



AVG

&

DPIA

Inhoud

Stap 1	Gegevensverwerking	3
Stap 2	AVG grondslagen	3
Stap 3	Functionaris Gegevensbescherming	4
Stap 4	Data Protection Assessment	4
Stap 5	Privacy	4
Stap 6	Verwerkingsregister	5
Stap 7	Beveiliging	6
Stap 8	Verwerkersovereenkomst	6
Stap 9	Informatieplicht Privacy document	7
Stap 10	Privacy rechten	7
Bijlage 1	DPIA voor Stichting Verdriet door je hoofd	8

Termen

In onderstaande AVG worden bedoeld met	= 'Wij'	Stichting Verdriet door je hoofd
	= 'Organisatie'	Stichtingen, instellingen, instituten en andere verenigingsvormen van 'organisaties' die zich richten op contact met en binnen hun doelgroep(en).
	= 'Gebruikers'	Lotgenoten, doelgroep en gebruikers worden als termen gebruikt voor de groep mensen die gebruik maken van de app.



Stap 1 Gegevensverwerking

Wij mogen bijzondere persoonsgegevens verwerken omdat wij voldoen aan 2 uitzonderingen op het verwerkingsverbod van bijzondere persoonsgegevens (zoals iemand's gezondheid):

Uitzondering 1	<i>'Iemand heeft uitdrukkelijk toestemming gegeven voor de verwerking van zijn/haar persoonsgegevens. Dat is vereiste bij Stichting Verdriet door je hoofd bij het inschrijven voor de app. De toestemmingen worden los (papier) opgeslagen.'</i>
Uitzondering 2	<i>'U verwerkt de gegevens als stichting, vereniging of andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is. Het gaat om gegevens van uw (oud)leden of personen met wie u regelmatig contact heeft gerelateerd aan uw doelstelling. En u verwerkt de gegevens voor gerechtvaardigde activiteiten en met passende waarborgen.'</i>

De Stichting Verdriet door je hoofd heeft het recht om (gewone) persoonsgegevens te verwerken omdat wij ons kunnen baseren op een van de zes grondslagen uit de Algemene verordening gegevensbescherming (AVG). In dit geval is een van die grondslagen dat iemand toestemming heeft gegeven om zijn of haar persoonsgegevens te verwerken.

De kernmotivatie voor het opslaan en verwerken van bijzondere persoonsgegevens ligt in de aard van ons werk, de lotgenoten contactapp voor ouders, kinderen en instellingen. Stichting Verdriet door je hoofd moet in staat zijn om de gebruikers zo optimaal mogelijk te kunnen beschermen tegen malversaties. Daarvoor moet Stichting Verdriet door je hoofd zo goed mogelijk kunnen nagaan wie wie is en of deze claim ook correct is.

Stap 2 AVG grondslagen

Wij hebben recht om (gewone) persoonsgegevens te verwerken omdat wij ons kunnen baseren op een van de zes grondslagen uit de Algemene verordening gegevens-bescherming (AVG).

Grondslag	Iemand toestemming heeft gegeven om zijn of haar persoonsgegevens te verwerken.	
De toestemming wordt	Vrijelijk gegeven	Middels een aangeschafte folder of digitale link die leidt naar een schriftelijke inschrijving met verklaring, voorzien van een dag- en handtekening.
	Ondubbelzinnig	Schriftelijke verklaring voorzien van een dag- en handtekening.
	Geïnformeerd	Via mondelinge, schriftelijke en digitale informatiestromen vanuit de organisatie wordt men geïnformeerd wij over: = de identiteit van de organisatie = Het doel van elke verwerking = welke persoonsgegevens worden verzamelt en gebruikt; = Het recht dat iemand heeft om de toestemming weer in te trekken, op ieder gewenst moment. Alle gegevens worden dan verwijderd.
	Specifiek	De toestemming is voor één specifiek doel (het gebruik van de app).
Jongeren onder 16	Voor hun wordt een expliciete goedkeuring en gesignde verklaring van/door de ouders vereist.	



Stap 3

Functionaris Gegevensbescherming

Volgens regelgeving heeft de Stichting Verdriet door je hoofd geen FG nodig (Functionaris gegevensbescherming) maar we stellen die wel aan. In ons geval is dat bestuurslid Bernard Neuhaus.

Stap 4

Data Protection Impact Assessment

Volgens het besluit van de Autoriteit Persoonsgegevens inzake de DPIA, gepubliceerd in **Staatscourant 2019 nr. 64418 27 november 2019** hoeven wij geen DPIA effectbeoordeling uit te voeren.

DPIA van de applicatie	Zie bijlage 1.
Gegevensverwerking	Gegevens worden encrypted verwerkt. Zowel de persoonlijke gegevens als de communicatie gegevens die in de applicatie zullen plaatsvinden tussen de gebruikers onderling.
Gerechtvaardigd belang	De gebruikers krijgen middels de app de kans om elkaar te leren kennen. Zonder deze app is het heel moeilijk om een lotgenoot te kunnen vinden die bij je past.
Noodzaak	Zonder de gegevens op te slaan in het systeem kan men elkaar niet vinden.
Proportionaliteit	Er worden alleen namen en gegevens verwerkt die de lotgenoten zélf willen tonen en dan nog met de restrictie dat wij nooit telefoonnummers zullen vermelden. De inbreuk op de privacy en hert niveau ervan ligt geheel in handen van de gebruiker (en ouderlijk toezicht).
Privacy risico	Bij inbreuk van buitenaf (hacken) kunnen eigenlijk alleen namen en 'avatars' van gebruikers zichtbaar worden. Dit is niet te herleiden tot e-mailadressen en personen omdat de systemen en partijen (bijvoorbeeld Hosting) waar wij mee werken voldoende afgeschermd zijn.
Veiligheidsmaatregel	In geval van inbreuk op de applicatie zullen wij de applicatie met alle inhoud direct vernietigen. Daarna maken we op een nieuwe plek met nieuwe coderingen een nieuwe app voor de gebruikers. Dit is mogelijk omdat het bij deze applicatie per definitie om kleine groepen gebruikers gaat.

Stap 5

Privacy

Bij Stichting Verdriet door je hoofd zijn de instellingen van onze producten, diensten en interne systemen privacy vriendelijk ingesteld.

Stichting Verdriet door je hoofd geeft geen gegevens door aan andere partijen

Bij Stichting Verdriet door je hoofd kunnen de gebruikers alleen hun eigen gegevens inzien.

Wachtwoorden zijn encrypted

De app, database en servers zijn encrypted

Kinderprotocol
Het kan zijn dat kinderen onderling woorden krijgen. Wij kunnen echter niet de gegevens hierover uit het systeem halen. Ouders zullen daarom samen met hun kind moeten overleggen wat de gegevens zijn en daarna wordt direct door persoonlijk contact samen gekeken wat de beste vervolgstappen gezet moeten en kunnen worden.



De encrypted communicatiegegevens in de applicatie worden na drie maanden automatisch gewist. Deze gegevens kunnen na overleg ook direct handmatig worden gewist.

De persoonsgegevens worden in overleg gewist (zie Stap 9 en Stap 10).

Verder verwijzen we naar de Verklaring Privacy Voorwaarden voor de app, te vinden in de footer op de website van de stichting Verdriet door je hoofd: www.kankerspoken.nl.

Stap 6 Verwerkingsregister

Doel	Gebruikers hebben contact met elkaar, wisselen gegevens uit en steunen elkaar. De organisatie die de applicatie gebruikt kan hulpverlening, informatie, evenementen en afleiding aan de gebruikers bieden.
Gebruik	De gegevens worden verzameld voor gebruik in de contact app. Hiermee kunnen de gebruikers: <ul style="list-style-type: none">= Elkaars profielen bekijken waar men zichzelf voorstelt. De profielen worden door de gebruikers zelf ingevuld.= De gebruikers moeten met elkaar kunnen chatten binnen de app. Dat kan één op één en in groepsvorm.= De gebruikers moeten zich kunnen opgeven voor besloten evenementen (online en offline).
Verwerking	De gegevens worden verwerkt op twee plekken. <ul style="list-style-type: none">= Standalone papieren archief bestaat uit ingevulde formulieren met de ingevulde gegevens van de gebruikers, inclusief signering, goedkeuring en datering van de gebruikers. Op de ingevulde (papieren) formulieren staat vermeld:<ul style="list-style-type: none">= Voornaam= Vermelding gewenste voornaam in de app= Achternaam= Vermelding gewenste achternaam in de app= E-mailadres= Geboortedatum= Woonplaats= Telefoonnummer= De gegevens die worden overgenomen in de app in het CMS van administratiesite van de app (afgesloten):<ul style="list-style-type: none">= Gewenste voornaam of avatar= Gewenste achternaam of avatar= Woonplaats= Leeftijd= E-mailadres= De gebruikers ontvangen bij het inschrijven een eenmalige inlog-wachtwoord dat ze direct moeten wijzigen.= Zijn gebruikers hun wachtwoord vergeten dan worden ze uitgeschreven en krijgen ze een nieuwe inschrijving met nieuwe inlogcodering.= Beide registers zijn uitsluitend toegankelijk door de FG (functionaris Gegevensbescherming).= Beide registers kunnen ieder moment gewijzigd worden in overleg met de gebruikers= Wij delen verder geen gegevens met externe organisaties. Ook worden gegevens niet uitgewisseld of gedeeld met gebruikers. De gebruikers zijn



zelf verantwoordelijk om voor verdere contacten met andere gebruikers eigen onderling verdere afspraken te maken.

= De gegevens uit beide archieven worden direct gewist als de gebruiker of de verantwoordelijke ouder/voogd dat aangeeft (mondeling of schriftelijk), en bij overlijden van de gebruiker.

Stap 7

Beveiliging

Beleid

Persoonsgegevens en informatiebeveiliging zijn slechts toegankelijk voor de FG (Functionaris Gegevensbescherming).

Iedereen krijgt een training 'omgaan met beveiliging' en een heldere instructie van de FG.

Beveiligingstesten vinden plaats via onze ondersteunende organisaties voor onderhoud en ondersteuning.

Datalekprotocol = Iedereen (medewerkers en gebruikers) die een data lek herkent dient dit terstond te melden aan de organisatie. Die neemt vervolgens direct contact op met de Autoriteit Persoonsgegevens voor het nemen van de juiste stappen.

= Bij een groot data lek wordt de hele applicatie direct gesloten en opgeheven. Alle gebruikers worden daarna direct op de hoogte gebracht en bij goedkeuring opnieuw ingeschreven in een nieuwe applicatie. Zij moeten dan de hele aanmeldingsprocedure geheel opnieuw doorlopen. (Wij kunnen deze rigoureuze stap zetten omdat de apps per definitie alleen door kleine groepen gebruikers zullen worden gebruikt).

Kwetsbaarheden in het systeem zullen direct en bovenaan op de prioriteitenlijst (backlog) van de uit te voeren onderhoudspunten geplaatst worden.

In de contracten van medewerkers staan hun bevoegdheden en hun geheimhoudings-overeenkomsten.

Wij werken op voorhand in de applicaties met een minimum aan persoonsgegevens.

Stap 8

Verwerkersovereenkomst

Er zijn geen partijen die persoonsgegevens voor ons verwerken. Wij hebben wel met hosting- en serverpartijen te maken maar die worden geacht hun systemen waar wij gebruik van maken zelf adequaat beveiligd hebben.

Medewerkers binnen de stichting Verdriet door je hoofd, die uit hoofde van hun functie persoonsgegevens moeten verwerken of inzien, hebben een bevoegdheid hiertoe die beperkt is tot hetgeen tot hun taak behoort. Deze medewerkers hebben een verwerkersovereenkomst ondertekend, waarin de beperkte bevoegdheid en de verplichtingen in het kader van privacy beschreven staan.



Stap 9

Informatieplicht Privacy document

VV	Stichting Verdriet door je hoofd is verwerkingsverantwoordelijk (VV): www.kankerspoken.nl
FG	Bernard Neuhaus, bestuurslid redactie@kankerspoken.nl
Doel gegevensverwerking	Onderling contact tussen gebruikers en het contact tussen de organisatie en de gebruikers.
Reden datadeling	Gebruikers is uitgelegd waarom de gegevens gebruikt worden (doel). Men is gerechtigd om hier niet aan mee te doen en wordt dan dus ook geen 'gebruiker'.
Ontvangers	Doelgroepen van de Stichting Verdriet door je hoofd: de gebruikers van de app.
Recht	De gebruikers mogen ten alle tijden: Gegevens = inzien = opvragen = wijzigen = verwijderen = Intrekken van toestemming = Indienen van een klacht bij de Autoriteit Persoonsgegevens
Doorgifte	Er vindt geen doorgifte van gegevens naar andere partijen plaats.
Automatisering	Er wordt geen gebruik gemaakt van geautomatiseerde besluitvorming en profilering.
Toestemming	De gebruikers wordt vooraf aan de inschrijving specifiek (in schrift en mondeling) gevraagd om toestemming voor het gebruik van gegevens. De AVG is altijd in te zien via de Documenten pagina op de site www.kankerspoken.nl . Minderjarigen mogen alleen dan meedoen als goedkeuring van ouders gegeven is, schriftelijk en mondeling.

Stap 10

Privacy rechten

De gebruikers mogen hun eigen persoonsgegevens:	= inzien = opvragen = Wijzigen, aan te vullen = Verwijderen (en vergeten worden)
De gebruikers mogen	= Beperken van de toestemming = Intrekken van toestemming = Bezwaar maken = Indienen van een klacht bij de Autoriteit Persoonsgegevens

Aangezien ons doel en 'het product' geheel ten dienste staat van de gebruikers is het 'Recht op een menselijke blik bij besluiten' natuurlijk vanzelfsprekend.



1. Doel en reikwijdte

Het doel van deze DPIA is om de privacyrisico's te beoordelen van de verwerking van persoonsgegevens door Stichting Verdriet door je hoofd. De verwerking betreft het opslaan van gegevens van lotgenoten en kinderen, waaronder namen, contactgegevens en medische informatie die gelieerd is aan de groep lotgenoten.

2. Beschrijving van de verwerking

Stichting Verdriet door je hoofd verzamelt gegevens van kinderen en lotgenoten om hen te ondersteunen en te helpen bij het omgaan met hun situatie. De gegevens worden opgeslagen in een database die wordt beheerd door Stichting Verdriet door je hoofd. De gegevens worden gebruikt om de kinderen en lotgenoten te kunnen informeren over activiteiten en bijeenkomsten, om deelname aan deze activiteiten te faciliteren en om ondersteuning te bieden in geval van nood.

3. Risicobeoordeling

De verwerking van persoonsgegevens door Stichting Verdriet door je hoofd brengt privacyrisico's met zich mee voor de betrokkenen. Hieronder staan de belangrijkste risico's en de maatregelen die Stichting Verdriet door je hoofd heeft genomen om deze risico's te beperken:

3.1 Risico: Ongeoorloofde toegang tot persoonsgegevens

Er bestaat een risico dat onbevoegden toegang krijgen tot persoonsgegevens van kinderen en lotgenoten. Dit kan leiden tot ongewenste publicatie van persoonsgegevens, identiteitsdiefstal of andere vormen van misbruik.

Maatregelen:

Stichting Verdriet door je hoofd heeft beveiligingsmaatregelen genomen om ongeoorloofde toegang tot persoonsgegevens te voorkomen. Dit omvat onder andere het gebruik van sterke wachtwoorden, het beperken van toegang tot de database tot geautoriseerd personeel en het regelmatig monitoren van de toegangslogboeken.

3.2 Risico: Onjuiste of onvolledige persoonsgegevens

Er bestaat een risico dat de persoonsgegevens die door Stichting Verdriet door je hoofd worden verwerkt onjuist of onvolledig zijn. Dit kan leiden tot foutieve communicatie of ondersteuning en kan de privacy van betrokkenen schaden.

Maatregelen:

Stichting Verdriet door je hoofd heeft procedures opgesteld om ervoor te zorgen dat persoonsgegevens juist en volledig zijn. Dit omvat onder andere het verifiëren van de gegevens bij de betrokkenen zelf en het regelmatig controleren en bijwerken van de gegevens in de database.



3.3 Risico: Gebruik van gevoelige persoonsgegevens

Stichting Verdriet door je hoofd verwerkt gevoelige persoonsgegevens, waaronder medische informatie. Dit brengt een risico met zich mee voor de privacy van betrokkenen, aangezien deze informatie gevoelig van aard is en kan worden gebruikt voor ongepaste doeleinden.

Maatregelen:

Stichting Verdriet door je hoofd heeft procedures opgesteld om ervoor te zorgen dat gevoelige persoonsgegevens alleen worden verwerkt voor de specifieke doeleinden waarvoor ze zijn verzameld. Dit omvat onder andere het beperken van de toegang tot deze gegevens tot geautoriseerd personeel en het zorgen voor de vertrouwelijkheid van deze informatie.

Stichting Verdriet door je hoofd zorgt ervoor dat de betrokkenen expliciet toestemming geven voor het verzamelen en verwerken van hun medische gegevens. Dit gebeurt via een toestemmingsformulier dat wordt verstrekt aan de betrokkenen.

Stichting Verdriet door je hoofd bewaart medisch gelieerde informatie alleen zo lang als nodig is voor het specifieke doel waarvoor deze informatie is verzameld. De informatie van de doelgroep blijft bestaan zolang het account in gebruik is.

4. Resultaten en conclusies

Op basis van de risicobeoordeling heeft Stichting Verdriet door je hoofd adequate maatregelen genomen om de privacy van betrokkenen te beschermen. Stichting Verdriet door je hoofd heeft procedures opgesteld om ervoor te zorgen dat persoonsgegevens juist en volledig zijn, dat gevoelige persoonsgegevens alleen worden verwerkt voor specifieke doeleinden en dat toegang tot persoonsgegevens beperkt is tot geautoriseerd personeel. Bovendien zorgt Stichting Verdriet door je hoofd ervoor dat betrokkenen expliciet toestemming geven voor het verzamelen en verwerken van hun medische gegevens en deze gegevens te allen tijde door de gebruikers zijn te verwijderen.

Op basis van deze conclusie is het aanbevolen om de DPIA periodiek te herzien en bij te werken, bijvoorbeeld bij veranderingen in de verwerking van persoonsgegevens, of wanneer nieuwe privacyrisico's zich voordoen.

