BGNU

Mei 2018

Model AVG-Verklaring

Harma Bodde Uitvaartzorg

Breemarsweg 277
7553 HK Hengelo
06-46414516
info@harmaboddeuitvaartzorg.nl

Versie: Mei 2018

BGNU

Mei 2018

1 Voorwoord

De Europese Algemene Verordening Gegevensbescherming (hierna AVG) vervangt per 25 mei 2018 de Wet bescherming persoonsgegevens. Er komt één uniforme privacywetgeving voor de hele EU. De AVG schept nieuwe verplichtingen voor gegevensverwerkers. U bent bijvoorbeeld al een verwerker van persoonsgegevens op het moment dat u persoonsgegevens (denk aan een kopie van het identiteitsbewijs) van uw personeel opneemt in uw administratie of gegevens van klanten bewaart. De wet is ook van toepassing op zelfstandigen zonder personeel en het midden- en kleinbedrijf.

Aansprakelijkheid voor verwerker van persoonsgegevens
De uitvaartondernemer is als verwerker aansprakelijk voor eventuele schending van de wettelijke verplichtingen uit de AVG en u moet kunnen aantonen waarom u gegevens verwerkt, en op basis van welke grondslag. U kunt toestemming aantonen door middel van algemene voorwaarden of een overeenkomst, of verstrekte toestemming via de website.

Indien er iets mis gaat en persoonsgegevens op straat komen te liggen (het verliezen van een laptop met gegevens van klanten is al voldoende) dan wordt dit een datalek genoemd, en bent u verplicht om dit te melden bij de Autoriteit Persoonsgegevens. U dient betrokkenen te informeren en alles omtrent het datalek te documenteren.

Documentatieplicht
De AVG zorgt er onder andere voor dat privacyrechten worden versterkt en uitgebreid en dat organisaties meer verantwoordelijkheden krijgen. De belangrijkste verantwoordelijkheid is dat organisaties zelf moeten kunnen aantonen dat zij zich aan de AVG houden, de zogenaamde documentatieplicht. Dit betekent in de praktijk dat er documenten aanwezig moeten zijn die aantonen dat de juiste organisatorische en technische maatregelen zijn genomen om persoonsgegevens te beschermen. Met behulp van dit document kunt u aan deze documentatieplicht voldoen.

De inhoud van deze Model AVG-verklaring
Dit basismodel bevat de verwerking van afspraken zoals die moeten worden gemaakt in het kader van de bovengenoemde documentatieplicht. Het doel van deze afspraken is om ervoor te zorgen dat het voor u en eventuele werknemers binnen Uw bedrijf duidelijk is hoe er *intern* en *extern* moet worden omgegaan met de persoonsgegevens van bijvoorbeeld het personeel, ingeleende arbeidskrachten, onderaannemers en betrokken bewoners. Dit document is dus te gebruiken voor ondernemers met én zonder personeel. Wij adviseren u om deze Model AVG-verklaring ook aan uw medewerkers ter beschikking te stellen en de verwerkingen van persoonsgegevens met hen door te nemen.

AVG voor Uitvaartondernemers
U verwerkt als uitvaartonderneming diverse persoonsgegevens van diverse betrokkenen. Dit zijn werknemers, de verzekerde/overledene, nabestaanden, leveranciers, dragers, maar ook bezoekers van uw website. U deelt persoonsgegevens met leveranciers, partners en overige derde partijen waar u me samen werkt. Voor de verwerking van informatie die tot een persoon te herleiden is moet altijd een grondslag bestaan en voor het delen van gegevens moet toestemming worden gegeven. Deze grondslag kan zijn toestemming van de betrokkene, op grond van een overeenkomst, een wettelijke verplichting, en enkele overige gronden.

AVG en uw brancheverenigingBGNU
Uw brancheverenigingheeft de afgelopen periode veel aandacht aan dit onderwerp besteed en wij verwijzen dan ook naar onze website. Specifiek willen wij u wijzen op de gratis scan voor de controle van de geslotenheid van uw digitale netwerk.

2 Inleiding

De AVG heeft gevolgen voor álle bedrijven en organisaties die werken met persoonsgegevens. Het vragen, opslaan, gebruiken en andere handelingen met persoonsgegevens heet ‘verwerken’. Deze term ziet u daarom in dit document steeds terug.

Bij persoonsgegevens kan men denken aan namen, adresgegevens en telefoonnummers van bijvoorbeeld opdrachtgevers. Heeft u personeel in dienst of huurt u arbeidskrachten in? Dan vallen de persoonsgegevens van die personen hier ook onder. Het heeft impact voor álle bedrijven, groot, klein én zelfstandigen. Een groot bedrijf dat systematisch bijzondere persoonsgegevens verwerkt, systematisch en uitvoerig persoonlijke aspecten evalueert en/of op grote schaal systematisch mensen volgt in een publiek toegankelijk gebied (met bijvoorbeeld camera’s), kan meer verplichtingen hebben dan een bedrijf dat bijvoorbeeld alleen maar gewone persoonsgegevens verwerkt. Dit geldt ook voor bedrijven die bijzondere persoonsgegevens verwerken.

2.1 Wat zijn gewone en bijzondere persoonsgegevens?

Gewone persoonsgegevens
Gewone persoonsgegevens worden het meest verwerkt. Denk daarbij bijvoorbeeld aan registratie van naam, geslacht, adres, woonplaats, e-mailadres, telefoonnummers, postcode, geboortedatum, geboorteplaats, burgerlijke staat, bankrekeningnummer, BSN-nummer of bijvoorbeeld een social media account zoals Facebook of Twitter.

Bijzondere persoonsgegevens
Bijzondere persoonsgegevens zijn gevoeligere gegevens. Zoals bijvoorbeeld: informatie over ras, geaardheid, politieke opvatting, geloofsovertuiging of het strafrechtelijk verleden van een persoon. Bijzondere persoonsgegevens van de overledene kunnen in veel gevallen ook aan de nabestaanden worden gekoppeld.

Gezien u als uitvaartondernemer bij de uitvoering van uw dienstverlening namelijk ook gegevens verwerkt over levensovertuiging, afkomst en/of gezondheid van betrokkenen en deze informatie van een overledene gekoppeld kan worden aan de persoonsgegevens van nabestaanden, zijn dit bijzondere persoonsgegevens en gelden er voor u aanvullende eisen op basis van de AVG. Om deze reden zijn er enkele aanpassingen verricht in documenten.
Het is van belang dat u deze aanpassingen ook doorvoert en gebruikt om goed te zijn ingedekt voor de privacywetgeving conform de AVG.

Bijzondere persoonsgegevens waar Uitvaartondernemers veelal mee te maken zal hebben zijn:

- informatie over de godsdienst en/of levensovertuiging van betrokkenen welke voortvloeit uit de wensen voor de uitvaartverzorging, welke informatie aan nabestaanden kan worden gekoppeld
- informatie over de afkomst en etniciteit van betrokkenen welke voortvloeit uit de wensen voor de uitvaartverzorging, welke informatie aan nabestaanden kan worden gekoppeld
- informatie over gezondheid van de overledene welke aan nabestaanden kan worden gekoppeld en waarmee informatie over eventuele erfelijke aandoeningen bekend kan worden

2.2 Wanneer mag ik persoonsgegevens verwerken?

Grondslag
U mag alleen persoonsgegevens verwerken als daar in de AVG een grondslag voor bestaat. Een grondslag is een reden op basis waarvan u de gegevens verwerkt.

De meest eenvoudige vorm van grondslag is toestemming op grond van een overeenkomst. Toestemming kan onderdeel zijn van een overeenkomst, of een aparte overeenkomst zijn met betrekking tot het geven van toestemming voor het verwerken van persoonsgegevens. Daarna is de grondslag van wettelijke vereisten de meest voorkomende.

Vraag uzelf altijd af bij het verwerken van gegevens waarom u iets verwerkt, en waarom het eventueel moet of noodzakelijk is. Mag het wel wat u doet, en is er een reden te bedenken om de persoonsgegevens te bewaren, en voor hoe lang?

De AVG kent zes grondslagen waarop u persoonsgegevens mag verwerken. Dit mag als:

1. De betrokken persoon toestemming heeft gegeven. Bij toestemming is het belangrijk dat iemand weet waarom u persoonsgegevens van iemand vraagt en wat u daarmee gaat doen, daarover moet de betrokken persoon geïnformeerd worden. Stel: als u een contactformulier op uw website heeft staan waar persoonsgegevens achtergelaten kunnen worden, dan is het raadzaam om een privacybeleid op te stellen waar betrokken personen kunnen lezen wat er met hun persoonsgegevens zal gebeuren.
2. Gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst, zoals bijvoorbeeld een overeenkomst van opdracht die u heeft gesloten met uw opdrachtgever of een arbeidsovereenkomst die u met een werknemer bent aangegaan.
   NB: Leg in het geval van een mondelinge overeenkomst zo spoedig mogelijk schriftelijk afspraken vast, desnoods eerst met een bevestiging per e-mail alvorens de overeenkomst van opdracht wordt gesloten.
3. Dit noodzakelijk is voor het nakomen van een wettelijke verplichting. Een voorbeeld is de verplichting om het BSN van uw werknemer te verwerken en inkomensgegevens door te geven aan de Belastingdienst.
4. Dit noodzakelijk is ter bescherming van vitale belangen. Denk hierbij bijvoorbeeld aan de situatie waarin iemand bewusteloos is of niet in staat is om mentaal toestemming te geven voor een in te schakelen hulpdienst.
5. Gegevensverwerking noodzakelijk is voor het vervullen van een taak van algemeen belang of uitoefening van openbaar gezag. Dit ziet alleen toe op organisaties die een (wettelijke) taak van algemeen belang uitvoeren, bijvoorbeeld een organisatie voor ontwikkelingssamenwerking.
6. Gegevensverwerking noodzakelijk is voor de behartiging van gerechtvaardigde belangen. Deze grondslag kan van toepassing zijn als één van de bovenstaande grondslagen niet van toepassing is. Denk hierbij bijvoorbeeld aan ‘direct marketing’: het gebruiken van klantgegevens voor latere acquisitie. Gegevens mogen niet zomaar oneindig bewaard worden. Intern beleid zou kunnen zijn dat bijvoorbeeld NAW-gegevens een jaar worden bewaard voor een bepaald doel.

Toestemming bij webformulieren

Om er zeker van te zijn dat u kunt aantonen dat u toestemming voor de verwerking van persoonsgegevens heeft, dient u bijvoorbeeld op uw website overal waar persoonsgegevens kunnen worden ingevuld en waarbij er nog geen overeenkomst als grondslag bestaat maatregelen te nemen om rechtmatig persoonsgegevens te verwerken.

U dient bij bijvoorbeeld een contactformulier (of iedere wijze waarop de klant persoonsgegevens kan invullen, bijvoorbeeld bij een webshop omgeving of het opgeven voor de nieuwsbrief) op uw website te vragen of de bezoeker akkoord gaan met het privacybeleid, waarnaar met een hyperlink verwezen dient te worden, en bezoekers middels het zetten van een vinkje toestemming te laten geven voor het verwerken van hun persoonsgegevens. Zonder dit vinkje zou een webformulier niet doorgestuurd moeten kunnen worden.

Het privacybeleid moet daarnaast makkelijk te vinden zijn. Dit dient bijvoorbeeld in de footer op uw website te zien te zijn, naast de algemene voorwaarden. Let op dat dit vinkje niet standaard aan mag staan, dit moet zelf door de bezoeker kunnen worden geplaatst omdat de toestemming zelf gegeven moet worden door middel van het zogeheten 'opt-in'. U dient aan te kunnen tonen dat u toestemming hebt gevraagd en verkregen, en dient dit derhalve te registreren.

Het is verstandig om even om de tafel te gaan zitten met uw webbeheerder/website bouwer/ICT-afdeling om te bespreken hoe de beveiliging van de website van uw uitvaartonderneming kan worden aangescherpt. Een SSL-certificaat ter beveiliging is inmiddels noodzakelijk

Toestemming bij het verzenden van nieuwsbrieven

Kijkt u ook even naar het beleid en systeem voor uw nieuwsbrieven. Ook voor oude adresbestanden geldt de nieuwe wetgeving. Indien u niet kunt aantonen toestemming te hebben voor het verwerken van persoonsgegevens en dus voor het verzenden van een nieuwsbrief, overtreedt u de AVG. U moet kunnen aantonen hoe u de (e-mail)adressen hebt verkregen, en waarvoor die personen precies toestemming hebben gegeven.
Er wordt onderscheid gemaakt in persoonsgegevens die worden verkregen via dienstverlening en levering producten, of andere inschrijvingen via de website dan wel via een aanbieding. Een oplossing kan zijn om binnen uw nieuwsbriefsysteem verschillende groepen of lijsten hieromtrent aan te leggen. Ook is het verstandig om in verband met de toestemmingsvereiste uw adressenbestand voordat de AVG ingaat nog eenmaal aan te schrijven met een korte nieuwsbrief, waarin u hen verzoekt om via het klikken op een link toestemming te geven om in de toekomst nog nieuwsbrieven te ontvangen.

2.3 Privacybeleid

Er is in de bijlage een algemeen privacybeleid opgesteld voor uitvaartondernemers. Zet de verklaring op een makkelijk te vinden plaats op uw website. En belangrijker nog: zorg dat u bij het moment van verzamelen (bijv. bij het invullen een online formulier) een linkje opneemt naar het privacybeleid, alsook een vinkje laat plaatsen voor akkoord oftewel toestemming en dat deze toestemming wordt opgeslagen. U dient namelijk te kunnen aantonen dat u toestemming heeft voor de verwerking van persoonsgegevens.

Ook moet u het privacybeleid als bijlage verstrekken bij iedere overeenkomst die u sluit, net als uw algemene voorwaarden.

Het privacybeleid is opgesteld met het oog op de wettelijke verplichting om iedereen van wie u persoonsgegevens verwerkt duidelijk te informeren over welke privacygevoelige gegevens u verzamelt en met welk doel. U moet namelijk kunnen aantonen dat u de betrokkenen duidelijk en tijdig hebt geïnformeerd over wat u doet met hun persoonsgegevens. Het privacybeleid is algemeen opgesteld in lijn met de nieuwe wetgeving.

Gezien BGNU echter uit vele lidbedrijven bestaat, is het goed mogelijk dat het opgestelde model privacybeleid niet precies aansluit bij de daadwerkelijke manier van verwerken van persoonsgegevens binnen uw organisatie.

Het moge duidelijk zijn dat dit model op onderdelen aangepast moet worden aan de hand van uw bedrijfsspecifieke situatie.

U wordt in dat geval verwezen naar https://veiliginternetten.nl/privacyverklaring/
Via deze site kunt u op eenvoudige wijze een zeer volledige en AVG-proof privacyverklaring op maat opstellen aan de hand van uw werkwijze en situatie.

2.4 Aanvullende eisen bij verwerking bijzondere persoonsgegevens

Omdat Uitvaartondernemers ook bijzondere categorieën persoonsgegevens verwerkt, moet u op grond van artikel 9 van de AVG aan strengere eisen voldoen. U verwerkt ten behoeve van het uitvoeren van uw dienstverlening persoonsgegevens en vertrouwelijke informatie van diverse betrokkenen omtrent hun afkomst, godsdienst of levensovertuiging en/of gezondheid. Dit is informatie welke als extra gevoelig wordt beschouwd.

Gezien u deze informatie echter niet op grote schaal verwerkt en/of het geen kernactiviteit van uw onderneming is, bent u in beginsel niet verplicht om een Functionaris Gegevensbescherming aan te stellen of een uitgebreide inventarisatie van de privacyrisico's zoals een DPIA uit te voeren. Dit mag u echter wel doen, en in sommige gevallen bent u dit verplicht.

PIA of DPIA
Een DPIA of PIA is een (Data) Protection Impact Assessment en dit kan in een light of uitgebreide vorm, afhankelijk van uw organisatie. Een PIA is in beginsel pas verplicht bij het op grote schaal verwerken van bijzondere persoonsgegevens, en als de verwerking van bijzondere persoonsgegevens een kernactiviteit is van uw onderneming.
In dit stadium zal dit voor de meeste uitvaartondernemers dus nog niet verplicht of noodzakelijk zijn.

Indien u een nieuw project gaat starten met betrekking tot het bouwen van een nieuw systeem en/of het aanleggen van databestanden, dient u vooraf te inventariseren wat voor impact dit op de privacy zal hebben. In dat geval is het voorafgaand uitvoeren van een PIA met klem aan te raden.

U kunt voor een PIA een organisatie inhuren, echter kunt u dit ook zelf verzorgen in vereenvoudigde vorm. Het gaat er om dat u als organisaties de privacyrisco's goed in kaart brengt, op een gestructureerde en heldere manier.

De kern van de PIA is het in kaart brengen van de verwerking (wat ga ik doen en met welk doel) en de impact daarvan op de privacy (wat zijn de gevolgen voor de mensen wiens gegevens worden verwerkt) en vervolgens kijkt u wat u kunt doen of welke maatregelen u kunt treffen om de impact op de privacy van betrokkenen te verkleinen.

Ook moet de noodzaak en de proportionaliteit van de verwerkingen beoordeeld. Is het verwerken van de bijzondere persoonsgegevens noodzakelijk om het doel te bereiken, en is de inbreuk op de privacy van de betrokkenen niet onevenredig in verhouding tot dit doel?
Ook moeten de privacy risico's van de betrokkenen worden beoordeeld, met de beoogde maatregelen om deze risico's aan te pakken.

Door middel van dit document tonen Uitvaartondernemers aan dat zij aan de AVG voldoet. De Uitvaartondernemer dient dit document echter wel zo uitgebreid mogelijk uit te voeren en te implementeren in diens organisatie, en in te vullen waar nodig.
Dit document is echter niet zo uitgebreid als een PIA.
Via deze link kunt u een document downloaden waarin staat beschreven hoe u een volledige PIA kunt uitvoeren. Ook de uitkomsten van een PIA moeten worden gedocumenteerd in een rapport.

Functionaris Gegevensbescherming/Data Protection Officer (DPO)
Een Functionaris Gegevensbescherming oftewel FG, ook wel Data Protection Officer oftewel DPO genoemd, is verplicht indien uw organisatie op grote schaal bijzondere persoonsgegevens verwerkt, en dit een kernactiviteit van uw bedrijfsvoering is.

U bent als uitvaartondernemer in beginsel dus niet verplicht om een FG aan te stellen, tenzij uw onderneming van een dusdanig grote omvang is, dat de verwerking van bijzondere persoonsgegevens als grootschalig kan worden beschouwd.

U mag echter wel een FG aanstellen op vrijwillige basis. Indien er een FG is aangesteld, zal de Autoriteit Persoonsgegevens zich in het geval van een incident ook meer terughoudend opstellen.
Indien u een Functionaris Gegevensbescherming aanstelt, dient u dit aan te melden bij de Autoriteit Persoonsgegevens

Een FG heeft zich echter wel aan de regels en richtlijnen uit de wet te houden. De vertaling van de geldende regels uit de AVG voor de Functionaris Gegevensbescherming zijn te vinden via deze link.

Het is aan u zelf om de keuze te maken of u een FG wenst aan te wijzen. Het is fijn om een vaste contactpersoon binnen een organisatie te hebben welke zich bezighoudt met de privacy. U kunt dit echter ook in het takenpakket van een medewerker toevoegen, en dit een ander naam geven, zoals privacy manager of medewerker privacy of informatiebeveiliging. Voordeel is dat u deze persoon niet bij de Autoriteit Persoonsgegevens hoeft aan te melden, en de specifieke regels en richtlijnen voor FG's uit de wet niet gelden.

Hoe dan ook dient er iemand verantwoordelijk te zijn voor het letten op de privacy binnen uw uitvaartonderneming, mede omdat u tevens gevoelige informatie omtrent afkomst, etniciteit, godsdienst, levensovertuiging en/of gezondheid van betrokkene(n) verzamelt en verwerkt ten behoeve van het verzorgen van de uitvaart. Hoewel dit primair ziet op de overledene, wordt er ook informatie over de nabestaanden verstrekt waar deze bijzondere persoonsgegevens aan kunnen worden gekoppeld en welke ook door nabestaanden zelf worden verstrekt.
Het is belangrijk om binnen uw organisatie toezicht te hebben op de vertrouwelijkheid van deze gegevens en goed bij te houden hoe deze gegevens worden verwerkt en beveiligd.

3 Verwerking van persoonsgegevens

Iedere organisatie verwerkt klantgegevens. De AVG verplicht ons om alles in kaart te brengen en te registreren wat voor soort gegevens u verwerkt en waarom, en met wie deze gegevens worden gedeeld.

De AVG is niet van toepassing op de persoonsgegevens van overleden personen, omdat zij krachtens de wet niet meer als 'natuurlijk persoon' worden beschouwd. Echter kunnen de persoonsgegevens van de overledene ook worden herleid tot de nabestaanden, en zijn er ook persoonsgegevens over de nabestaanden bij u als uitvaartondernemer bekend. Daarop is de AVG van toepassing.

Ook verwerkt u persoonsgegevens van uw personeel en overige partijen waar u mee samenwerkt. Er is voor uw organisatie dus sprake van verwerking van diverse persoonsgegevens.

3.1 Welke persoonsgegevens verzamelen we?

Een uitvaartondernemer verzamelt diverse persoonsgegevens van alle betrokkenen bij een uitvaart, maar ook van personeel, leveranciers, leden van een verenging en bezoekers van de website. Gegevens worden gedeeld met bijvoorbeeld een administratiekantoor of webbeheerder, of met een begraafplaats of crematorium. Binnen de AVG moet nu worden nagedacht of het opvragen en/of delen van die gegevens wel echt noodzakelijk is voor het kunnen uitvoeren van de dienstverlening, en waarom u deze verzamelt.

Ga eens met een kritisch oog door uw opdrachtovereenkomst en/of overige vragenlijsten heen. Is het bijvoorbeeld noodzakelijk om bepaalde informatie op te vragen? Vraag alleen wat u nodig heeft. Bewaar gegevens niet langer dan noodzakelijk, en als u gegevens langer bewaart, doe dit met een goede reden.

De AVG en voorheen de Wbp verbieden niet dat u persoonsgegevens verstrekt aan belanghebbenden zoals partijen met wie u in het kader van uw dienstverlening dient samen te werken (begraafplaatsen, crematoria, mortuaria, drukkerij, grafmonument specialist, kerken, et cetera), echter dient u daar in beginsel wel toestemming voor te hebben. Op dit gebied is een aanpassing binnen de overeenkomst van opdracht gemaakt, welke u in de bijlage vindt.

Ook dient u te kunnen documenteren hoe u aan de persoonsgegevens komt, waarom u deze registreert en hoe lang u deze zult bewaren. U krijgt uw persoonsgegevens van de rechthebbenden zelf of van diens nabestaanden en gebruikt die gegevens voor de uitvoering van uw dienstverlening.
Het is belangrijk om bewust te zijn met welke persoonsgegevens er wordt gewerkt. Heeft u personeel in dienst, dan is het belangrijk dat de werknemers ook op de hoogte zijn van de regels omtrent het waarborgen van privacy, maar ook dat de privacy van de werknemers zelf wordt gewaarborgd.

Het is noodzakelijk om een beeld te krijgen van de verwerkingen en de soort persoonsgegevens die er bij uw bedrijf aanwezig zijn. Er dient bepaald te worden voor welk doel die persoonsgegevens gebruikt worden, hoe en hoe lang de gegevens bewaard worden en wie er verantwoordelijk voor is. Bedenk altijd dat u alleen maar persoonsgegevens mag verwerken als u daarvoor een doel heeft. Vraag dus nooit naar gegevens waar u vervolgens niks mee doet.

3.2 Basisregister Verwerkingsactiviteiten

De AVG introduceert een registratieplicht oftewel documentatieplicht voor alle verwerkingen van persoonsgegeven. De registratie van alle verwerkingen helpt u om gedocumenteerd aan te kunnen tonen dat de gegevensverwerking binnen uw bedrijf op orde is.
In Bijlage V bij deze Model AVG-Verklaring is in een Excel-document een uitgebreid basisregister van persoonsgegevens en verwerkingsactiviteiten opgesteld met betrekking tot de bedrijfsactiviteiten van een uitvaartondernemer. U dient dit schema door te nemen en aan te passen op de werkelijk bestaande situatie binnen uw organisatie.

Om u op weg te helpen zijn er al veel gegevens ingevuld. Aan dit schema kunnen echter geen rechten worden ontleend. Het basisregister is met de grootste zorg samengesteld en geeft een leidraad voor het opstellen van een volledig register van de verwerkingsactiviteiten van uitvaartondernemer. De uitvaartondernemer zal zelf beoordelen of de ingevulde informatie in het basisregister van toepassing is op haar organisatie en noodzakelijke aanpassingen verrichten.

Ter voorbereiding voor het register met verwerkingsactiviteiten kunt u starten door middel van het (laten) invullen van onderstaand schema binnen diverse afdelingen van uw organisatie teneinde de stromen van persoonsgegevens en alle relevante informatie te inventariseren. Dit schema is tevens een bijlage bij de Verwerkersovereenkomst.

Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen
Het onderstaande schema is behulpzaam bij iedere verwerking van diverse persoonsgegevens. Het geeft een 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. Wij adviseren u om dit schema binnen uw organisatie op verschillende gebieden in te vullen en op te nemen in deze AVG Verklaring.

Dit schema is eveneens een bijlage bij de Verwerkersovereenkomst.

Beschrijving verwerkingsactiviteiten door Verwerker:	Persoonlijke gegevens voor het aanvragen van begraven/cremeren, kerkdiensten, aangifte burgerlijke stand, contactgegevens opdrachtgever.
Verwerkingsdoelen:	
Verwerkingsverantwoordelijke:	Harma Bodde
Verwerker:	Harma Bodde
Sub verwerkers:	Koehorst advies Denekamp (boekhouding)
Verwerkte Persoonsgegevens:	
Locatie verwerkingen:	
Bewaartermijn:	10 jaar

3.3 Categorieën Persoonsgegevens

[De uitvaartondernemer) verklaart in de uitvoering van haar activiteiten te maken te hebben met de volgende categorieën betrokkenen, waarbij de verwerking van persoonsgegevens een rol *kan* spelen:

Vink aan welke categorieën op uw bedrijf van toepassing zijn

Sollicitanten	
Werknemers	
Verzekerden/Overledenen	x
Opdrachtgevers/Nabestaanden	x
Zzp'ers/opdrachtnemers	
Bezoekers website	x
Leveranciers/Partners	
Derden	

[Uitvaartondernemer] verklaart een uitgebreid register aan te leggen van al diens verwerkingsactiviteiten op basis van bovenstaande categorieën waarin zij verklaart welke persoonsgegevens worden verzameld voor welk doel en op basis van welke wettelijke grondslag. Alle mogelijke ontvangers worden gedocumenteerd en indien noodzakelijk wordt een verwerkingsovereenkomst met hen afgesloten.
De wijze van bewaren van de persoonsgegevens en de bewaartermijn worden vastgelegd, evenals de veiligheidsmaatregelen.

Verklaring technische en organisatorische 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 de tabel in het vorige hoofdstuk en/of in het Basisregister Verwerkingsactiviteiten heeft u onder andere per categorie betrokkenen verklaard welke persoonsgegevens u verwerkt, wie daarvoor verantwoordelijk is en hoe u deze gegevens bewaart.

Nu is het nog van belang om vast te leggen welke technische en organisatorische beveiligingsmaatregelen u heeft getroffen. Dit dient u eveneens in het Basisregister Verwerkingsactiviteiten vast te leggen.

U dient een overzicht te maken van de beveiligingsnormen die uw organisatie oplegt, zowel intern als extern. 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.

Voorbeelden technische beveiligingsmaatregelen
- Up to date virus scan
- 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

Voorbeelden 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 en bewaring van USB-sticks
- Geheimhoudingsverklaring

Tip: Leg afspraken hierover vast in uw huisreglement/arbeidsovereenkomst
Beschrijf aan de hand hiervan voor uw organisatie de organisatorische en technische maatregelen ten aanzien van het beveiligen van persoonsgegevens. Hiervoor kunt u het volgende schema invullen:

Omschrijf per categorie de getroffen technische en organisatorische beveiligingsmaatregelen:

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			

4 Geheimhoudingsverklaring

Naast het treffen van technische en organisatorische maatregelen is het raadzaam om de medewerker(s) die persoonsgegevens verwerken, een geheimhoudingsplicht op te leggen. Dit kan door hen een geheimhoudingsverklaring te laten tekenen of dit op te nemen in de individuele arbeidsovereenkomst of overeenkomst van opdracht. Het is verstandig om onderstaande voorbeeldtekst in uw arbeidsovereenkomsten op te nemen.

Ook voor ingeleende arbeidskrachten, zoals een uitzendkracht of een zelfstandige, is het raadzaam om een geheimhouding overeen te komen als zij gedurende hun werkzaamheden ook toegang krijgen tot persoonsgegevens.

Voorbeeldtekst Geheimhoudingsverklaring

Het is opdrachtnemer/werknemer verboden aan derden mededelingen te doen omtrent feiten en (persoons)gegevens van het bedrijf van [Uitvaartondernemer], waarvan opdrachtnemer/werknemer weet of behoort te weten dat deze vertrouwelijk van aard zijn en/of beschermd op basis van de Algemene Verordening Gegevensbescherming. Op overtreding van deze bepaling staat een direct door [Uitvaartondernemer] opeisbare boete ten bedrage van € 2.500,-- bij elke overtreding, onverminderd het recht om volledige schadevergoeding te vorderen.

5 Meldplicht Datalekken

Een datalek is een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of dat persoonsgegevens zijn gelekt of toegankelijk zijn geworden voor personen of bedrijven zonder dat dit de bedoeling is. Er is sprake van een datalek als de verplichte technische of organisatorische beveiligingsmaatregelen zoals die staan omschreven in het vorige hoofdstuk, niet hebben gewerkt. 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.

In iedere verwerkersovereenkomst van [Uitvaartondernemer] met derde partijen is een uitgebreide handleiding omtrent het melden van datalekken opgenomen, inclusief de relevante vragen hierbij. Dit staat in bijlage 3 van de verwerkersovereenkomst. De model-verwerkersovereenkomst is als Bijlage III aan deze Model AVG Verklaring gehecht.

5.1 Registratieplicht

U dient een registratie bij te houden van alle datalekken die u overkomen. Daarin moet u in ieder geval bijhouden: de details van het datalek, alsmede welke systemen en hoeveel betrokkenen door het lek geraakt zijn, de gevolgen die het had voor de betrokkenen en de maatregelen die u heeft voorgesteld of genomen om het datalek aan te pakken inclusief de eventuele maatregelen om de mogelijke nadelige gevolgen ervan te beperken. Deze registratie moet de Autoriteit Persoonsgegevens in staat stellen om na te gaan of u zich heeft gehouden aan de meldplicht datalekken.

Deze registratie wordt als volgt opgeslagen:

Comlap computers gevestigd in Albergen.

5.2 Melden aan de Autoriteit Persoonsgegevens

Een datalek dient u binnen 72 uur nadat het bij u bekend is geworden te melden bij de Autoriteit Persoonsgegevens. U dient een verantwoordelijke contactpersoon hieromtrent aan te wijzen binnen uw organisatie.

De verantwoordelijke persoon voor het melden van een datalek is:

Naam	Marco Nijboer van Comlap
Functie	eigenaar
Emailadres	info@comlap.nl
Telefoonnummer	06-10105476

Hieronder vindt u 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

Ieder datalek dient u te melden bij de Autoriteit Persoonsgegevens, tenzij het lek geen risico's inhoudt voor de veiligheid of rechten van de betrokkenen. Dit is een behoorlijk strenge eis, dus u moet een datalek al snel melden aan de Autoriteit Persoonsgegevens. Bij twijfel, altijd melden!

Wat te doen bij twijfel?
Als u op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stelt u zichzelf 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?

Bij twijfel, neem het zekere voor het onzekere en neem altijd contact op met de verantwoordelijke persoon in verband met de privacy en persoonsgegevens binnen het bedrijf van [Uitvaartondernemer]. Wij adviseren u bij twijfel altijd een melding te doen bij de Autoriteit Persoonsgegevens.

5.3 Externe verwerkers

Zoals aangegeven in het Basisregister Verwerkingsactiviteiten onder hoofdstuk 2.2 en Bijlage I van deze Model AVG-Verklaring worden bepaalde persoonsgegevens vanwege het doel gedeeld met een derde (externe) verwerker. Wij verklaren met iedere externe verwerker een verwerkersovereenkomst te sluiten zoals opgenomen in Bijlage III van deze Model AVG-verklaring.

In het model verwerkersovereenkomst wordt in ieder geval omschreven:

- De verplichting voor de externe verwerker om een potentieel datalek binnen 24 uur te melden aan de verantwoordelijke.
- De verplichting voor de externe verwerker om alle informatie en ontwikkelingen door te geven aan de verantwoordelijke.
- De verplichting voor de externe verwerker om de genomen maatregelen kenbaar te maken aan de verantwoordelijke.

6 Verklaring

[Uitvaartondernemer] verklaart de informatie in deze Model AVG-verklaring en bijbehorende bijlagen zorgvuldig doorlopen te hebben en naar waarheid te hebben ingevuld om zodoende te voldoen aan de verplichtingen die voortvloeien uit de AVG.

Dit model heeft een dynamisch karakter en zal derhalve herhaaldelijk beoordeeld worden en zo nodig up-to-date gehouden worden.

Datum: 24-05-2018
Plaats: Hengelo

Gegevens verantwoordelijke:

Bedrijfsnaam:	Harma Bodde Uitvaartzorg
Naam:	Harma Bodde
Functie:	Eigenaar
Adres:	Breemarsweg277
Telefoon:	074-2051007
Email:	info@harmaboddeuitvaartzorg.nl

Handtekening: ……..

7 BIJLAGEN:

7.1 Toestemmingsverklaringen persoonsgegevens /bijzondere persoonsgegevens (2 verklaringen)

Laat u deze verklaring ondertekenen door alle partijen waarmee u een bestaande overeenkomst heeft gesloten. Dus ook met uw werknemers/opdrachtnemers en overige partijen.

De verklaring inzake de verwerking van bijzondere persoonsgegevens is uitgebreider en wordt aangeraden om te laten ondertekenen door opdrachtgevers/nabestaanden waarmee u een lopende overeenkomst heeft, en zo lang u de wijzigingen in de overeenkomst van opdracht nog niet heeft doorgevoerd.

De toestemmingsverklaring persoonsgegevens kunt u ook door uw werknemers met lopende arbeidsovereenkomsten laten ondertekenen.

7.1.1 Toestemming verwerking persoonsgegevens AVG

1. Ondergetekende:
    a. Naam……
    b. Geboortedatum ……
    c. Adres ……
    d. Emailadres ……
    e. Telefoonnummer ……

2. Ondergetekende verklaart met ondertekening van deze verklaring ondubbelzinnig toestemming te verstrekken aan Harma Bodde Uitvaartzorg] en in te stemmen met het feit dat Harma Bodde Uitvaartzorg op grond van de Algemene Verordening Gegevensbescherming de persoonsgegevens van ondergetekende verwerkt met het doel om uitvoering te geven aan de dienstverlening/overeenkomst.
3. Harma Bodde Uitvaartzorg houdt zich vanzelfsprekend aan alle wettelijke vereisten vanuit de Algemene Verordening Gegevensbescherming en doet er alles aan om vertrouwelijke persoonsgegevens en eventueel door ondergetekende verstrekte bijzondere persoonsgegevens te beschermen en te beveiligen.
4. In het Privacy Beleid va Harma Bodde Uitvaartzorg en welke als bijlage aan onderhavige overeenkomst is gehecht, te vinden is op de website www.harmaboddeuitvaartzorg.nl en op eerste verzoek kosteloos wordt toegezonden, is meer informatie te vinden over de inhoud van het privacy beleid van Harma Bodde Uitvaartzorg en de wijze waarop Harma Bodde Uitvaartzorg met de verwerking van persoonsgegevens omgaat. Hiermee informeert Harma Bodde Uitvaartzorg ondergetekende nader omtrent de redenen en de omvang van de gegevensverwerking en de mogelijkheid om, indien gewenst, bezwaar te maken dan wel de toestemming in te trekken.
5. Ondergetekende heeft te allen tijde het recht om diens persoonsgegevens kosteloos in te zien, op te vragen, te wijzigen of te laten verwijderen.
6. Ondergetekende kan diens toestemming voor de verwerking van persoonsgegevens te allen tijde intrekken en kan zich hieromtrent wenden tot [Uitvaartondernemer] via info@harmaboddeuitvaartzorg.nl of telefonisch via 06-46414516. Op een dergelijk verzoek tot inzien, wijzigen of verwijderen van gegevens wordt uiterlijk binnen 4 weken gereageerd.

7. Plaats: ……
8. Datum: ……
9. Naam ondergetekende: ……
10. Handtekening: ……

7.1.2 Toestemming verwerking bijzondere persoonsgegevens AVG

1. Ondergetekende:
   Naam ……
   Geboortedatum……
   Adres ……
   Emailadres ……
   Telefoonnummer ……
2. Ondergetekende verklaart met ondertekening van deze verklaring ondubbelzinnig toestemming te verstrekken aan en Harma Bodde Uitvaartzorg in te stemmen met het feit dat [Uitvaartondernemer] op grond van de Algemene Verordening Gegevensbescherming de persoonsgegevens van ondergetekende verwerkt met het doel om uitvoering te geven aan de dienstverlening.
3. Ondergetekende is zich ervan bewust dat door het gebruik maken van de dienstverlening door Harma Bodde Uitvaartzorg door ondergetekende ook bijzondere persoonsgegevens omtrent gezondheid, afkomst en/of levensovertuiging aan Harma Bodde Uitvaartzorg kunnen worden verstrekt en dientengevolge worden verwerkt. Ondergetekende geeft door ondertekening van deze verklaring en door het gebruik maken van de dienstverlening van Harma Bodde Uitvaartzorg tevens uitdrukkelijke toestemming aan Harma Bodde Uitvaartzorg om ook bijzondere persoonsgegevens te verwerken met als doel de uitvoering van de dienstverlening door Harma Bodde Uitvaartzorg indien deze bijzondere persoonsgegevens ook daadwerkelijk door ondergetekende op eigen initiatief aan Harma Bodde Uitvaartzorg worden verstrekt Harma Bodde Uitvaartzorg. benadrukt dat het verstrekken van bijzondere persoonsgegevens nimmer verplicht is.
4. Harma Bodde Uitvaartzorg houdt zich vanzelfsprekend aan alle wettelijke vereisten vanuit de Algemene Verordening Gegevensbescherming en doet er alles aan om vertrouwelijke persoonsgegevens en bijzondere persoonsgegevens te beschermen en te beveiligen.
5. In het Privacy Beleid van Harma Bodde Uitvaartzorg welke als bijlage aan onderhavige overeenkomst is gehecht, te vinden is op de website www.harmaboddeuitvaartzorg.nl en op eerste verzoek kosteloos wordt toegezonden, is meer informatie te vinden over de inhoud van het privacy beleid van Harma Bodde Uitvaartzorg en de wijze waarop Harma Bodde Uitvaartzorg met de verwerking van persoonsgegevens en bijzondere persoonsgegevens omgaat. Hiermee informeert Harma Bodde Uitvaartzorg ondergetekende nader omtrent de redenen en de omvang van de gegevensverwerking en de mogelijkheid om, indien gewenst, bezwaar te maken dan wel de toestemming in te trekken.
6. Ondergetekende heeft te allen tijde het recht om diens persoonsgegevens kosteloos in te zien, op te vragen, te wijzigen of te laten verwijderen. Ondergetekende kan diens toestemming voor de verwerking van persoonsgegevens en bijzondere persoonsgegevens te allen tijde intrekken en kan zich hieromtrent wenden tot Harma Bodde Uitvaartzorg via info@harmaboddeuitvaartzorg.nl of telefonisch via 06-46414516. Op een dergelijk verzoek tot inzien, wijzigen of verwijderen van gegevens wordt uiterlijk binnen 4 weken gereageerd.

Plaats: ……
Datum: ……
Naam ondergetekende: ……
Handtekening: ……

7.1.3 Verwerkersovereenkomst

Met alle derde partijen waarmee de uitvaartondernemer gegevens deelt, dient een verwerkersovereenkomst te worden afgesloten. Dit is een verplichting vanuit de AVG.

Derde partijen zijn bijvoorbeeld:
Begraafplaatsen, crematoria, mortuaria, gemeenten, kerken of gebedshuizen, grafmonument specialisten, drukkerij, ICT-dienstverleners zoals een website bouwer, programmeur, website hosting,
Google Analytics, Mailchimp voor nieuwsbrieven, (loon)administratiekantoren, boekhouder/accountant, Belastingdienst, pensioenfonds, Arbodienst, reclame- of marketingbureaus en diverse verzekeraars.

De procedure voor het melden van datalekken bij deze overeenkomst dient te worden gevolgd bij incidenten (zie Wijzigingen in Algemene Voorwaarden en Overeenkomst van Opdracht).

De bijlagen bij de Verwerkersovereenkomst dienen zo volledig als mogelijk te worden ingevuld door partijen.

VERWERKERSOVEREENKOMST

PARTIJEN

1. Verantwoordelijke; [Uitvaartondernemer], statutair gevestigd te [PLAATS], aan het adres ADRES], vertegenwoordigd door [NAAM], [FUNCTIE].
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 [Uitvaartondernemer]
Naam:
Functie:
Datum en plaats:
Handtekening:

2. Bewerker
Ondertekend voor en namens [STATUTAIRE NAAM]
Naam:
Functie:
Datum en plaats:
Handtekening:

7.1.4 Bijlagen bij de verwerkingsovereenkomst

7.1.4.1 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:	

7.1.4.2 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			

7.1.4.3 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 de [De uitvaartondernemer].

Waar meld je het beveiligingsincident?
Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met [Uitvaartondernemer]:

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.

[Uitvaartondernemer] 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.

7.1.5 Wijzigingen in Algemene Voorwaarden en Overeenkomst van Opdracht

De Algemene Voorwaarden BGNU zijn alleen op artikel 14 aangepast in verband met de AVG. Uw branchebureau zal dit aangepaste document separaat naar u toesturen.

Toelichting: Aanpassing Algemene Voorwaarden:
In de Algemene Voorwaarden kan, in tegenstelling tot de regels bij de Wbp, geen toestemming meer worden verkregen voor de verwerking van persoonsgegevens. Deze toestemming moet duidelijk en ondubbelzinnig worden gegeven, bij voorkeur in de overeenkomst. Er is ook een aanvullend artikel m.b.t toestemming voor gebruik in de overeenkomst van opdracht opgesteld, en een apart toestemmingsformulier voor het aantonen van toestemming bij lopende overeenkomsten.

overeenkomst van opdracht
In de overeenkomst van opdracht dient eveneens een clausule te worden toegevoegd omtrent de vereiste toestemming voor de verwerking van persoonsgegevens. Uw Branchebureau zal deze overeenkomst ook hierop aanpassen.

De betreffende clausule is eveneens aangepast om te worden opgenomen in uw arbeidsovereenkomsten.

LET OP:
Voor bestaande overeenkomsten dient u een toestemmingsverklaring door de wederpartij te laten ondertekenen. Zie hiervoor Toestemmingsverklaringen persoonsgegevens /bijzondere persoonsgegevens (2 verklaringen)

Overeenkomst van Opdracht:
Uw digitale overeenkomst van opdracht dient zodanig te worden aangepast, dat hieruit blijkt dat de opdrachtgever toestemming heeft gegeven voor de verwerking van diens persoonsgegevens. Nabestaanden die nauw betrokken zijn bij de uitvaart naast de opdrachtgever kunnen desgewenst een toestemmingsformulier invullen, waarmee zij eveneens toestemming geven voor de verwerking van hun persoonsgegevens.
Deze toestemming is van cruciaal belang, omdat toestemming de meest belangrijke en makkelijke grondslag is om persoonsgegevens te mogen verwerken. U dient ook aan te kunnen tonen dat u deze toestemming heeft gekregen van de betrokkene.
Geef het privacybeleid ook mee als bijlage bij de overeenkomst van opdracht, net als uw algemene voorwaarden!

NB:
Uw branche bureau zal bij u navragen wie van u ons BGNU-document nog gebruikt.
In ieder geval zult u een check moeten doen of uw digitale formulier overeenkomst van opdracht voldoet aan de AVG-vereisten.

Toevoeging aan formulier overeenkomst van opdracht

Artikel … Persoonsgegevens en privacy:

1. [Uitvaartondernemer], haar personeel en de voor haar werkzame personen zullen de door opdrachtgever verstrekte (bijzondere) persoonsgegevens en informatie vertrouwelijk behandelen. [Uitvaartondernemer] conformeert zich daarbij aan de geldende privacywetgeving en de Algemene Verordening Gegevensbescherming en neemt de vereiste maatregelen om persoonsgegevens te beschermen en beveiligen.
2. Bij het sluiten van de overeenkomst geeft de Opdrachtgever middels ondertekening van deze overeenkomst toestemming aan [Uitvaartondernemer] om diens vertrouwelijke informatie en/of (bijzondere) persoonsgegevens te verwerken ten behoeve van het uitvoeren van de dienstverlening, klantbeheer en marketingdoeleinden. Opdrachtgever is vooraf geïnformeerd omtrent de verwerking van diens persoonsgegevens en verklaart de verwerking conform bovenstaande verwerkingsdoelen te aanvaarden.
3. Opdrachtgever is zich ervan bewust dat door het gebruik maken van de dienstverlening van [Uitvaartondernemer] volgens de wensen van Opdrachtgever ook bijzondere persoonsgegevens omtrent gezondheid, etniciteit en/of levensovertuiging aan [Uitvaartondernemer] kunnen worden verstrekt, en

dientengevolge worden verwerkt. Opdrachtgever geeft middels ondertekening van deze overeenkomst nadrukkelijk tevens toestemming om ook bijzondere persoonsgegevens te verwerken met als doel de uitvoering van de dienstverlening van [Uitvaartondernemer], indien deze bijzondere persoonsgegevens ook daadwerkelijk door Opdrachtgever worden verstrekt. [Uitvaartondernemer] benadrukt dat het verstrekken van bijzondere persoonsgegevens nimmer verplicht is.

4. [Uitvaartondernemer] zal de persoonsgegevens en vertrouwelijke informatie van Opdrachtgever niet doorgeven aan derden, tenzij dit noodzakelijk en overeengekomen is voor het uitvoeren van de dienstverlening conform de uitvaart zoals begraafplaats of crematorium, kerk, drukkerij, grafmonumentspecialist, of uitvaartverzekeraar.
5. [Uitvaartondernemer] heeft met alle partijen waarmee zij persoonsgegevens deelt afspraken gemaakt om de privacy te waarborgen. [Uitvaartondernemer] zal alleen de strikt noodzakelijke gegevens delen met deze derde partijen. Bijzondere persoonsgegevens zoals genoemd in lid 3 worden nimmer met derden gedeeld.
6. De contactgegevens van Opdrachtgever worden in verband met bovenstaande doeleinden voor een periode van 5 jaren bewaard. Overige informatie zal na het uitvoeren van de dienstverlening worden vernietigd, tenzij Opdrachtgever toestemming geeft om bepaalde gegevens te bewaren.
7. Opdrachtgever heeft te allen tijde het recht om diens persoonsgegevens kosteloos in te zien, op te vragen, te wijzigen of te laten verwijderen. Hiervoor kan er contact worden opgenomen met [Uitvaartondernemer] via [info@emailadres] of telefonisch via [TELEFOONNUMMER]. Op een dergelijk verzoek wordt uiterlijk binnen 4 weken gereageerd.
   In het Privacy Beleid van [Uitvaartondernemer] is meer informatie te vinden over de inhoud van het privacy beleid van [Uitvaartondernemer] en de wijze waarop [Uitvaartondernemer] met de verwerking van (bijzondere) persoonsgegevens en vertrouwelijke informatie omgaat. Hiermee informeert [Uitvaartondernemer] de Opdrachtgever nader omtrent de redenen en de omvang van de gegevensverwerking en de mogelijkheid om, indien gewenst, bezwaar te maken dan wel de toestemming in te trekken. Het privacybeleid wordt als bijlage bij deze overeenkomst meegegeven en is tevens te vinden op de website van [Uitvaartondernemer]. Indien gewenst wordt op eerste verzoek kosteloos een exemplaar toegezonden.

7.1.6 Wijzigingen in de Arbeidsovereenkomst

Op grond van de AVG heeft u een informatieplicht jegens werknemers zodra u persoonsgegevens van het personeel verwerkt. U moet hen bepaalde informatie verstrekken. Werknemers moeten op de hoogte zijn van welke organisaties in het kader van de arbeidsrelatie persoonsgegevens van hen verwerken, en het doel van de verwerking van deze gegevens. Ook moet de werknemer worden gewezen op diens rechten omtrent de verwerking van persoonsgegevens, en op de hoogte worden gesteld van de bewaartermijn.

De arbeidsovereenkomst kan met het volgende artikel worden aangevuld:

Artikel … Persoonsgegevens en privacy:

1. [Uitvaartondernemer] verwerkt persoonsgegevens van haar personeel ten behoeve van het geven van uitvoering aan de arbeidsovereenkomst en het voldoen aan wettelijke verplichtingen.
2. [Uitvaartondernemer], haar personeel en de voor haar werkzame personen zullen de door werknemer verstrekte (bijzondere) persoonsgegevens en informatie vertrouwelijk behandelen. [Uitvaartondernemer] conformeert zich daarbij aan de geldende privacywetgeving en de Algemene Verordening Gegevensbescherming en neemt de vereiste maatregelen om persoonsgegevens te beschermen en beveiligen.
3. Bij het sluiten van de overeenkomst geeft de werknemer middels ondertekening van deze overeenkomst toestemming aan [Uitvaartondernemer] om diens vertrouwelijke informatie en/of (bijzondere) persoonsgegevens te verwerken ten behoeve van het uitvoeren van de arbeidsovereenkomst. Werknemer is vooraf geïnformeerd omtrent de verwerking van diens persoonsgegevens en verklaart de verwerking conform bovenstaande verwerkingsdoelen te aanvaarden.
4. [Uitvaartondernemer] zal de persoonsgegevens en vertrouwelijke informatie van werknemer niet doorgeven aan derden, tenzij dit noodzakelijk en overeengekomen is voor het uitvoeren van de arbeidsovereenkomst zoals de loon- en/of salarisadministratie, pensioenfonds, belastingdienst, of arbodienst.
5. [Uitvaartondernemer] heeft met alle partijen waarmee zij persoonsgegevens deelt afspraken gemaakt om de privacy te waarborgen. [Uitvaartondernemer] zal alleen de strikt noodzakelijke gegevens delen met deze derde partijen.
6. Werknemer heeft te allen tijde het recht om diens persoonsgegevens kosteloos in te zien, op te vragen, te wijzigen of te laten verwijderen. Hiervoor kan er contact worden opgenomen met [Uitvaartondernemer] via [info@emailadres] of telefonisch via [TELEFOONNUMMER]. Op een dergelijk verzoek wordt uiterlijk binnen 4 weken gereageerd.
7. De persoonsgegevens van de werknemer worden indien daar een wettelijke verplichting toe bestaat 5 tot 7 jaar na het beëindigen van de arbeidsovereenkomst bewaard. Persoonsgegevens waar geen wettelijke bewaarplicht voor bestaat worden binnen 3 maanden na beëindiging van de arbeidsovereenkomst vernietigd.
8. In het Privacy Beleid van [Uitvaartondernemer] is meer informatie te vinden over de inhoud van het privacy beleid van [Uitvaartondernemer] en de wijze waarop [Uitvaartondernemer] met de verwerking van persoonsgegevens en vertrouwelijke informatie omgaat. Hiermee informeert [Uitvaartondernemer] de werknemer als betrokkene nader omtrent de redenen en de omvang van de gegevensverwerking en de mogelijkheid om, indien gewenst, bezwaar te maken dan wel de toestemming in te trekken. Het privacybeleid wordt als bijlage bij deze overeenkomst meegegeven en is tevens te vinden op de website van [Uitvaartondernemer]. Indien gewenst wordt op eerste verzoek kosteloos een exemplaar toegezonden.

7.1.7 Privacybeleid Algemeen

Dit is een privacybeleid dat in algemene zin is opgesteld. Het verdient aanbeveling om een privacybeleid op maat te maken voor de werkwijze van uw organisatie aan de hand van de door u bijgewerkte versie van het bijgevoegde excel bestand Basisregister Verwerkingsactiviteiten. Dit kunt u doen via: https://veiliginternetten.nl/privacyverklaring/

Privacybeleid
Het bewaken van uw privacy en het zorgdragen voor de naleving van de wettelijke bepalingen zoals opgenomen in de Algemene Verordening Gegevensbescherming (AVG) vinden wij erg belangrijk.

Hieronder valt het zorgvuldig omgaan met uw persoonsgegevens. Wij willen u op de hoogte stellen van ons privacybeleid en u wijzen op uw rechten.

Voorbeeld document

[Uitvaartondernemer], gevestigd te [PLAATS] is verantwoordelijk voor de verwerking van persoonsgegevens zoals weergegeven in deze privacyverklaring.

Contactgegevens
[ADRES]
[POSTCODE] [PLAATS]
[WEBSITE]
[TELEFOONNUMMER]
[EMAILADRES]
[KVK-NUMMER]

Persoonsgegevens die wij verwerken
[Uitvaartondernemer] verwerkt uw persoonsgegevens doordat u gebruik maakt van onze diensten en/of omdat u deze zelf aan ons verstrekt. Hieronder vindt u een overzicht van de persoonsgegevens die wij verwerken:

- Voor- en achternaam
- Geslacht
- Geboortedatum
- Adresgegevens
- Telefoonnummer
- E-mailadres
- IP-adres
- Overige persoonsgegevens die u actief verstrekt bij het sluiten van een overeenkomst
- Overige persoonsgegevens die u actief verstrekt bijvoorbeeld door een contactformulier op deze website aan te maken, in correspondentie en telefonisch
- Gegevens over uw activiteiten op onze website
- Gegevens over uw surfgedrag over verschillende websites heen (bijvoorbeeld omdat dit bedrijf onderdeel is van een advertentienetwerk)
- Internetbrowser en apparaat type

Bijzondere en/of gevoelige persoonsgegevens die wij verwerken
[Uitvaartondernemer] verwerkt de volgende bijzondere en/of gevoelige persoonsgegevens van u, indien u deze aan ons verstrekt ter uitvoering van de dienstverlening:

- godsdienst of levensovertuiging
- gezondheid
- afkomst of etniciteit

Met welk doel en op basis van welke grondslag wij persoonsgegevens verwerken
[Uitvaartondernemer] verwerkt uw persoonsgegevens voor de volgende doelen:

- Het uitvoeren van de dienstverlening
- Het verstrekken van een aanbod
- Het afhandelen van uw betaling
- Klantenbeheer
- Verzenden van onze nieuwsbrief en/of reclamefolder
- Reclame- en/of marketingdoeleinden
- U te kunnen bellen of e-mailen indien dit nodig is om onze dienstverlening uit te kunnen voeren
- U te informeren over wijzigingen van onze diensten en producten

U de mogelijkheid te bieden een account aan te maken

[Uitvaartondernemer] analyseert uw gedrag op de website om daarmee de website te verbeteren en het aanbod van producten en diensten af te stemmen op uw voorkeuren.
[Uitvaartondernemer] verwerkt ook persoonsgegevens als wij hier wettelijk toe verplicht zijn, zoals gegevens die wij nodig hebben voor onze belastingaangifte.

Geautomatiseerde besluitvorming
[Uitvaartondernemer]neemt niet op basis van geautomatiseerde verwerkingen besluiten over zaken die (aanzienlijke) gevolgen kunnen hebben voor personen. Het gaat hier om besluiten die worden genomen door computerprogramma's of -systemen, zonder dat daar een mens (bijvoorbeeld een medewerker van [Uitvaartondernemer]) tussen zit.

[Uitvaartondernemer] gebruikt de volgende computerprogramma's of -systemen:

[aanvullen met naam van het systeem, waarom het gebruikt wordt, onderliggende logica, belang en verwachte gevolgen voor betrokkene]

Hoe lang we persoonsgegevens bewaren
[Uitvaartondernemer] bewaart uw persoonsgegevens niet langer dan strikt nodig is om de doelen te realiseren waarvoor uw gegevens worden verzameld. Wij houden uw gegevens in bezit tot het moment waarop beide partijen aan alle verplichtingen hebben voldaan. Mocht het niet tot een overeenkomst leiden, dan houden wij uw gegevens in bezit tot de datum waartegen ons aanbod aan u is komen te vervallen.

Na het uitvoeren van de dienstverlening houden wij uw gegevens slechts met uw instemming in bezit als daarvoor een aan te wijzen doel is. Hier stemt u in elk geval mee in als wij een overeenkomst aangaan voor langer dan een jaar.

Ook houden wij uw gegevens in ons bezit als daar een wettelijke verplichting toe bestaat.
Indien u heeft aangegeven onze nieuwsbrief te willen ontvangen, dan zullen wij uw naam en emailadres met het doel van verzending van de nieuwsbrief bewaren.

Delen van persoonsgegevens met derden
[Uitvaartondernemer] verkoopt uw gegevens niet aan derden en verstrekt deze uitsluitend indien dit nodig is voor de uitvoering van onze overeenkomst met u of om te voldoen aan een wettelijke verplichting. Met bedrijven die uw gegevens verwerken in onze opdracht, sluiten wij een verwerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. [Uitvaartondernemer] blijft verantwoordelijk voor deze verwerkingen.

Cookies of vergelijkbare technieken die wij gebruiken
[Uitvaartondernemer] gebruikt alleen technische en functionele cookies. En analytische cookies die geen inbreuk maken op uw privacy. Een cookie is een klein tekstbestand dat bij het eerste bezoek aan deze website wordt opgeslagen op uw computer, tablet of smartphone. De cookies die wij gebruiken zijn noodzakelijk voor de technische werking van de website en uw gebruiksgemak. Ze zorgen ervoor dat de website naar behoren

werkt en onthouden bijvoorbeeld uw voorkeursinstellingen. Ook kunnen wij hiermee onze website optimaliseren.
Onze cookies kunnen niet worden gebruikt om personen te identificeren. U kunt zich afmelden voor cookies door uw internetbrowser zo in te stellen dat deze geen cookies meer opslaat. Daarnaast kunt u ook alle informatie die eerder is opgeslagen via de instellingen van uw browser verwijderen.
Door gebruik te maken van onze website gaat u akkoord met het gebruik van cookies.

Gegevens inzien, aanpassen of verwijderen
U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast heeft u het recht om uw eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van uw persoonsgegevens door [Uitvaartondernemer] en heeft u het recht op gegevensoverdraagbaarheid. Dat betekent dat u bij ons een verzoek kunt indienen om de persoonsgegevens die wij van u beschikken in een computerbestand naar u of een ander, door u genoemde organisatie, te sturen.

U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens sturen naar [EMAILADRES]. Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan, vragen wij u een kopie van uw identiteitsbewijs met het verzoek mee te sturen. Maak in deze kopie uw pasfoto, MRZ (machine readable zone, de strook met nummers onderaan het paspoort), paspoortnummer en Burgerservicenummer (BSN) zwart. Dit ter bescherming van uw privacy. We reageren zo snel mogelijk, maar binnen vier weken, op uw verzoek.

[Uitvaartondernemer] wil u er tevens op wijzen dat u de mogelijkheid heeft om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens. Dat kan via de volgende link: https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteit-persoonsgegevens/tip-ons

Hoe wij persoonsgegevens beveiligen
[Uitvaartondernemer] neemt de bescherming van uw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Wij dragen zorg voor een goede beveiliging van (de opslag van) uw persoonsgegevens.
Als u de indruk heeft dat uw gegevens niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact op met onze klantenservice.
[Uitvaartondernemer] behoudt zich het recht voor om de inhoud van dit privacybeleid te allen tijde te wijzigen.

7.1.8 Basisregister Verwerkingsactiviteiten – Excel

Dit register dient door u te worden ingevuld aan de hand van de verwerkingsactiviteiten, verwerkingsdoelen en beveiligingsmaatregelen die binnen uw organisatie daadwerkelijk plaatsvinden.

Dit register is in **basisvorm** samengesteld en dient derhalve door u te worden gecontroleerd en aangevuld zodat u hiervan een eigen op maat document ontwikkelt. Wij adviseren u om uw document jaarlijks bij te werken.

Disclaimer:
Het Basisregister Verwerkingsactiviteiten is door BGNU en MKB HuisJuristen met de grootste zorg samengesteld, maar aan de inhoud hiervan kunnen geen rechten worden ontleend. Het register biedt slechts een basis voor het registreren van alle activiteiten die met de verwerking van persoonsgegevens te maken hebben, en uw verplichtingen daarbij. U kunt zich desgewenst wenden tot MKB HuisJuristen voor inhoudelijke ondersteuning bij het invullen van het register en al uw overige vragen.