenkomst de volgende afspraken schriftelijk wensen vast te leggen.

KOMEN OVEREEN ALS VOLGT:

1. Verlening van opdracht tot verwerking persoonsgegevens

1.1 Verwerkingsverantwoordelijke verleent opdracht aan Verwerker voor het verwerken van de Persoonsgegevens welke opdracht Verwerker hierbij aanvaardt inclusief de daarbij behorende bijlagen:

1.1.1 Overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen

1.1.2 Overzicht met beveiligingsmaatregelen

1.1.3 Proces rondom het melden van Datalekken en de te verstrekken informatie met betrekking tot het Datalek vast wat Verwerker wel en niet mag doen met de Persoonsgegevens.

1.2 Partijen bevestigen dat Verwerkingsverantwoordelijke volledig verantwoordelijk is voor het vaststellen van het doel en de middelen voor de verwerking van persoonsgegevens. De Verwerker verwerkt de persoonsgegevens uitsluitend ten behoeve van de Verwerkingsverantwoordelijke overeenkomstig diens instructies en onder diens verantwoordelijkheid. De Verwerker heeft geen zeggenschap over het doel en de middelen van de verwerking noch over de persoonsgegevens.

2. Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

2.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (**'de Betrokkene'**); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
2.2 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
2.3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lid statelijke recht worden vastgesteld, kan daarin worden bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (**'Verwerkingsverantwoordelijke'**).
2.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt (**'Verwerker'**).
2.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte Persoonsgegeven betrekking hebben.
2.6 Verwerkersovereenkomst: deze Overeenkomst inclusief de bijlagen (**'Verwerkersovereenkomst'**).
2.7 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit. Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofd verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (**'Datalek'**).
2.8 Toezichthoudende autoriteit: een onafhankelijk overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens.
2.9 Subverwerker: De partij die met toestemming van de verantwoordelijke namens de verwerker persoonsgegevens verwerkt voor de verantwoordelijke.
2.10 Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofd verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens

3. Totstandkoming, duur en beëindiging van deze Verwerkersovereenkomst

3.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.
3.2 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.
3.3 Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd
3.4 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor Verwerker, zoals het melden van Datalekken waarbij Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn, de bewaartermijnen en de plicht tot geheimhouding blijven voortduren.

3.5 Partijen zijn gerechtigd deze overeenkomst met onmiddellijke ingang en zonder rechterlijke tussenkomst te ontbinden, of de ontbinding ervan in rechte te vorderen, zonder gehoudenheid tot betaling van (enige vorm van) schadevergoeding of compensatie, indien de andere Partij na een schriftelijke ingebrekestelling waarin een termijn van 14 werkdagen is gesteld voor zuivering van de tekortkoming, toerekenbaar tekortschiet in de nakoming van een verplichtingen uit deze overeenkomst. De schriftelijke ingebrekestelling dient een volledige en gedetailleerde omschrijving van de tekortkoming te bevatten

3.6 Partijen zijn gerechtigd deze overeenkomst met onmiddellijke ingang en zonder rechterlijke tussenkomst te ontbinden, of de ontbinding ervan in rechte te vorderen, zonder dat enige aanmaning of ingebrekestelling zal zijn vereist, en zonder gehoudenheid tot betaling van (enige vorm van) schadevergoeding of compensatie, indien: (i) de andere Partij (voorlopige) surseance van betaling aanvraagt of hem (voorlopige) surseance van betaling wordt verleend, (ii) de andere Partij faillissement aanvraagt, een derde het faillissement van de andere Partij aanvraagt, of een rechter de andere Partij in staat van faillissement verklaart, en (iii) de onderneming van de andere Partij wordt geliquideerd, (iv) de bedrijfsuitoefening van de andere Partij wordt gestaakt.

3.7 Ontbinding en opzegging van deze overeenkomst dient door middel van aangetekend schrijven aan de andere Partij plaats te vinden.

3.8 Een beroep op het recht deze overeenkomst te ontbinden laat onverlet het recht van de ontbindende Partij op schadevergoeding met uitzondering van artikel 3.9.

3.9 Partijen zijn gerechtigd deze overeenkomst met onmiddellijke ingang en zonder rechterlijke tussenkomst te beëindigen, ontbinden, of de ontbinding ervan in rechte te vorderen indien er sprake is van wijziging van wet- en regelgeving (incl. verzoeken CvdM) van zodanige aard, dat ongewijzigde nakoming van de overeenkomst in redelijkheid niet van Partijen kan worden gevergd. In deze gevallen zijn Partijen gerechtigd tot ontbinding dan wel beëindiging met inachtneming van een opzegtermijn van 6 maanden tenzij de toezichthouder of wetgever anders vereist zonder enige vorm van (schade)vergoeding in welke vorm dan ook.

3.10 Beëindiging, ontbinding of opzegging van deze overeenkomst, op welke grond of wijze dan ook, laat verbintenissen van Partijen onverlet welke naar hun aard bedoeld zijn voort te duren na beëindiging, waaronder in ieder geval begrepen geheimhoudingplichten, vrijwaringsplichten, aansprakelijkheidsbepalingen en bepalingen omtrent toepasselijk recht en jurisdictie.

4. Verwerken Persoonsgegevens

4.1 Verwerker verwerkt alleen Persoonsgegevens in opdracht van Verwerkingsverantwoordelijke en Verwerker heeft geen zeggenschap over de Persoonsgegevens. Verwerker volgt instructies van Verwerkingsverantwoordelijke ten aanzien van de verwerking op en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Verwerkingsverantwoordelijke Verwerker daarvan tevoren toestemming of opdracht voor geeft.

4.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Verwerker precies zal verwerken en voor welke verwerkingsdoeleinden.

4.3 Verwerker houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.

4.4 Verwerker mag zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.

4.5 Wanneer Verwerker met toestemming van Verwerkingsverantwoordelijke andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.

4.6 Wanneer Verwerkingsverantwoordelijke een verzoek van een Betrokkene ontvangt ten aanzien van het uitoefenen van zijn of haar rechten, dan werkt Verwerker daar binnen een

termijn van 7 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.

5 Beveiligen Persoonsgegevens

5.1 Verwerker zorgt ervoor dat de Persoonsgegevens voldoende worden beveiligd. Om verlies en onrechtmatige verwerkingen te voorkomen neemt Verwerker voldoende passende technische en organisatorische maatregelen.

5.2 Deze maatregelen zijn afgestemd op het risico van de Verwerking. Een overzicht van deze Maatregelen en het beleid daaromtrent wordt opgenomen in Bijlage 2.

5.3 Ter controle van de genomen beveiligingsmaatregelen zal Verwerker aan Verwerkingsverantwoordelijke ieder jaar een rapportage sturen waarin de genomen maatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor brengt Verwerker geen kosten in rekening aan Verwerkingsverantwoordelijke.

5.4 Verwerkingsverantwoordelijke mag een audit laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Verwerker verleent hierbij zijn medewerking. Waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.

5.5 De kosten voor de uitvoering van deze audit zullen voor rekening van Verwerker komen wanneer blijkt dat Verwerker zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.

5.6 De controle op de algehele verwerking van Persoonsgegevens door Verwerker kan, naast de auditmogelijkheid, ook geschieden via zelfevaluatie door Verwerker. Verwerker zal hierbij aan Verwerkingsverantwoordelijke een rapport verstrekken waarin Verwerker aantoont dat hij voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Verwerker.

5.7 Wanneer Partijen vinden dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Partijen in overleg over de wijziging daarvan. De kosten gemoeid met het wijzigen van de beveiligingsmaatregelen komen voor rekening van degene die de kosten maakt.

6. Exporteren Persoonsgegevens

6.1 Verwerker mag geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van Verwerkingsverantwoordelijke.

7. Geheimhouding

7.2 Verwerker zal de verstrekte Persoonsgegevens geheimhouden, tenzij dit op basis van een wettelijke verplichting niet kan. Als opdrachtnemer wettelijk verplicht is gegevens te verstrekken, dan meldt de opdrachtnemer de verwerkingsverantwoordelijke dat wettelijk voorschrift voorafgaand aan de verstrekking, tenzij die wetgeving deze kennisgeving verbiedt.

7.3 Verwerker verplicht zich geen product-, markt- en bedrijfsgegevens die Verwerkingsverantwoordelijke betreffen aan derden kenbaar te maken, tenzij deze informatie – zonder dat dit veroorzaakt is doordat de onderhavige geheimhoudingsverplichting is geschonden – van algemene bekendheid is. Verwerker zal deze informatie uitsluitend gebruiken voor de uitvoering van deze overeenkomst.

7.4 Een Partij (of alleen de Verwerker) zal aan derden uitsluitend mededeling doen over de inhoud van deze overeenkomst indien en voor zover van de andere partij daarvoor vooraf schriftelijke toestemming is verkregen
7.5 Verwerker zorgt dat zijn/haar personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-)contracten op te nemen.

8. Datalekken

8.1 In geval van een ontdekking van een mogelijk Datalek zal Verwerker Verwerkingsverantwoordelijke hierover onmiddellijk informeren doch uiterlijk binnen een termijn van 12 uur overeenkomstig het proces volgend uit Bijlage 3, zodat Verwerkingsverantwoordelijke indien nodig een melding van het Datalek bij de Toezichthouder kan doen. De Verwerker treft onmiddellijk adequate maatregelen om de gevolgen van het incident te beperken en herhaling te voorkomen.
8.2 Verwerker zal Verwerkingsverantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek, ook zal Verwerker de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan Verwerkingsverantwoordelijke.
8.3 Verwerker mag geen melding van een Datalek aan de Toezichthoudende Autoriteit doen of aan enige andere derde, wanneer bij het Datalek Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn. Ook mag Verwerker de Betrokkenen niet informeren over het Datalek. Deze verantwoordelijkheid ligt bij Verwerkingsverantwoordelijke.
8.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

9. Aansprakelijkheid

9.1 Als Verwerker de verplichtingen uit deze Verwerkersovereenkomst niet nakomt, kan Verwerkingsverantwoordelijke Verwerker daarvoor aansprakelijk stellen.
9.2 Verwerker is jegens Verwerkingsverantwoordelijke aansprakelijk voor alle schade die voortvloeit uit enige tekortkoming van Verwerker en andere partijen of organisaties die zij inschakelt / Subverwerkers (dan definiëren) in de nakoming van haar verplichting uit deze overeenkomst
9.3 Verwerker zal Verwerkingsverantwoordelijke vrijwaren tegen en schadeloos houden voor alle aanspraken van derden die ontstaan als gevolg van, of die verband houden met, een werkelijke of vermeende schending van toepasselijke wet- en regelgeving en gedragscodes ter zake van de bescherming van persoonsgegevens, waaronder in ieder geval mede begrepen de Algemene Verordening Gegevensbescherming en de Telecommunicatiewet. Verwerker draagt zorg voor voldoende dekking van de aansprakelijkheid.
9.4 Onverminderd hetgeen elders in deze overeenkomst overeengekomen, zal de aansprakelijkheid van Verwerker voor de totale schade die voortvloeit uit of in verband met een eventuele toerekenbare tekortkoming van Verwerker of die op enige andere rechtsgrond kan worden gebaseerd, per gebeurtenis of reeks van gebeurtenissen beperkt zijn tot maximaal hetgeen de verzekeraar van Verwerker in een voorkomend schadegeval uitkeert. Verwerker heeft een bedrijfsaansprakelijkheid verzekering onder VNAB-nummer [VNAB-nummer] (polis). De polis is desgewenst opvraagbaar bij Verwerker. Iedere verdere aansprakelijkheid van Verwerker ten opzichte van Verwerkingsverantwoordelijke is hierbij uitgesloten, daaronder begrepen iedere aanvullende schadevergoeding bijvoorbeeld als gevolg van enige gevolgschade (waaronder in ieder geval wordt verstaan indirecte schade, schade wegens gederfde omzet of winst, imago schade).

9.5 Verwerker is aansprakelijk voor de aan Verwerkingsverantwoordelijke opgelegde bestuurlijke boete door de Toezichthouder als de schade het gevolg is van het onrechtmatig of nalatig handelen van Verwerker.
9.6 Verwerkingsverantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkene of andere personen en organisaties waar Verwerker de samenwerking mee is aangegaan of waarvan Verwerker Persoonsgegevens verwerkt, als dit het gevolg is van het onrechtmatig of nalatig handelen van Verwerker.

Overdracht

Het is Partijen niet toegestaan rechten en/of verplichtingen uit deze overeenkomst aan (een) derde(n) over te dragen zonder de voorafgaande schriftelijke toestemming van de andere Partij.
Partijen zullen een op grond van deze overeenkomst vereiste toestemming voor overdracht niet op onredelijke gronden onthouden en het geven van deze toestemming niet onredelijk vertragen.

Teruggave Persoonsgegevens en bewaartermijn

Na het beëindigen van deze Verwerkersovereenkomst geeft Verwerker de Persoonsgegevens terug aan Verwerkingsverantwoordelijke binnen 30 dagen na beëindiging van de deze Verwerkersovereenkomst.
De overgebleven Persoonsgegevens en kopieën daarvan zal Verwerker vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van Verwerkingsverantwoordelijke. Hierbij valt bijvoorbeeld te denken aan Persoonsgegevens die om belastingtechnische redenen bewaard moeten blijven.
Verwerker zal na de teruggave en/of vernietiging van de Persoonsgegevens schriftelijk aan Verwerkingsverantwoordelijke verklaren niet langer in het bezit te zijn van de Persoonsgegevens.

Slotbepalingen

Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.
Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst ten aanzien van de verwerking van Persoonsgegevens.
Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.
De verplichtingen van de Verwerker uit deze overeenkomst, gelden ook voor degenen die persoonsgegevens verwerken onder het gezag van Verwerker en/of door Verwerker worden ingezet.
De Verwerkingsverantwoordelijke draagt er zorg voor dat die gegevens die van belang zijn voor de uitvoering van de met Verwerker overeengekomen werkzaamheden zullen worden doorgegeven aan Verwerker.
De Verwerker voorziet de Verwerkingsverantwoordelijke (via de Beheersorganisatie) van de noodzakelijke informatie waardoor Verwerkingsverantwoordelijke een oordeel kan vormen over de naleving door Verwerker van deze overeenkomst.
Verwerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures gericht op de naleving van deze overeenkomst
Wijziging van deze overeenkomst of aanvullingen daarop zijn slechts geldig indien deze schriftelijk zijn overeengekomen in een door beide Partijen ondertekend wijzigingsdocument
Indien een bepaling van deze overeenkomst nietig, vernietigbaar, of anderszins onafdwingbaar is of wordt, dan blijven de overige bepalingen van deze overeenkomst

volledig van kracht. Partijen zullen in dat geval te goeder trouw in onderhandeling treden om de nietige, vernietigbare, of anderszins onafdwingbare bepaling te vervangen door een uitvoerbare alternatieve bepaling, waarbij Partijen zoveel mogelijk rekening zullen houden met het doel en strekking van de nietige, vernietigde of anderszins niet afdwingbare bepaling
Deze overeenkomst prevaleert boven alle voorgaande schriftelijke dan wel mondelinge afspraken en correspondentie betreffende de verwerking van persoonsgegevens indien deze strijdigheid met de toepasselijke wet- en regelgeving zou opleveren.

Toepasselijk recht en jurisdictie
Alle geschillen welke betrekking hebben op, voortvloeien uit, of verband houden met deze overeenkomst die niet in der minne kunnen worden geschikt, kunnen in eerste instantie uitsluitend ter beslechting worden voorgelegd aan de bevoegde rechter van de rechtbank Gelderland.
Op deze overeenkomst is Nederlands recht van toepassing.

Aldus door Partijen overeengekomen en ondertekend:

Verwerkingsverantwoordelijke:	**Verwerker**
Ondertekend voor en namens:	Ondertekend voor en namens
Stichting Paleis Het Loo, Nationaal Museum Koninklijk Park 1 7315 JA Apeldoorn	[STATUTAIRE NAAM]
Mevrouw P. Harms *Zakelijk Directeur*	Naam: *Functie:*
Apeldoorn, / / 2022	Datum en plaats:
Handtekening:	Handtekening

Bijlage 1: Overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen

Het onderstaande schema zal ingevuld moeten worden elke keer dat een Verwerkersovereenkomst wordt gesloten. Het geeft een volledig overzicht van de Persoonsgegevens die verwerkt zullen worden. Dit maakt het makkelijker om aan te kunnen tonen waar, door wie en voor welk doel de Persoonsgegevens worden verwerkt.

Beschrijving verwerkingsactiviteiten door Verwerker:	
Verwerkingsdoelen:	
Verwerkingsverantwoordelijke:	
Verwerker:	
Sub-Verwerkers:	
Verwerkte Persoonsgegevens:	
Locatie verwerkingen:	
Bewaartermijn:	

Bijlage 2: Overzicht met beveiligingsmaatregelen

Overzicht van de beveiligingsnormen die de Verwerkingsverantwoordelijke aan de Verwerker oplegt.
Om vast te stellen wat passende beveiligingsmaatregelen zijn, moet een afweging worden gemaakt op basis van de risico's van de verwerking aan de hand van onder meer de volgende punten:

- Het soort Persoonsgegevens dat verwerkt wordt (normaal, bijzonder of gevoelig) en eventueel de daarbij behorende (risico)classificatie die de organisatie zelf aan de gegevens heeft gegeven. *Gaat het bijvoorbeeld om een naam of een e-mailadres, wat minder gevoelige Persoonsgegevens zijn, of gaat het om het verwerken van een BSN.*
- De hoeveelheid betrokkenen van wie gegevens worden verwerkt. *Hoe meer betrokkenen er zijn, hoe meer eisen er worden gesteld aan de beveiliging van de gegevens.*
- Het doel waarvoor gegevens worden verwerkt.
- De duur en de wijze waarop gegevens bewaard moeten worden.

Er kan vervolgens onderscheid gemaakt worden tussen organisatorische beveiligingseisen, zoals het voorkomen van diefstal van een laptop met daarop Persoonsgegevens uit de auto, en technische beveiligingseisen, zoals een uitgebreide IT-omgeving die beveiligd wordt tegen virussen en waar encryptie van de gegevens wordt toegepast. Van een grote organisatie wordt meer verwacht ten aanzien van de te nemen beveiligingseisen.

De onderstaande maatregelen zijn suggesties voor beveiligingsmaatregelen en de aanwezigheid hiervan kan een indicatie zijn van een gepast beveiligingsniveau.

Technische beveiligingsmaatregelen

☐ Up-to-date virusscanner op elke laptop, pc en tablet
☐ Beveiligde USB-sticks
☐ Accurate beveiliging medewerkerstelefoon
☐ Bitlocker toegangsmechanisme
☐ Unieke inlogcode en wachtwoord (regelmatig aanpassen)
☐ Versleutelde e-mail
☐ Geen onbeveiligde externe harde schijven
☐ Geen onbeveiligde back-ups maken
☐ Geen documenten op privélaptop opslaan

Organisatorische beveiligingsmaatregelen

☐ Clean desk policy
☐ Laptop niet onbemand achterlaten
☐ Laptop nooit achterlaten in de auto
☐ Privacy screens medewerkers
☐ Oude documenten op juiste manier vernietigen
☐ Zorgvuldig gebruik van USB-sticks

Bijlage 3: Proces rondom het melden van Datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?

Een datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de Verwerkingsverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met login-gegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met Persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT-systeem.
- Een verloren of gestolen telefoon waar Persoonsgegevens op aanwezig zijn.

Wat te doen bij twijfel?

Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteit)fraude mee kan worden gepleegd, zoals een Burgerservicenummer?
- Zijn er grote hoeveelheden Persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de Persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met de privacy officer.

Waar meld je het beveiligingsincident?

Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met de privacy officer:
Peter Schilder

Telefoon: 055-5772400
Of
E-mail: privacy@paleishetloo.nl

Geef in je e-mail beantwoording op de onderstaande vragen
Wij willen graag dat je de onderstaande vragen voor ons beantwoord. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

De privacy-officer kan je helpen met de beantwoording hiervan. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingslek/beveiligingsincident/datalek: wat is er gebeurd? Vermeld hier ook de naam van het betrokken systeem.
2. Welke typen Persoonsgegevens zijn betrokken bij het beveiligingsincident?
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. Van hoeveel personen zijn de Persoonsgegevens betrokken bij het beveiligingsincident?
   Geef a.u.b. een minimum en maximum aantal personen.
4. Omschrijving groep personen om wiens gegevens het gaat.
   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers.
   Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.
5. Zijn de contactgegevens van de betrokken personen bekend?
   Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?
6. Wat is de oorzaak (root cause) van het beveiligingsincident?
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?
   Geef dit a.u.b. zo specifiek mogelijk aan.
8. Geef aan welke maatregelen de Verwerker eventueel reeds heeft getroffen.