

Eigenaar: Directie Stichting Boerderij 'De Viermarken' en Viermarkenraad

Evaluatie datum: maart 2024

1. BEGRIPSBEPALINGEN.

1. **PERSOONSgegevens:** elk gegeven over een geïdentificeerde natuurlijke persoon.
2. **BIJZONDERE PERSOONS GEGEVENS:** gegevens over godsdienst of levensovertuiging, ras, politieke gezindheid, lidmaatschap van een vakvereniging, gezondheid, seksuele leven, strafrechtelijke persoonsgegevens of persoonsgegevens over onrechtmatig of hinderlijk handelen.
3. **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.
4. **VERSTREKKEN VAN GEGEVENS:** het bekend maken of ter beschikking stellen van gegevens.
5. **BESTAND:** elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens op een functioneel bepaalde wijze verspreid is, dat toegankelijk is en betrekking heeft op verschillende personen.
6. **BETROKKENE:** degene op wie een persoonsgegeven betrekking heeft. Binnen "De Viermarken" wordt hieronder verstaan dat degene die de diensten van 'De Viermarken' afneemt of diens vertegenwoordiger.
7. **VERANTWOORDELIJKE:** de persoon die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Deze persoon is verantwoordelijk voor bewerking en gebruik van de gegevens.
8. **BEWERKER:** degene die ten behoeve van de verantwoordelijke, het beheer heeft over de verwerking van de betreffende persoonsgegevens.
9. **TOESTEMMING VAN BETROKKENE:** elke vrije en specifieke, en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.
10. **DIRECTIE:** de directeur die als taak heeft toe te zien op de verwerking van persoonsgegevens. Dus daar verantwoordelijk voor is.

2. REIKWIJDTE

Dit reglement is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van de persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

3. DOEL

1. Het doel van dit reglement is een praktische uitwerking te geven van de bepalingen van de Wet Bescherming Persoonsgegevens, verder te noemen WBP/ WGBO de wet geneeskundige behandelovereenkomst.
2. Dit reglement is van toepassing binnen Stichting Boerderij 'De Viermarken' te Enschede

4. VERTEGENWOORDIGING

1. Indien de betrokkene ouder is dan achttien jaar en niet in staat kan worden geacht tot een redelijke waardering van zijn/haar belangen ter zake, treedt in volgorde als hier weergegeven de vertegenwoordiger voor hem/haar op.
 - Indien de betrokkene onder curatele staat of ten behoeve van hem/haar het mentorschap is ingesteld: De curator/mentor.
 - Indien de betrokkene deze schriftelijk heeft gemachtigd: de persoonlijk gemachtigde.
 - Indien de persoonlijk gemachtigde ontbreekt of niet optreedt: de echtgenoot of andere levensgezel van de betrokkene.
 - Indien een echtgenoot of levensgezel dat niet wenst of ontbreekt: een ouder, broer of zus of kind van de betrokkene.
2. De persoon, die in de plaats treedt van de betrokkene, betracht de zorg van een goed vertegenwoordiger. Hij/Zij is gehouden betrokkene zoveel mogelijk bij de vervulling van zijn/haar taken te betrekken.

5. VOORWAARDEN VOOR RECHTMATIGE VERWERKING.

1. Persoonsgegevens worden in overeenstemming met dit reglement op behoorlijke nette en zorgvuldige wijze verwerkt.
2. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de 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 verantwoordelijke draagt er zorg voor dat er passende technische en organisatorische maatregelen worden uitgevoerd ter beveiliging tegen verlies of enige vorm van onrechtmatige verwerking.

6. VERWERKING VAN PERSOONSgegevens

Persoonsgegevens mogen slechts worden verwerkt indien aan één van de onderstaande voorwaarden is voldaan:

1. De betrokkene voor de verwerking zijn toestemming heeft verleend.
2. Dit noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor handelingen die op verzoek van de betrokkene worden verricht en die noodzakelijk zijn voor het sluiten van een overeenkomst.
3. Dit noodzakelijk is om een wettelijke verplichting na te komen.
4. Dit noodzakelijk is ter bestrijding van ernstig gevaar voor de gezondheid van betrokkene.
5. Dit noodzakelijk is met het oog op belang van de verantwoordelijke of van een derde en het belang van degene van wie de gegevens worden verwerkt niet prevaleert.

7. REGELS VOOR DE VERWERKING VAN BIJZONDERE PERSOONSGEGEVENS.

Bijzondere persoonsgegevens worden slechts verwerkt indien aan één van de volgende voorwaarden is voldaan.

1. De verwerking geschiedt met uitdrukkelijke toestemming van de betrokkene.
2. De verwerking geschiedt door medewerker van 'De Viermarken' voor zover dat noodzakelijk is in aanvulling op de verwerking van persoonsgegevens betreffende iemands gezondheid met het oog op een goede behandeling, begeleiding, ondersteuning of verzorging van de betrokkene, dan wel noodzakelijk is voor het beheer van de betreffende zorg locatie
3. De gegevens worden alleen verwerkt door personen die uit hoofde van hun functie, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.
4. Zonder toestemming van de betrokkene kunnen ten behoeve van statistiek of wetenschappelijk onderzoek aan een ander gegevens over de cliënt worden verstrekt indien:
 - Het vragen van toestemming in redelijkheid niet mogelijk is en met betrekking tot de uitvoering van het onderzoek is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de cliënt niet wordt geschaad.
 - Het vragen van toestemming, gelet op de aard en het doel van het onderzoek in redelijkheid niet kan worden verlangd en de hulpverlener zorg heeft gedragen dat de gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen wordt voorkomen.
 - Verstrekking is pas mogelijk indien het onderzoek het algemeen belang dient.
 - Het onderzoek niet zonder desbetreffende gegevens kan worden uitgevoerd.
 - Voor zover de betrokken cliënt tegen een verstrekking niet uitdrukkelijk bezwaar heeft gemaakt.
 - De betrokkene zelf deze gegevens al openbaar heeft gemaakt.
 - Als de verwerking noodzakelijk is voor het vaststellen, het uitoefenen of het verdedigen van een recht in een gerechtelijke procedure.

8. INFORMATIEVERSTREKKING AAN DE BETROKKE NE

1. Indien bij de betrokkene zelf de persoonsgegevens worden verkregen, deelt de verantwoordelijke voor het moment van verkrijging de betrokkene mede:
 - Zijn identiteit.
 - De doeleinden van de verwerking waarvoor de gegevens zijn bestemd, tenzij de betrokkene daarvan al op de hoogte is.
 - Bij verkrijging van persoonsgegevens buiten de betrokkene om, verstrekt de verantwoordelijke deze gegevens op het moment dat de verantwoordelijke de gegevens vastlegt.
2. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

3. Het bepaalde onder 2 is niet van toepassing indien de mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast.

9. RECHT OP INZAGE EN AFSCHRIFT VAN OPGENOMEN PERSOONSgegevens

1. De betrokkene heeft het recht kennis te nemen van de op zijn persoon betrekking hebbende verwerkte gegevens.
2. De gevraagde inzage en/of het gevraagde afschrift zal uiterlijk binnen vier weken worden verstrekt.
3. De binnen 'De Viermarken' gevolgde werkwijze bij inzage is in bijlage 2 van deze notitie opgenomen.

10. RECHT OP AANVULLING, CORRECTIE OF VERWIJDERING VAN OPGENOMEN PERSOONSgegevens

1. Desgevraagd worden de opgenomen gegevens aangevuld met een door de betrokkenen afgegeven verklaring met betrekking tot de opgenomen gegevens.
2. De betrokkene kan verzoeken om correctie van op hem/haar 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 in de verwerking voor komen.
3. De verantwoordelijke draagt zorg dat een beslissing tot correctie zo spoedig mogelijk wordt uitgevoerd.
4. De betrokkene kan verzoeken om verwijdering van op hem/haar betrekking hebbende gegevens.
5. De verantwoordelijke bericht degene schriftelijk, die het verzoek indient van correctie/verwijdering binnen vier weken na de schriftelijke ontvangst. Een weigering moet gegrond zijn. Dit wordt ook weer schriftelijk vastgelegd.
6. De verantwoordelijke verwijdert de gegevens binnen twee maanden na een daartoe strekkend verzoek van de betrokkene, tenzij redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de betrokkene, alsmede voor zover bewaring op grond van een wettelijk voorschrift vereist is.

11. BEWAREN VAN GEGEVENS

1. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.
2. In principe bewaart Stichting Boerderij "De Viermarken" persoonsgegevens niet langer dan noodzakelijk voor het doel waarvoor deze zijn verstrekt dan wel op grond van de wet is vereist. Na beëindiging van een dienstverband is dit 2 jaar, voor medische dossiers is dit 20 jaar. De financiële administratie wordt 10 jaar bewaard.
3. Indien de bewaartermijn van de persoonsgegevens is verstreken of de betrokkene doet een verzoek tot verwijdering vóór het verstrijken van de bewaartermijn, dan worden de desbetreffende gegevens verwijderd. Binnen een termijn van twee maanden.
4. Indien de bewaartermijn van de persoonsgegevens is verstreken of de betrokkene doet een verzoek tot verwijdering vóór het verstrijken van de bewaartermijn, dan worden desbetreffende gegevens verwijderd, binnen een termijn van twee maanden.
5. Verwijdering blijft achterwege wanneer redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de betrokkene, alsmede bewaring op grond van een

wettelijk voorschrift vereist is of indien daarover tussen de betrokkene en de verantwoordelijke overeenstemming bestaat.

KLACHTEN

1. Als de betrokkene van mening is dat de bepalingen van dit reglement niet worden nageleefd of andere reden heeft tot klagen, kan hij/zij zich wenden tot de wettelijk verantwoordelijke.
2. Als dit voor de betrokkene niet leidt tot een acceptabel resultaat heeft hij/zij de volgende mogelijkheden.
3. De Viermarkenraad in te lichten.
4. De verantwoordelijke schriftelijk te wijzen op hoofdstuk 8, de WBP (wet bescherming persoonsgegevens).

13. WIJZIGINGEN, INWERKINGTREDING EN INZAGE VAN DIT REGLEMENT

1. Wijzigingen van dit reglement worden aangebracht door de directie.
2. De wijzigingen van dit reglement zijn van kracht vier weken na de verspreiding van de nieuwe gegevens aan betrokkenen.

BIJLAGE 2: WERKWIJZE INZAKE INZAGE PERSOONSgegevens

1. Een verzoek tot inzage in de eigen persoonsgegevens kan mondeling, schriftelijk of via de e-mail worden ingediend. Het is verplicht dat de verzoeker de reden hiervoor aangeeft.
2. Binnen uiterlijk twee weken wordt er op dit verzoek mondeling, schriftelijk of per e-mail gereageerd.
3. In principe wordt inzage in alle gegevens gegeven, mits is voldaan aan de volgende voorwaarden.
 - De verzoeker is achttien jaar of ouder.
 - De verzoeker is degene op wie de gegevens betrekking hebben. De identiteit van de betrokkene is aangetoond.
4. Inzage kan gedeeltelijk geweigerd worden als de gevraagde informatie ook informatie betreft over anderen en deze persoon hiertegen desgevraagd bezwaar maakt.
5. Inzage kan geheel en gedeeltelijk geweigerd worden.
 - Ter voorkoming, opsporing en vervolging van strafbare feiten
 - Bij gewichtige economische en financiële belangen.
 - Voor het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van opsporing en vervolging van strafbare feiten
 - Als dat nodig is ter bescherming van rechten en vrijheden van anderen, waaronder die van "De Viermarken".
6. Inzage in de gegevens wordt verstrekt met instemming van de directie.
7. Verzoeker heeft het recht om correctie te vragen en verzet aan te tekenen.
8. Als de verzoeker het niet eens is met de beslissing dan dient deze schriftelijk bezwaar in bij zijn /haar werkbegeleider. Als dit niet tot voldoende resultaat leidt dan verwijst de vertegenwoordiger hem/haar door naar de klachtenfunctionaris die deze klacht moet afhandelen.

Datalek? Dit moeten we doen

Een datalek kan in iedere organisatie gebeuren. Door snel te handelen, beperken we de gevolgen van het datalek voor de privacy van klanten, medewerkers of werknemers. Ook kunnen we imagoschade voorkomen of beperken door snel in actie te komen bij een datalek. Verder moeten we het datalek mogelijk melden aan de Autoriteit Persoonsgegevens (AP) en soms ook aan de slachtoffers.

Een datalek is bijvoorbeeld:

- Persoonsgegevens die aan een verkeerde geadresseerde zijn verstuurd;
- Inzage in een medisch dossier door een onbevoegde medewerker;
- Het verlies van een USB-stick met niet-versleutelde persoonsgegevens;
- Een cyberaanval waarbij persoonsgegevens zijn buitgemaakt;
- Een besmetting met ransomware (gijzelsoftware) waarbij persoonsgegevens ontoegankelijk zijn gemaakt.

Er zijn 3 soorten datalekken:

1. Inbreuk op de vertrouwelijkheid: persoonsgegevens zijn openbaar gemaakt of er is toegang geweest tot persoonsgegevens. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.
2. Inbreuk op de integriteit: persoonsgegevens zijn gewijzigd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.
3. Inbreuk op de beschikbaarheid: de organisatie waar het datalek is (geweest) kan niet meer bij de persoonsgegevens komen. Of de gegevens zijn vernietigd. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.

Stappenplan datalek

Bij een datalek nemen we de volgende stappen:

1. Zorg voor overzicht op de situatie.
2. Neem onmiddellijk maatregelen om het datalek te stoppen en de schade van het datalek te beperken. Schat daarbij ook de risico's in.
3. Bepaal of u het datalek wel of niet moet melden aan de AP. Zo ja, doe dit dan onmiddellijk.
4. Bepaal of u de slachtoffers wel of niet moet informeren over het datalek. Zo ja, doe dit dan zo snel mogelijk.
5. Registreer het datalek in het datalekregister (zie bijlage 1: registratieformulier datalek)

Stap 1: Overzicht krijgen bij datalek

De eerste stap bij een datalek is zorgen voor overzicht op de situatie, zodat we de juiste vervolgstappen kunnen nemen. Daarvoor moeten we allereerst weten om wat voor soort datalek het gaat. (Zie ook bijlage 2: beoordelen datalek)

Als we weten om welke soort datalek het gaat, dan helpen de volgende vragen om verder overzicht te krijgen op de situatie:

- Wat is de oorzaak van het datalek?
- Wanneer is het datalek ontstaan? En is het datalek nog steeds gaande?

- Hoe lang na het ontstaan van het datalek is het ontdekt? En hoe is het ontdekt?
- Wat voor soort persoonsgegevens zijn gelekt? Bijvoorbeeld naam, adres, e-mailadres, creditcardgegevens en/of bijzondere persoonsgegevens.
- Hoeveel persoonsgegevens zijn er (bij benadering) gelekt? Om hoeveel personen gaat het?
- Om wat voor groepen mensen gaat het? Bijvoorbeeld klanten, werknemers, medewerkers, overige...
- Hoeveel onbevoegden hadden of hebben bij benadering (mogelijk) toegang tot de gelekte persoonsgegevens?
- Hebben we zicht op wie die onbevoegden zijn? En is het waarschijnlijk dat de onbevoegden kwade bedoelingen hebben met de gegevens? Of gaat het om een bekende, betrouwbare ontvanger?
- Hebben we zelf vooraf maatregelen getroffen waardoor de gelekte persoonsgegevens (deels) ontoegankelijk zijn voor onbevoegden? Bijvoorbeeld omdat de gegevens versleuteld zijn?

Stap 2: Beperken schadelijke gevolgen datalek

Ten eerste moeten we het datalek onmiddellijk zien te stoppen als het nog bestaat. Daarnaast moeten we maatregelen nemen om de negatieve gevolgen te beperken.

Voorbeelden van maatregelen om schade bij een datalek te beperken zijn:

- Een laptop, tablet of smartphone op afstand wissen of versleutelen.
- Een gepubliceerd bestand offline halen.
- Een verkeerde ontvanger vragen om een bevestiging dat de gegevens uit een brief of e-mail zijn vernietigd. Hoewel u op basis van zo'n bevestiging niet 100% zeker weet dat de gegevens gewist zijn, kunt u het wel meenemen in uw risico-inschatting.
- De toegang tot een medewerkersaccount of clouddienst op afstand blokkeren.
- Wanneer we verplicht zijn om de [slachtoffers te informeren](#), aangeven wat zij zelf kunnen doen om de schade te beperken.

Stap 3: Melden datalek en informeren slachtoffers

We kunnen verplicht zijn om het datalek binnen 72 uur te melden bij de AP. Ook kunnen we verplicht zijn om de slachtoffers te informeren over het datalek. (Zie bijlage3: [Datalek: wel of niet melden](#) en bijlage 4: hoe informeer je slachtoffers)

Stap 4: Registreren datalek in datalekregister

Volgens de AVG zijn we verplicht een datalekregister op te stellen en bij te houden. Hierin houdt staat welke datalekken er zijn geweest. In het register moeten we alle datalekken vastleggen die zich binnen onze organisatie hebben afgespeeld. Ook de datalekken die we niet aan de AP hebben gemeld.

Het doel van het datalekregister is dat we:

- Leren van eerdere datalekken en bewust bent van datalekken die in het verleden hebben plaatsgevonden;
- Effectieve maatregelen nemen om de kans op nieuwe, soortgelijke datalekken te verminderen;

- Met het datalekregister aan de AP kunnen laten zien dat we ons houden aan de meldplicht datalekken.
-

Vorm en inhoud datalekregister

De wettelijk verplichte informatie moet in het register worden opgenomen. Over elk datalek moeten we in ieder geval de volgende informatie vermelden:

- De feiten over het datalek, zoals de oorzaak, wat er precies is gebeurd en om welke persoonsgegevens het gaat;
- De gevolgen van het datalek;
- De corrigerende maatregelen die u heeft genomen.