- Privacyreglement –

Vereniging Stads- en Kinderboerderijen Nederland (vSKBN)

www.vskbn.nl

November 2019, versie 1

Inhoudsopgave

Voorwoord

Iedereen heeft recht op bescherming van zijn persoonlijke levenssfeer. Om die bescherming te waarborgen geeft de privacywetgeving (Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG) aan hoe we moeten omgaan met persoonsgegevens, wat de rechten zijn van degene van wie persoonsgegevens worden verwerkt en wat de plichten zijn van degene die met de gegevens werkt.

Binnen Vereniging Stads- en Kinderboerderijen Nederland (hierna te noemen vSKBN) werken we met persoonsgegevens van bestuursleden, leden, medewerkers, vrijwilligers en contactpersonen.

Met dit reglement willen we inzicht geven in de manier waarop wij met gegevensverwerking omgaan en welke afspraken er gemaakt zijn. In dit reglement zijn de algemene privacybepalingen rondom gegevensverwerking opgenomen en de rechten en plichten van partijen. In de bijlagen zijn onze documenten opgenomen, zoals de procedure bij datalekken en de formulieren die we gebruiken.

Artikel 1 Begripsbepalingen

1. *Persoonsgegevens*: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
2. *Verwerking van persoonsgegevens*: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
3. *Verstrekken van persoonsgegevens*: het bekend maken of ter beschikking stellen van gegevens;
4. *Verzamelen van persoonsgegevens*: het verkrijgen van persoonsgegevens;
5. *Identificeerbare gegevens*: gegevens die zonder onevenredige tijd en moeite aan de betrokkene zijn te koppelen;
6. *Bestand*: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
7. *Verantwoordelijke*: bestuur Stichting Kinderboerderij De Goudse Hofsteden te Gouda.
8. *Bewerker*: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
9. *Betrokkene*: diegene op wie een persoonsgegeven betrekking heeft;
10. *Derde*: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
11. *Ontvanger*: degene aan wie de persoonsgegevens worden verstrekt;
12. *Datalek*: een inbreuk op de beveiliging van persoonsgegevens waardoor die gegevens verloren gaan of onrechtmatig worden verwerkt.
13. *Toestemming van de betrokkene*: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt;
14. *De Autoriteit Persoonsgegevens*: de organisatie die tot taak heeft toe te zien op de verwerking van persoonlijke gegevens krachtens de privacywetgeving;
15. *Klachtenregeling*: De wijze waarop de kinderboerderij omgaat met klachten en meldingen. Dit is opgenomen in de informatiemap.
16. Vereniging Stads- en Kinderboerderijen Nederland (vSKBN), statutair gevestigd te Geldermalen

Artikel 2 Toepassingsgebied

1. Het doel van dit reglement is een praktische uitwerking te geven aan de bepalingen van de Europese Algemene Verordening Gegevensbescherming (AVG).
2. Dit reglement is van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens. Het is eveneens van toepassing op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
3. Dit reglement is van toepassing op de vSKBN heeft betrekking op de verwerkingen van persoonsgegevens van bestuursleden, leden, medewerkers, vrijwilligers en contactpersonen.

Artikel 3 Doel van de verwerking van persoonsgegevens

1. Persoonsgegevens worden in overeenstemming met de wet en dit reglement op behoorlijke en zorgvuldige wijze verwerkt.
2. Persoonsgegevens worden niet verwerkt op een wijze die onverenigbaar is met doeleinden waarvoor ze zijn verkregen.
3. Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.
4. De kaders waarbinnen de doelstelling van de verwerking van persoonsgegevens dient te blijven zijn als specificatie (verwerkingsregister). Deze is opgenomen in bijlage 1 en omvatten in grote lijnen:
   - communicatie
   - veiligheid
   - wettelijke verplichting
   - ondersteuning van de bedrijfsvoering.

   De verantwoordelijke is verantwoordelijk voor het goed functioneren van de verwerking van persoonsgegevens. Zijn handelen met betrekking tot de verwerking van de persoonsgegevens en de verstrekking van gegevens wordt bepaald door dit reglement.
5. De verantwoordelijke zal niet meer persoonsgegevens verwerken dan voor het doel van de verwerking noodzakelijk is.
6. De verantwoordelijke is aansprakelijk voor de eventuele schade als gevolg van het niet naleven van dit reglement.

Artikel 4 Wijze waarop de verwerking van persoonsgegevens plaatsvindt

1. De verantwoordelijke is verplicht de wijze waarop de verwerking van persoonsgegevens plaatsvindt vast te leggen.
2. Bij de beoordeling of een verwerking onverenigbaar is als bedoeld in artikel 3 lid 2, houdt de verantwoordelijke in ieder geval rekening met:
   - de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
   - de aard van de betreffende gegevens;
   - de gevolgen van de beoogde verwerking voor de betrokkene;
   - de wijze waarop de gegevens zijn verkregen en
   - de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Artikel 5 Verwerking van persoonsgegevens

1. De verantwoordelijke is aanspreekbaar voor het goed functioneren van de verwerking van de persoonsgegevens en voor de naleving van de bepalingen van dit reglement. Zijn handelen, met betrekking tot de verwerking van de persoonsgegevens en de verstrekking van gegevens wordt bepaald door dit reglement.
2. De verantwoordelijke treft de nodige voorzieningen ter bevordering van de juistheid en volledigheid van de opgenomen gegevens. Hij draagt tevens zorg voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van de persoonsgegevens tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan.
3. Persoonsgegevens mogen slechts worden verwerkt indien:
   - de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;

- de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor handelingen die op verzoek van de betrokkene worden verricht;
- de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
- de gegevensverwerking noodzakelijk is ter bestrijding van ernstig gevaar voor de gezondheid van betrokkene of ter vrijwaring van een vitaal belang van de betrokkene;
- de gegevensverwerking noodzakelijk is voor de vervulling van een publiekrechtelijke taak;
- de gegevensverwerking noodzakelijk is met het oog op het belang van de verantwoordelijke of van een derde én het belang van degene van wie de gegevens worden verwerkt niet prevaleert.

Artikel 6 Toegang tot persoonsgegevens

1. Alleen die personen hebben toegang tot de persoonsgegevens voor zover dat noodzakelijk is voor de uitoefening van hun functie.
2. Een ieder die toegang heeft tot de persoonsgegevens heeft een geheimhoudingsplicht ter zake van de gegevens waarvan hij op grond van die toegang heeft kennisgenomen.
3. Derden die door de vSKBN zijn ingehuurd om werkzaamheden te verrichten, hebben toegang tot de verwerkingen van persoonsgegevens, voor zover dit noodzakelijk is voor hun taakuitoefening en worden via een contractuele overeenkomst gehouden aan de geheimhoudingsplicht.
4. De verantwoordelijke, de bewerker, of een derde zijn verplicht te zwijgen tegen anderen over alle informatie die zij over betrokkene hebben. Na overlijden van de betrokkene blijft deze zwijgplicht bestaan. De zwijgplicht kan slechts worden doorbroken:
   - op grond van een wettelijk voorschrift;
   - indien de betrokkene toestemming heeft gegeven.

Artikel 7 Beveiliging van de persoonsgegevens

1. Er wordt zorgvuldig omgegaan met persoonsgegevens. Hiertoe worden de gegevens beveiligd.
2. De verantwoordelijke stelt beveiligingsvoorschriften voor de persoonsgegevens op (zie bijlage instructies gegevensbeveiliging).

Artikel 8 Verstrekking van persoonsgegevens

1. Tenzij zulks noodzakelijk is ter uitvoering van een wettelijk voorschrift is voor verstrekking aan persoonsgegevens aan derden de toestemming nodig van betrokkene.
2. De persoonsgegevens worden alleen verstrekt aan personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.

Artikel 9 Vertegenwoordiging betrokkene

1. Indien de betrokkene minderjarig is en de leeftijd van zestien jaren nog niet heeft bereikt of indien de betrokkene meerderjarig is en onder curatele is gesteld, dan wel er ten behoeve van de betrokkene een mentorschap is ingesteld, is in de plaats van de toestemming van de betrokkene de toestemming van zijn wettelijk vertegenwoordiger vereist. De toestemming wordt schriftelijk vastgelegd. Indien de betrokkene een schriftelijk machtiging heeft afgegeven ter zake diens vertegenwoordiging jegens verwerker, dan is mede toestemmingdoor de schriftelijk gemachtigde vereist.
2. Een toestemming kan door de betrokkene, diens schriftelijk gemachtigde of zijn wettelijk vertegenwoordiger te allen tijde worden ingetrokken.

Artikel 10 Kennisgeving en informatieverstrekking

1. De verantwoordelijke zal een verwijzing naar het reglement opnemen op de website, een toelichting op de AVG en verwijzing naar het privacy reglement opnemen in de informatiemap medewerkers en vrijwilligers en in het beleidsplan van de kinderboerderij en op aanvraag digitaal ter beschikking stellen.
2. Indien de te verwerken gegevens bij betrokkene zelf worden verkregen, dan dient deze op de hoogte te worden gesteld op het moment van het verzamelen van de gegevens. Indien de gegevens buiten de betrokkene om verkregen worden, dan dient betrokkene geïnformeerd te worden op het moment van vastlegging of van eerste verstrekking aan derden.
3. Indien andere doelen dan omschreven in art. 3.4 een doelstelling vormen van de verwerking van persoonsgegevens, heeft de verantwoordelijke de plicht de betrokkene gericht vooraf te informeren omtrent de aard van de gegevens, die over de betrokkene verwerkt worden, alsmede omtrent de doeleinden die daarmee worden nagestreefd.
4. Indien de persoonsgegevens voor een dergelijk ander doel verwerkt worden en identificeerbaar zijn, is toestemming voor de verwerking van de persoonsgegevens door de betrokkene vereist. Indien de persoonsgegevens niet identificeerbaar verwerkt worden, is geen toestemming van de betrokkene vereist.

Artikel 11 Inzage en afschrift van verwerking van gegevens

1. De betrokkene heeft recht op inzage in en afschrift van de op zijn/haar persoon betrekking hebbende verzamelde en verwerkte gegevens. De betrokkene dient daartoe een schriftelijk verzoek in te dienen bij de verantwoordelijke.
2. Aan een verzoek als bedoeld in dit artikel wordt binnen vier weken na ontvangst van het verzoek voldaan.
3. Het recht op inzage wordt alleen toegestaan aan betrokkene of diens gemachtigde. Betrokkene of diens gemachtigde dienen zich te kunnen legitimeren.
4. De verantwoordelijke kan weigeren aan een in dit artikel bedoeld verzoek te voldoen voor zover dit noodzakelijk is in het belang van de bescherming van de rechten en vrijheden van anderen, de voorkoming, opsporing en vervolging van strafbare feiten.

Artikel 12 Correctie/verbetering, aanvulling, verwijdering of afscherming van gegevens

1. De betrokkene kan het bestuur verzoeken om verbetering, aanvulling, verwijdering, gedeeltelijke verwijdering of afscherming van op hem betrekking hebbende gegevens, indien deze feitelijk onjuist voor het doel van de verwerking, onvolledig of niet ter zake dienend zijn dan wel in strijd met een wettelijk voorschrift verwerkt zijn/worden.
2. Het bestuur, bericht de verzoeker zo spoedig mogelijk doch uiterlijk binnen vier weken na ontvangst van het verzoek schriftelijk of, en dan wel in hoeverre, hij daaraan voldoet. Een weigering is met redenen omkleed.
3. Het bestuur die op verzoek persoonsgegevens heeft verbeterd, aangevuld, verwijderd of afgeschermd, is verplicht aan derden aan wie de gegevens daaraan voorafgaand zijn verstrekt, zo spoedig mogelijk kennis te geven van de verbetering, aanvulling, verwijdering of afscherming, tenzij dit onmogelijk blijkt of een onevenredige inspanning vraagt.

Artikel 13 Vernietiging van gegevens

1. De betrokkene heeft het recht te verzoeken om vernietiging van tot zijn persoon identificeerbare gegevens. Daartoe dient hij een schriftelijk gemotiveerd verzoek in te dienen bij het bestuur.
2. Het verzoek tot vernietiging kan slechts geweigerd worden indien bewaring op grond van een wettelijk voorschrift vereist is, dan wel redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de betrokkene.
3. De betreffende gegevens worden uiterlijk binnen drie maanden na daartoe strekkend verzoek vernietigd. Het bestuur deelt zijn beslissing schriftelijk aan de betrokkene mede.

Artikel 14 Recht van verzet

1. Indien gegevens worden verwerkt in verband met de totstandbrenging of de instandhouding van een directe relatie tussen de verantwoordelijke of een derde en de betrokkenen met het oog op werving voor commerciële of charitatieve doelen, moet de betrokkene uitdrukkelijke toestemming hebben gegeven voor deze verwerking. De betrokkene kan hiertegen bij de verantwoordelijke te allen tijde kosteloos verzet aantekenen.
2. De verantwoordelijke zal in het geval van verzet maatregelen treffen om deze vorm van verwerking terstond te beëindigen.

Artikel 15 Bewaartermijnen

1. Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de realisatie van de doelen waarvoor zij worden verzameld of vervolgens worden verwerkt, conform het bepaalde in de wet.
2. Persoonsgegevens dienen in elk geval langer dan de vastgestelde bewaartermijnen bewaard te worden indien:
   - de betrokkene hierom verzoekt;
   - de bewaring van aanmerkelijk belang is voor een ander dan de betrokkene, waaronder de verantwoordelijke (bijvoorbeeld t.a.v. risicodossiers).

Artikel 16 Archivering

De verantwoordelijke treft de nodige voorzieningen ter bevordering van de juistheid en volledigheid van de opgenomen gegevens en draagt zorg voor maatregelen van technische en organisatorische aard ter beveiliging van de verwerking van persoonsgegevens zoals opgenomen in bijlage 1 (verwerkingsregister).

Artikel 17 Datalekken

1. De verantwoordelijke zal op grond van het protocol 'Melding Datalekken' datalekken melden bij de autoriteit Persoonsgegevens en betrokkene(n) te informeren.
2. De verantwoordelijke verplicht de bewerker in een verwerkersovereenkomst tot het melden van datalekken.

Artikel 18 Sancties

Bij overtreding van de voorgeschreven toegangsbevoegdheden en wanneer sprake is van onbevoegde toegang, raadpleging en wijziging van persoonsgegevens kan de verantwoordelijke de daarvoor geëigende maatregelen nemen.

Artikel 19 Onvoorzien

In gevallen waarin dit reglement niet voorziet beslist de verantwoordelijke, met in achtneming van het bepaalde in de wet en het doel en de strekking van dit reglement.

Artikel 20 Klachten

1. Indien de betrokkene van mening is dat de bepalingen van dit reglement niet worden nageleefd of indien hij andere redenen heeft tot klagen, dient hij zich te wenden tot de verantwoordelijke.
2. De verantwoordelijke zal de klacht conform het geldende klachtenreglement in behandeling nemen.

Artikel 21 Wijzigingen en inwerkingtreding

1. Wijzigingen in dit reglement worden aangebracht door de verantwoordelijke.
2. De wijzigingen in het reglement zijn van kracht vier weken nadat ze bekend zijn gemaakt aan betrokkenen.
3. Dit reglement is per [datum] in werking getreden en vastgesteld door het bestuur de vereniging Stads- en Kinderboerderijen Nederland (vSKBN).

Bijlage 1 Verwerkingsregister

Verwerkingsregister: In verband met andere type bestand, wordt deze apart toegevoegd

Bijlage 2. Procedure bij datalek vSKBN

Dit document beschrijft de procedure met daarin te nemen maatregelen die binnen de vSKBN genomen moeten worden bij een datalek volgens de meldplicht datalekken van de Algemene Verordening Gegevensbescherming (AVG).

Samenvatting

1. Is de meldplicht datalekken uit de AVG van toepassing?
2. Is een gebeurtenis te beschouwen als een datalek?
3. Moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?
4. Hoe en wanneer moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?
5. Moet het datalek ook worden gemeld aan de betrokkene, dat is degene van wie de persoonsgegevens zijn gelekt?
6. Hoe en wanneer moet het datalek worden gemeld aan de betrokkene?
7. Welke gegevens moeten worden vastgelegd?
8. Registratie en evaluatie

Definities

Datalek	*een inbreuk op de beveiliging van persoonsgegevens waardoor die gegevens verloren gaan of onrechtmatig worden verwerkt*
Bewerker	*degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen*
Persoonsgegevens	*elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*
Autoriteit Persoonsgegevens (AP)	*de organisatie die tot taak heeft toe te zien op de verwerking van persoonlijke gegevens krachtens de privacywetgeving*
Betrokkene	*diegene op wie een persoonsgegeven betrekking heeft*

Reikwijdte van de meldplicht datalekken

Indien er sprake is van een inbreuk op de beveiliging van persoonsgegevens als bedoeld in de artikelen 32 en 33 van AVG die leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens dan wordt dit als een datalek gekwalificeerd en zal dit bij de Autoriteit Personengegevens moeten worden gemeld.

Er moet dus sprake zijn van het 'lekken van data' en dat het lekken een onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens tot gevolg heeft. Een enkele tekortkoming of kwetsbaarheid in de beveiliging is geen datalek. Dit is wel het geval wanneer redelijkerwijs niet kan worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid.

Datalekken kunnen ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen);
- calamiteit (brand datacentrum, wateroverlast);
- verloren USB stick of laptop;
- verzenden van email met emailadressen van alle geadresseerden;
- maar ook het onrechtmatige verwerking van gegevens (DDS applicatie aantekening VOA).

Meldingen
Een datalek kan door een bestuurslid, lid of medewerker worden ontdekt. Deze ontdekking wordt aan het bestuur medegedeeld die vervolgens over zal gaan tot de beoordeling of er sprake is van een datalek. De manager/beheerder, in samenwerking met het bestuur onderzoeken het incident. Hierbij is aandacht voor de volgende aspecten:

1. wat is de aard van het datalek (bijzondere of gevoelige gegevens dienen per definitie te worden gemeld) ;
2. wat is de oorzaak dat dit incident heeft plaatsgevonden;
3. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
4. is de organisatie verwijtbaar.

Indien sprake is van een datalek dan zal het bestuur binnen 2 dagen maar niet later dan 72 uur na ontdekking zorg dragen voor een melding bij de Autoriteit Persoonsgegevens (https://datalekken.autoriteitpersoonsgegevens.nl/). In ieder geval zal gemeld moeten worden:

- Aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, beschrijving gegevens;
- Beschrijving van de te verwachten gevolgen;
- Getroffen en/of voorgestelde maatregelen;
- Informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- Contactgegevens voor betrokkene

Let op: Indien de melding niet binnen 72 uur bij de Autoriteit Persoonsgegevens plaatsvindt, dan goede onderbouwing als reden voor vertraging. Anders kan er een boete opgelegd worden!

Registratie
Het bestuur zal een overzicht bijhouden van alle datalekken binnen de vSKBN. Per datalek wordt in het overzicht aangegeven wat de feiten en gegevens zijn van de aard van de inbreuk. Een datalek wordt voor minimaal 1 jaar in het overzicht bewaard.

Na de melding datalek ontvangt de vSKBN een ontvangstbevestiging van de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens zal contact met de kinderboerderij opnemen mocht na een melding aanleiding zijn om nadere te ondernemen. Hierbij zal met name de herkomst van de melding worden geverifieerd en kan de kinderboerderij aanwijzingen van de Autoriteit Persoonsgegevens krijgen.

Wanneer vaststaat dat een datalek bij de Autoriteit Persoonsgegevens gemeld moet worden, dan dient hierna beoordeeld te worden of een datalek ook aan betrokkene moet worden gemeld. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. In het geval van de kinderboerderij worden de bezoekers, vrijwilligers en werknemers, stagiaires, derden en sponsoren aangemerkt als betrokkenen indien het om persoonsgegevens gaat van de natuurlijke persoon.

Een betrokkene moet ook onverwijld in kennis worden gesteld van de inbreuk. Indien de inbreuk waarschijnlijk geen ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene of wanneer de technische beschermingsmaatregelen (bijvoorbeeld encryptie) die zijn genomen voldoende bescherming bieden, kan melding van het datalek aan de betrokkene achterwege blijven. Na de melding bij de Autoriteit Persoonsgegevens en eventuele getroffen maatregelen zal (indien nodig) terugkoppeling plaatsvinden bij de betrokkene(n).

Taken, verantwoordelijkheden en bevoegdheden

1. Iedere medewerker of verwerker van de vSKBN die direct of indirect kennis draagt of krijgt van een datalek, is verplicht dit direct te melden aan het bestuur;
2. Het bestuur is verantwoordelijk voor het onderzoeken van het incident;
3. Het bestuur is verantwoordelijk voor de beoordeling of een datalek aan de Autoriteit Persoonsgegevens gemeld moet worden respectievelijk of een datalek aan de betrokkene moet worden gemeld;
4. Het bestuur is verantwoordelijk voor de melding van datalekken bij de Autoriteit Persoonsgegevens;
5. Het bestuur is verantwoordelijk voor het bijhouden van een overzicht van alle datalekken die onder de meldplicht vallen voor minimaal 1 jaar;
6. Het bestuur is verantwoordelijk voor het ondernemen van preventieve, reparatoire en repressieve maatregelen.
7. Het bestuur is verantwoordelijk voor de melding richting betrokkene(n) en tevens (indien van toepassing) de terugkoppeling.

Interne controle

1. Het bestuur analyseert jaarlijks de meldingen datalekken en stelt indien nodig in samenwerking met het bestuur een verbeterplan ter voorkoming van datalekken.
2. Het bestuur beoordeelt minimaal jaarlijks of de procedure en de uitvoering van dit protocol nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de protocol.

Bijlage 3: Formulier Melding Datalek

Dit gedeelte alleen in te vullen door de melder

Formulier opsturen als bijlage naar	:	Bestuur vSKBN

1)	Organisatie gegevens				
	Organisatie	:	**Vereniging Stads- en Kinderboerderijen Nederland**		
	Adres	:			
	Postcode	:			
	Plaats	:			
	Telefoon	:			
2)	**Melder van het datalek** - met wie de beheerder contact kan opnemen voor meer informatie				
	Naam	:			
	Functie	:			
		:			
		:			
		:			
	Telefoon	:			
	E-mailadres	:			
3)	**Wat is er gebeurd?** Geef een beschrijving van het incident, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan:				
4)	**Wanneer vond het datalek plaats?**				
	Op bepaalde datum	:			
	Tussen (begindatum periode) en (einddatum periode)	:			
	Tijdstip	:			
5)	**Waar vond het datalek plaats?**				
	Werkplek bij de kinderboerderij	:			
	Werkplek bij bewerker	:			
	Werkplek bij andere organisatie	:			
	Anders	:			
6)	**Van hoeveel personen zijn persoonsgegevens via datalek naar buiten gebracht of verloren gegaan?** (Vul een aantal in)				
	Minimaal: (vul aan)	:			
	Maximaal: (vul aan)	:			
7)	**Wat is de aard van het datalek?** (er zijn meerdere antwoorden mogelijk)				
	Lezen (vertrouwelijkheid)			□	
	Kopieën (gemaakt en onbewust verloren)			□	
	Gegevens verkeerd aangepast (integriteit)			□	
	Verlies, verwijderen of vernietigen (beschikbaarheid)			□	
	Diefstal (vanuit kantoor, thuis, auto, enz.)			□	
	Anders:			□	
8)	**Om welke gegevensdragers (middelen) of devices (apparaten) gaat het?**				
	Papier			□	
	USB, portal harddisk, Smart Phone, tablet, laptop, SIM card anders,…..			□	
	Digitale informatie-uitwisseling/online communicatie (verkeerde geadresseerde E-mail, SMS, whats app en/of Wetransfer) anders,….			□	
	Anders:			□	

9)	**Om welke typen persoonsgegevens gaat het?** (er zijn meerdere antwoorden mogelijk)		
	a) Naam-, adres- en woonplaatsgegevens	□	
	b) Telefoonnummers	□	
	c) E-mailadressen of andere adressen voor digitale communicatie	□	
	d) Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)	□	
	e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)	□	
	f) Burgerservicenummer (BSN) of sofi-nummer	□	
	g) Paspoortkopieën of kopieën van andere legitimatiebewijzen	□	
	h) Geslacht, geboortedatum en/of leeftijd	□	
	i) Bijzondere gegevens (zoals medische gegevens, informatie over religie etc.)	□	
	j) Behandel/Onderwijs/Onderzoek informatie	□	
	k) Overige gegevens, namelijk (vul aan)	□	
	Ruimte voor verdere toelichting		

Dit gedeelte alleen in te vullen door het bestuur vSKBN

Datum en tijd ontvangst melding?	**Datum:**	**Tijd:**
Nader onderzoek / analyse? Primair vaststellen of melding bij Autoriteit Persoonsgegevens (AP) gedaan moet worden. Indien de oorzaak niet bij de kinderboerderij ligt maar bij een verwerker, dan deze betrekken bij het onderzoek. <u>Let op de 72 uur waarbinnen dit moet plaatsvinden!!</u> www.autoriteitpersoonsgegevens.nl	□ JA □ NEE	**Wie zijn bij het onderzoek / analyse betrokken?** **Wie heeft de leiding over het onderzoek?**
Moet het datalek aan de AP worden gemeld? - zie protocol -	□ JA	**Datum en tijdstip melding?** **Door wie?** = svp kopie melding + ontvangst toevoegen aan het dossier =
	□ NEE	**Reden waarom niet en wie waren betrokken bij de beslissing om geen melding te doen?**
Volgt er een opvolgactie vanuit AP?	□ JA □ NEE	Indien Ja, svp alle stukken nalopen en voorbereiden voor nader onderzoek.
Moet het datalek worden gemeld aan de betrokkene(n)? Een melding is vereist als er sprake is van een concrete kans op negatieve gevolgen voor de persoonlijke levenssfeer en de verwezenlijking daarvan, tenzij er zwaarwegende redenen zijn om de melding niet te doen. Melding aan betrokkene(n) ook binnen 72 uur! - zie de betreffende richtlijnen van de AP -	□ JA	**Datum en tijdstip melding?** **Door wie?** = svp kopie melding (letterlijke weergave) toevoegen aan het dossier =
	□ NEE	**Waarom zie je af van het melden van het datalek aan de betrokkenen?** □ De technische beschermingsmaatregelen die wij hebben getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten □ Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (vul aan) □ Wij hebben zwaarwegende redenen om de melding aan de betrokkene achterwege te laten (artikel 43, Wbp), namelijk: (vul aan)

		□ Anders, namelijk (artikel 34a, lid 6, Wbp): (vul aan)
Evaluatie en dossiervorming Evalueer zowel (de oorzaken van) het incident zelf als de afhandeling ervan, en beoordeel of een aanpassing van de organisatie inclusief ICT-omgeving noodzakelijk of wenselijk is, en bespreek dit binnen het bestuur. Stel vast dat alle aspecten rond het incident adequaat zijn vastgelegd, en archiveer alle relevante vastleggingen rond het incident .		
Zijn er aanpassingen nodig n.a.v. onderzoek / evaluatie? Dus, welke technische en/of organisatorische maatregelen heeft de Parkhoeve getroffen om het datalek aan te pakken en om verder datalekken te voorkomen?	□ JA □ NEE	svp omschrijven:

Akkoord bestuur d.d.	**Naam en functie bestuurder:**	**Handtekening:**
Formulier gearchiveerd d.d.	**Naam beheerder:**	**Paraaf:**

Aanvulling technische (hulp)vragen (indien van toepassing)

	Zijn de persoonsgegevens versleuteld, gehasht* of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? **) Gehashte data is niet te herleiden tot de oorspronkelijke data: er wordt namelijk gebruik gemaakt van een onomkeerbaar algoritme.*		Ja/Nee
	Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?		

Autoriteit Persoonsgegevens (AP): autoriteitpersoonsgegevens.nl

Bijlage 4: Overeenkomst en instructie gegevensbeveiliging

Overeenkomst en instructie gegevensbeveiliging voor bestuursleden

Door het nemen van de juiste beveiligingsmaatregelen en het in acht nemen van de juiste beveiligingsprocedures willen we voorkomen dat onbevoegden toegang krijgen tot onze systemen, onze vertrouwelijke informatie en de persoonsgegevens die wij beheren. Neem daarom gegevensbeveiliging serieus en volg onderstaande instructies en werkwijzen zorgvuldig op.

Computers, laptops en tablets

1. Beveilig de toegang tot je computers, laptops, tablets en/of smartphone met een sterk en uniek wachtwoord.
2. Stel indien mogelijk een multifactor authenticatie in.
3. Stel de schermbeveiliging in op maximaal 5 minuten.
4. Installeer betrouwbare antivirus-software en houd deze up-to-date.
5. Stel een firewall in en houd deze up-to-date.
6. Ga alleen online via een beveiligde verbinding (zijnde geen openbaar publiek netwerk).
7. Stel de automatische update-functie in om besturingssystemen en andere software up-to-date te houden.
8. Download alleen betrouwbare nieuwe software en apps.

Losse externe dataopslagapparatuur

1. Voorbeelden van externe dataopslagapparatuur zijn USB-sticks, externe harde schijven (cloud), geheugenkaartjes en cd's/dvd's/blu-ray-discs.
2. Beveilig de toegang tot de losse dataopslagapparatuur met een sterk en uniek wachtwoord.
3. Beveilig de toegang tot de individuele documenten op de losse dataopslagapparatuur met een sterk en uniek wachtwoord.
4. Verwijder na gebruik gegevens van de losse dataopslagapparatuur.

Smartphone

1. Beveilig de toegang tot je telefoon met een pincode van minimaal 4 cijfers.
2. Stel 'zoek mijn iPhone/Android' in en test of dit werkt.
3. Download alleen apps uit de officiële appstores: App-store, Google Play en Windows-store.

Fysieke documenten

1. Voorzie documenten met vertrouwelijke informatie of persoonsgegevens van een duidelijk predicaat 'vertrouwelijk'.
2. Berg fysieke documenten met vertrouwelijke informatie of persoonsgegevens op in een afsluitbare opslagruimte en zorg dat alleen bevoegden toegang hebben tot deze fysieke documenten.

De ondergetekende heeft toegang tot (kruis aan wat van toepassing is):

0 Online databestand met leden (Davilex)
0 Lijst met mailadressen leden (Mailchimp)
0 Eigen pc/ datadrager/ smartphone met documenten en/ of mails die persoonsgegevens bevatten
0 Gegevens (en mails) die zijn opgeslagen in de cloud en persoonsgegevens bevatten
0 Overig, te weten:

Ondergetekende verklaart dat hij/zij de bovengenoemde instructies hanteert, welke van toepassing zijn op onderstaande situatie(s):

Datum:

Naam:

Handtekening:

Bijlage 5 Toestemmingsformulier verwerking persoonsgegevens

Van de leden die ons ondersteunen hebben we gegevens nodig. De AVG (Algemene Verordening Gegevensbescherming) geeft aan dat we hiervoor toestemming moeten vragen en moeten uitleggen op welke manier we met deze gegevens omgaan. Dit doen we door middel van dit formulier.

Via onze nieuwsbrief houden we u op de hoogte van activiteiten en nieuws. Afmelden kan op elk moment via de link onderaan de nieuwsbrief.

0 Ja, ik wil de digitale nieuwsbrief van de kinderboerderij (blijven) ontvangen

Verwerking van de persoonsgegevens:

- *De toestemming kan op ieder moment worden ingetrokken, bij voorkeur schriftelijk.*
- *De gegevens kunnen op aanvraag worden ingezien. Hiervoor is een schriftelijk verzoek nodig bij de beheerder.*
- *De gegevens worden digitaal in de cloud bewaard en er wordt een back-up van gemaakt. Deze gegevens zijn beveiligd en alleen toegankelijk met een wachtwoord.*
- *De gegevens zijn alleen toegankelijk voor de beheerder, de medewerker die de adopties verwerkt en de communicatie verzorgd hiervoor en de administratief medewerker ten bate van de betalingen.*
- *Wanneer de dieradoptant stopt worden de persoons- of bedrijfsgegevens verwijderd uit de administratie na een periode van 7 jaar (verplichte bewaartermijn voor de belastingdienst).*
- *Wanneer de dieradoptant stopt wordt de foto na beëindigen van de adoptietermijn van het adoptiebord en onze Facebookpagina gehaald.*
- *Het mailadres wordt verwijderd van de mailinglijst.*

Meer informatie is te lezen in het Privacyreglement. Deze is digitaal op te vragen bij de beheerder.

Bijlage 6 Toestemmingsformulier gebruik beeldmateriaal

- **Ondergetekende geeft hierbij toestemming zich te laten fotograferen en/of filmen.**
- **Tevens verklaart hij/zij ermee in te stemmen dat een selectie van de gemaakte foto's of film wordt opgenomen in de beeldbank van de vSKBN ten behoeve van gebruik in communicatiemiddelen en geeft hij/zij toestemming voor gebruik van deze foto's in publicaties van de vSKBN.**

Toelichting: Het gaat om foto's of filmmateriaal waarmee een persoon geïdentificeerd kan worden. Dat betekent dus herkenbaar in beeld is.

Naam	
E-mail	
Telefoonnummer	

Ondertekening

Plaats	
Datum	
Handtekening *(bij jonger dan 16 jaar handtekening van ouder / rechtsgeldig vertegenwoordiger)*	

Beschrijving soort foto/ film

Locatie:

_____

Toelichting op foto/ film situatie: _____

_____

_

_____

_

Beschrijving persoon:

_____

_____

- *De toestemming kan op ieder moment worden ingetrokken, bij voorkeur schriftelijk.*
- *Deze gegevens worden bewaard [invullen]*

Toestemmingsformulier verwerking persoonsgegevens

Van de bestuursleden, medewerkers en vrijwilligers die bij ons werkzaamheden verrichten, hebben we gegevens nodig. De AVG (Algemene Verordening Gegevensbescherming) geeft aan dat we je hiervoor toestemming moeten vragen en uitleggen op welke manier we met je gegevens omgaan. Dit doen we door middel van dit formulier.

De ondergetekende,

Naam	
Woonplaats	
Geboortedatum	

Verwerken persoonsgegevens
Geeft met dit formulier toestemming voor het verwerken van zijn / haar persoonsgegevens door de vSKBN in het kader van de navolgende doeleinden:

- Inschrijving als vrijwilliger
- Inschrijving als bestuurslid

Dit wordt gebruikt ten bate van informatie voor de werkzaamheden en communicatie.

Ik geef hier WEL / GEEN toestemming voor.

Gebruik beeldmateriaal: foto's en films
Via onze website en social media kanalen houden we iedereen graag op de hoogte van de activiteiten van de vSKBN. Hiervoor maken we gebruik van foto's en video's. Voor de toestemming gaat het om foto's of filmmateriaal waarmee je als persoon geïdentificeerd kan worden. Dat betekent dus dat je herkenbaar in beeld bent.

Ik heb WEL / GEEN bezwaar tegen het plaatsen van foto's en video's waarop ik te zien ben.

Datum:

Handtekening

Verwerking van de persoonsgegevens:

- *De toestemming kan op ieder moment worden ingetrokken, bij voorkeur schriftelijk.*
- *Wanneer de betrokkene stopt met werkzaamheden worden de papieren gegevens versnipperd en de gegevens verwijderd van de computer.*
- *Het mailadres wordt verwijderd van de mailinglijst.*