VERWERKERSOVEREENKOMST

PARTIJEN

1. Verantwoordelijke; Vredehof Uitvaartverzorging, statutair gevestigd te Enschede, aan het adres Weth. Beversstraat 104 te Enschede, vertegenwoordigd door P. Swier, Algemeen Directeur

hierna te noemen: “Ik”,

en

2. Verwerker; [STATUTAIRE NAAM], statutair gevestigd te [PLAATS] aan het adres [ADRES], vertegenwoordigd door [NAAM EN/OF NAAM BESTUURDER]

hierna te noemen: “Jij”,

gezamenlijk aan te duiden als: “Wij”;

OVERWEGENDE DAT

Wij hebben op [DATUM] een Overeenkomst met betrekking tot [OMSCHRIJVING] gesloten. Ter uitvoering van onze Overeenkomst worden Persoonsgegevens verwerkt.

Ik hecht grote waarde aan het beschermen van deze Persoonsgegevens, daarom ben Ik verantwoordelijk voor de gegevens die Jij gaat verwerken en leggen wij onze afspraken vast, ook in verband met de eisen uit de Algemene Verordening Gegevensbescherming waar partijen zich aan wensen te houden.

Bij deze Verwerkersovereenkomst horen de volgende bijlagen:

1. Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen;

2. Overzicht met beveiligingsmaatregelen;

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

Hiermee leggen wij vast wat Jij wel en niet mag doen met de Persoonsgegevens.

Artikel 1. Definities:

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

1.1 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

1.2 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;

1.3 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 lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegeven betrekking hebben;

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief de bijlagen;

1.7 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;

1.8 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 ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (“Datalek”);

1.9 Toezichthoudende autoriteit: een onafhankelijke 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;

Artikel 2. Totstandkoming, doel, duur en beëindiging van deze Verwerkersovereenkomst

2.1 Deze verwerkersovereenkomst treedt in werking per datum ondertekening.

2.2 Deze verwerkersovereenkomst is onderdeel van de Overeenkomst tussen partijen en zal gelden voor zolang de Overeenkomst voortduurt. Jij verricht zelf alleen op basis van afspraken uit deze overeenkomst verwerkingen.

2.3 Indien de Overeenkomst eindigt, eindigt de Verwerkingsovereenkomst automatisch. Aparte opzegging is niet mogelijk.

2.4 Na beëindiging van deze Verwerkingsovereenkomst zullen de lopende verplichtingen voor jou, zoals het melden van Datalekken waarbij de Persoonsgegevens van mij betrokken zijn, en de plicht tot geheimhouding blijven voortduren.

2.5 Het doel van deze verwerkingsovereenkomst is [invullen, wat gaat de bewerker precies doen en waarom?]
Eventueel: Jij stelt ten behoeve van de verwerkingen ICT-middelen ter beschikking die door mij te gebruiken zijn voor de doelen zoals vermeld.

Artikel 3. Verwerken Persoonsgegevens

3.1 Jij zult alleen Persoonsgegevens verwerken in mijn opdracht op basis van deze verwerkersovereenkomst, en hebt geen zeggenschap over de Persoonsgegevens.
Jij volgt mijn instructies hierover op en je mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Ik jou daar van tevoren toestemming of opdracht voor geef.

3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Jij precies zal verwerken en voor welke verwerkingsdoeleinden.

3.3 Jij houdt je aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze conform de afspraken in deze verwerkingsovereenkomst.

3.4 Jij mag zonder mijn voorafgaande schriftelijke toestemming geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.

3.5 Wanneer Jij met mijn toestemming andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.

3.6 Wanneer Ik een verzoek krijg van een Betrokkene die zijn of haar privacy rechten wil uitoefenen, werk je daar binnen een termijn van 14 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.

3.7 Jij bent niet verantwoordelijk voor overige verwerkingen van persoonsgegevens, waaronder in ieder geval maar niet beperkt tot:
- het verzamelen van persoonsgegevens door mij;
- Verwerkingen door mij voor doeleinden, welke niet aan jou zijn gemeld;
- Verwerkingen door derden die ik heb ingeschakeld

3.8 Ik garandeer dat de inhoud, het gebruik en de opdracht tot de verwerkingen van de persoonsgegevens zoals bedoeld in deze Overeenkomst, niet onrechtmatig is en geen inbreuk maken op enig recht van derden.

Artikel 4. Beveiligen van Persoonsgegevens

4.1 Jij zorgt ervoor dat je de Persoonsgegevens voldoende beveiligt. Om verlies en onrechtmatige verwerkingen te voorkomen neem Jij passende technische en organisatorische maatregelen tegen verlies of tegen enige vorm van onrechtmatige verwerking zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de persoonsgegevens.

4.2 Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid daarover neem je op in Bijlage 2.

4.3 Ik blijf juridisch verantwoordelijk voor de naleving van de maatregelen zoals gesteld in deze Verwerkingsovereenkomst en moet er daardoor zeker van zijn dat jij de vereiste beveiligingsmaatregelen hebt getroffen. Ter controle zal Jij aan mij ieder jaar een rapportage sturen waarin de genomen maatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor zult Jij aan mij geen kosten in rekening brengen.

4.4 Ik mag een inspectie of naar eigen wens in jouw organisatie laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Hierbij zult Jij je medewerking verlenen, waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.

4.5 De kosten voor de uitvoering van deze audit zullen voor jouw rekening komen wanneer blijkt dat Jij je niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.

4.6 De controle op de algehele verwerking van Persoonsgegevens door jou kan, naast de audit mogelijkheid, ook gebeuren via zelfevaluatie. Jij zal hierbij aan Mij een rapport verstrekken waarin Jij aantoont dat je voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de jouw organisatie.

4.7 Wanneer een van ons vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Wij in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor de rekening van degene die de kosten maakt.

Artikel 5. Doorgeven van Persoonsgegevens

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

5.2 Jij mag alleen met voorafgaande schriftelijke toestemming van mij persoonsgegevens buiten Nederland verwerken, in een ander land binnen de Europese Unie. De hiervoor bedoelde toestemming zal niet op onredelijke gronden worden geweigerd.

5.3 In het geval dat een Betrokkene een verzoek doet tot inzage/verbetering/aanvulling/wijziging/afscherming met betrekking tot diens persoonsgegevens, zal Jij het verzoek doorsturen naar mij en zal ik het verzoek verder afhandelen. Jij mag de Betrokkene hiervan op de hoogte stellen.

Artikel 6. Geheimhouding

6.1 Jij zult de aan jouw verstrekte Persoonsgegevens geheimhouden jegens derden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.

6.2 Jij zult ervoor zorgen dat ook jouw personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.

6.3 Jij zult de aan jou verstrekte Persoonsgegevens niet voor een ander doel gebruiken dan waarvoor jij deze hebt verkregen, zelfs niet wanneer deze in een zodanige vorm is gebracht zodat deze niet tot Betrokkenen is te herleiden.

Artikel 7. Datalekken

7.1 In geval van een ontdekking van een mogelijk datalek zal Jij mij hierover informeren binnen 24 uur via [e-mailadres en telefoonnummer] en mij de informatie verstrekken die is aangegeven in (zie 7.1.5.), zodat Ik indien nodig een melding bij de Toezichthouder kan doen.

7.2 Na de melding van een Datalek aan mij, zult je mij op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek en de maatregelen die Jij hebt getroffen om de omvang van het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.

7.3 Het niet toegestaan dat Jij een melding van een Datalek doet aan de Toezichthouder en ook mag Jij de Betrokkenen niet informeren over het Datalek. Dit is mijn verantwoordelijkheid.

7.4 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.

Artikel 8. Aansprakelijkheid

8.1 Als Jij jouw verplichtingen uit deze Verwerkersovereenkomst niet nakomt, stel Ik jou daarvoor aansprakelijk.

8.2 Jij bent aansprakelijk voor alle schade en nadeel geleden door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door jouw werkzaamheden.

8.3 Indien Jij de verplichtingen in deze Verwerkersovereenkomst niet naleeft, ben Jij aan mij een direct opeisbare boete verschuldigd van € 2.500,- voor iedere overtreding en €500,- voor iedere dag dat je de overtreding begaat. Daarnaast behoud Ik het recht om aanvullende schadevergoeding te vorderen voor zowel directe als indirecte schade welke ik door jouw toedoen lijdt.

8.4 Onder directe schade wordt uitsluitend verstaan alle schade bestaande uit:
a. De tijd gemoeid met het melden van een datalek, de boete die ik krijg van instanties, het omzetverlies dat het geval is van het vertrekken van een klant waarbij het datalek de directe aanleiding is;
b. redelijke en aantoonbare kosten om de betreffende partij er toe te manen de

verwerkersovereenkomst (weer) deugdelijk na te komen;
c. redelijke kosten ter vaststelling van de oorzaak en de omvang van de schade voor zover betrekking hebbende op de directe schade zoals hier bedoeld is; en

d. redelijke en aantoonbare kosten die Verantwoordelijke heeft gemaakt ter voorkoming of beperking van de directe schade zoals in dit artikel bedoeld.

8.5 Onder indirecte schade wordt verstaan alle schade die geen directe schade is en daarmee in ieder geval, maar niet beperkt tot, gevolgschade, gederfde winst, gemiste besparingen, verminderde goodwill, schade door bedrijfsstagnatie, schade door het niet bepalen van marketingdoeleinden, schade verband houdende met het gebruik van door Verantwoordelijke voorgeschreven gegevens of databestanden, of verlies, verminking of vernietiging van gegevens of databestanden.

8.6 Jij bent aansprakelijk voor de aan mij opgelegde bestuurlijke boete door de Toezichthouder als de geleden schade het gevolg is van jouw onrechtmatig of nalatig handelen.

8.7 Ik ben niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar Jij de samenwerking mee bent aangegaan of waarvan Jij Persoonsgegevens verwerkt, als dit het gevolg is van jouw onrechtmatig of nalatig handelen.

8.8 De in dit artikel bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid of grove nalatigheid van de betreffende Partij of haar bedrijfsleiding.

8.9 Tenzij nakoming door de betreffende Partij blijvend onmogelijk is, ontstaat de aansprakelijkheid van die Partij wegens toerekenbare tekortkoming in de nakoming van de Overeenkomst slechts indien de ene Partij de andere Partij onverwijld schriftelijk in gebreke stelt, waarbij een redelijke termijn voor de zuivering van de tekortkoming wordt gesteld, en de andere Partij ook na die termijn toerekenbaar blijft tekortschieten in de nakoming van haarverplichtingen. De ingebrekestelling dient een zo volledig en gedetailleerd mogelijke omschrijving van de tekortkoming te bevatten, opdat de betreffende Partij in de gelegenheid wordt gesteld adequaat te reageren.

Artikel 9. Teruggave Persoonsgegevens en bewaartermijn

9.1 Na het beëindigen van deze Verwerkersovereenkomst geef Jij de Persoonsgegevens terug. Eventuele achtergebleven Persoonsgegevens zal je op een zorgvuldige en veilige manier vernietigen.

9.2 De Persoonsgegevens die Jij verwerkt volgens deze Verwerkersovereenkomst zult je vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van mij.

Artikel 10. Slotbepalingen

10.1 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.

10.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst.

10.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Wij dit samen schriftelijk afspreken.

Aldus door ons overeengekomen en ondertekend;

Verantwoordelijke:

Ondertekend voor en namens Vredehof Uitvaartverzorging

Naam: P. Swier

Functie: Algemeen Directeur

Datum en plaats:

Handtekening:

2. Bewerker

Ondertekend voor en namens [STATUTAIRE NAAM]

Naam:

Functie:

Datum en plaats:

Handtekening:

Bijlagen bij de verwerkingsovereenkomst

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

Ter voorkoming van het verliezen, wijzigen, ongeoorloofde verstrekking, ongeoorloofde toegang of anderszins onrechtmatige verwerkingen van de persoonsgegevens, dienen zowel technische als organisatorische beveiligingsmaatregelen getroffen te worden.

Bij technische maatregelen kan gedacht worden aan software technische beveiligingsoplossingen en het werken met beveiligde documenten en apparaten waarop persoonsgegevens opgeslagen worden. Bij organisatorische maatregelen kan gedacht worden aan fysieke maatregelen die moeten voorkomen dat onbevoegden toegang hebben tot apparaten of locaties waar persoonsgegevens zijn opgeslagen.

In deze bijlage moet een overzicht van de beveiligingsnormen opgenomen worden 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 emailadres, 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.

Doorhalen wat niet van toepassing is:

Technische beveiligingsmaatregelen

☐ Up to date virusscan

☐ Beveiligde USB-sticks

☐ Accurate beveiliging medewerkerstelefoon

☐ Bitlocker toegangsmechanisme

☐ Unieke inlogcode en wachtwoord (regelmatig aanpassen)

☐ Versleutelde email

☐ Geen onbeveiligde externe harde schijven

☐ Geen onbeveiligde back ups maken

☐ Geen documenten op privé laptop op slaan

Organisatorische beveiligingsmaatregelen

☐ Clean Desk Policy

☐ Laptop niet onbemand achterlaten

☐ Laptop nooit achterlaten in de auto

☐ Privacy screen medewerkers

☐ Oude documenten op de juiste manier vernietigen

☐ Zorgvuldig gebruik van USB-sticks

☐ Geheimhoudingsverklaring personeel

Het is van belang om vast te leggen welke technische en organisatorische maatregelen de verwerker heeft getroffen per categorie van verwerkingsactiviteiten. Onderstaand schema kunt u hiervoor gebruiken en desgewenst aanvullen.

Verwerkingsactiviteit: [invullen]

Manier van bewaren	Technische maatregelen	Organisatorische maatregelen	Toegang tot gegevens
Computer	Naam systeem en omschrijving wijze beveiliging, zoals virusscanner/wachtwoordbeveiliging	Toegang tot Computer	Naam en contactgegevens verantwoordelijke
ICT-systeem	Naam systeem en omschrijving wijze beveiliging	Toegang tot ICT-systeem	Naam en contactgegevens verantwoordelijke
Gegevensdragers	Naam systeem en omschrijving wijze beveiliging	Opslag en toegang gegevensdragers	Naam en contactgegevens verantwoordelijke

Fysieke opslag	N.v.t.	Eventuele omschrijving elektrische toegang/alarmsysteem	Naam en contactgegevens verantwoordelijke
Vul eventueel aan			

Verwerkingsactiviteit: [invullen]

Manier van bewaren	Technische maatregelen	Organisatorische maatregelen	Toegang tot gegevens
Computer	Naam systeem en omschrijving wijze beveiliging, zoals virusscanner/wachtwoordbeveiliging	Toegang tot Computer	Naam en contactgegevens verantwoordelijke
ICT-systeem	Naam systeem en omschrijving wijze beveiliging	Toegang tot ICT-systeem	Naam en contactgegevens verantwoordelijke
Gegevensdragers	Naam systeem en omschrijving wijze beveiliging	Opslag en toegang gegevensdragers	Naam en contactgegevens verantwoordelijke
Fysieke opslag	N.v.t.	Eventuele omschrijving elektrische toegang/alarmsysteem	Naam en contactgegevens verantwoordelijke
Vul eventueel aan			

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, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Het is wettelijk verplicht om een registratie bij te houden van alle datalekken binnen een organisatie. Daarin moet je in elk geval alle details van het datalek vermelden, alsmede welke systemen en hoeveel betrokkenen door het lek geraakt zijn, en de gevolgen die het datalek had of heeft voor de betrokkenen. Tot slot dien je de maatregelen die je hebt voorgesteld of genomen om het datalek aan te pakken te documenteren en de eventuele maatregelen om de nadelige gevolgen zo veel als mogelijk te beperken.

Op basis van deze informatie kan de Autoriteit Persoonsgegevens bepalen of je je hebt gehouden aan de wettelijke meldplicht voor datalekken.

De verwerker moet een (potentieel) datalek binnen 24 uur melden aan de verwerkingsverantwoordelijke, inclusief alle informatie, ontwikkelingen en genomen maatregelen.

De verwerkingsverantwoordelijke dient het datalek vervolgens te melden bij de Autoriteit Persoonsgegevens indien het een ernstig datalek betreft. Het Meldloket Datalekken van de Autoriteit Persoonsgegevens kan hier verder in adviseren.

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

- De website met logingegevens 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 (identiteits)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?

Is het antwoord op 1 van de vragen 'ja'? Dan is er sprake van een beveiligingsincident oftewel datalek.

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met Vredehof Uitvaartverzorging.

Waar meld je het beveiligingsincident?

Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met Vredehof Uitvaartverzorging

Naam	
Functie	
Emailadres	
Telefoonnummer	

met daarbij de volgende informatie:

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.

Vredehof Uitvaartverzorging kan je helpen met de beantwoording hiervan. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd?

Vermeld hier ook de naam van het betrokken systeem.

1. 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.

2. Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?
   Geef a.u.b. een minimum en maximum aantal personen.

3. 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.

4. 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?

5. Wat is de oorzaak (root cause) van het beveiligingsincident?
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?

6. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?
   Geef dit a.u.b. zo specifiek mogelijk aan.