Data Protection Impact Assessment (DPIA) Gegevensbeschermingseffectbeoordeling

Dit formulier is ontwikkeld op basis van de volgende bronnen:

- De AVG zelf
- De Handleiding Algemene Verordening Gegevensbescherming, uitgave van de Autoriteit Persoonsgegevens. Auteurs: Bart W. Schermer, Dominique Hagenauw, Nathalie Falot
- Richtsnoeren voor gegevensbeschermingseffectbeoordelingen door groep Gegevensbescherming, Zoals laatstelijk gewijzigd en vastgesteld op 4 oktober 2017
- Privacy Impact Assessment (PIA): Introductie, handreiking en vragenlijst Versie 1.2 - November 2015 uitgegeven door NOREA

Organisatiegegevens

Naam, adres van organisatie: Guido Terhorst, Terhorst Consultancy B.V. – Burgemeester Hogguerstraat 861

Opsteller DPIA:Guido Terhorst

Naam en contactgegevens FG (als deze is aangesteld):
Er is op het moment nog geen FG aangesteld, deze taak wordt voorlopig aangehouden door Guido Terhorst.

Overige betrokkenen en geraadpleegde experts:
Er zijn bij het invullen van de Data Protection Impact Assessment geen overige betrokkenen of experts geraadpleegd.

Stappenplan uitvoering:
De Data Protection Impact Assessment is uitgevoerd en ingevuld op 14 april 2020

Gegevens van de verwerking

Beschrijf hier om welke persoonsgegevens het gaat (naam, email, medisch, ...).

Het gaat om de verwerking van klanten op het gebied van naam, lichaamstemperatuur, telefoonnummer, geslacht, geboortedatum en e-mailadres.

Daarnaast worden de NAW gegevens en beroepsgegevens van dokters opgeslagen.

Met welk doel en in welk proces worden deze gegevens gebruikt?

De gegevens worden verwerkt in het kader van onderzoeksdoeleinden van het RIVM en opsporing van infectieziektegevallen. Ook worden de gegevens gebruikt in het bepalen van een afspraak op het gebied van huisartsenzorg.

Welke groepen betrokkenen zijn de persoonsgegevens van (websitebezoekers, leerlingen, klanten, ...)

De groepen die betrokken zijn gekoppeld aan de websitebezoekers en gebruikers op het gebied van patiënten en doktoren van de app.

Is deze DPIA voor een bestaande situatie, of voor een nieuw voorgestelde situatie?

Deze DPIA is voor een nieuw voorgestelde situatie.

Moet een DPIA worden uitgevoerd

Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt). Dat is in ieder geval zo als een organisatie:

1. systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profilering;
2. op grote schaal bijzondere persoonsgegevens verwerkt;
3. op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Om te bepalen of er mogelijk sprake is van een hoog risico hanteren de toezichthouders de onderstaande vuistregel. Er is sprake van een hoog risico men aan twee of meer van de onderstaande negen criteria voldoet:

1. evaluatie van personen of scoretoekenning;
2. geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg;
3. stelselmatige monitoring;
4. gevoelige gegevens of gegevens van zeer persoonlijke aard;
5. op grote schaal verwerkte gegevens;
6. matching of samenvoeging van datasets;
7. gegevens met betrekking tot kwetsbare betrokkenen;
8. innovatieve toepassing van nieuwe technologische of organisatorische oplossing;
9. blokkering van een recht, dienst of contract.

Aan welke criteria voldoet deze verwerking? Geef voor elk criteria een korte motivatie

1. De evaluatie van personen vindt plaats door de koppeling van persoonsgegevens en patiëntgegevens waarop een besluit genomen wordt om een vervolgtraject in te zetten van het testen van een patiënt of een doktersafspraak maken.
2. Er vindt een geautomatiseerde besluitvorming plaats wanneer een patiënt bepaalde hoge waarden consistent doorgeeft.
3. Er vindt een stelselmatige monitoring plaats doordat er frequent vragen worden gesteld wanneer een patiënt heeft aangegeven dat hij waarschijnlijk ziek is
4. Gevoelige gegevens op het gebied van NAW, doktersgegevens en additionele patiëntgegevens worden hierin meegenomen
5. De gegevens worden op grote schaal verwerkt
6. Datasets wordt niet met elkaar samengevoegd
7. De gegevens met betrekking tot kwetsbare betrokken en worden doorgestuurd
8. Hier is sprake van een toepassing van een innovatieve nieuwe technologie die het mogelijk maakt om patiënten in kaart te krijgen en hierop te acteren.
9. Er is geen sprake van een blokkering van een recht, dienst of contract

Systematische omschrijving van de gegevensverwerking

Beschrijf hier in meer detail hoe de gegevensverwerking gaat.

De gegevensverwerking vindt plaats op het gebied van een formulier op de website die de naam, telefoonnummer, e-mailadres en locatie van patiënten verzameld.

Daarnaast worden op de app de informatie verwerkt van patiënten en doktoren die via een beveiligde verbinding worden verwrkt.

Hoe / waar wordt de informatie verzameld?

De gegevens worden verzameld via een inschrijfformulier op de website en een formulier op de app van Touristdoc.

Waar wordt deze opgeslagen? Wie kan hier bij?

De gegevens worden opgeslagen bij een Nederland webhosting provider op een beveiligde server. De naam van de webhosting provider is Vservs die servers vervolgens huurt van Transip dat een Nederlandse ISP is.

Hoe wordt de informatie gebruikt? Wordt elk veld gebruikt?

De informatie wordt gebruikt om contact op te nemen met de patient en een beoordeling te maken of vervolgstappen noodzakelijk zijn.

Wat zijn de doelen van de verwerking? Kunnen deze doelen ook zonder de gegevens worden behaald?

De doelen van de verwerking is dat een vervolgstap succesvol doorgezet kan worden en op basis van de informatie een succesvolle assesment gemaakt kan worden.

Wordt binnen het proces om toestemming gevraagd? Zijn er latere uitschrijf/opt-out-mogelijkheden?

Binnen het proces wordt vantevoren toestemming gevraagd voor het gebruik van bepaalde hardwarefunctionaliteiten als bluetooth en bij het invullen van het formulier wordt de patiënt of dokter geattendeerd op het privacybeleid van Touristdoc.

Wat is de bewaartermijn van de gegevens? Hoe is de verwijdering van de gegevens geregeld?

De gegevens worden bewaard op basis van de wettelijke bewaartermijn van 15 jaar m.b.t. de wet de geneeskundige behandelingsovereenkomst.

Welke hardware en software wordt gebruikt bij de gegevensverwerking?

Bij de gegevensverwerking wordt gebruikgemaakt van hardware op het gebied van bluetooth en via de app en website wordt additionele informatie verzameld die al dan niet in relatie staan tot het gebruik van de hardware.

Welke afdelingen, leveranciers en andere partijen zijn als verwerker bij de verwerking betrokken?

Als verwerker bij de verwerking zijn betrokken Vservs als ISP en Microsoft als clouddienst waar de e-mails worden opgeslagen en de patiëntgegevens die verstrekt worden aan de GGD.

Is er sprake van internationale doorgifte? Welke landen betreft dit?

Er is geen sprake van automatische internationale doorgifte, het is mogelijk dat de patiënt zijn gegevens op papier mee kan nemen naar het buitenland.

Waar wordt de data gearchiveerd? Is dit papier of digitaal?

De data wordt digitaal gearchiveerd op de server(s) van de organisatie.

Wat is de verwachte omvang van de gegevensverwerking (aantallen betrokkenen)

Er is nog geen zicht op de verwachte omvang van de gegevensverwerking.

Beoordeling noodzaak en proportionaliteit

Is er sprake van een duidelijk gespecificeerd doel? Wat is dit doel precies, en waarom is dit legitiem?

Het duidelijk gespecificeerd doel is de opsporing van infectieziekten en de behandeling van toeristen door lokale huisartsen.

Kan dit doel ook zonder deze persoonsgegevens worden behaald? Waarom niet, of waarom doet u het niet anders?

Dit doel kan niet zonder persoonsgegevens worden behaald die wij vanuit de app of de website halen omdat er contact opgenomen moet worden van patiënten die wij nog niet kennen en niet vooraf ergens op kunnen slaan.

Is er sprake van een duidelijke maximale bewaartermijn?

De wettelijke bewaartermijn op het gebied van de medische wet worden aangehouden.

Wordt er voldoende informatie verstrekt aan betrokkene? Is het voor betrokkenen duidelijk welke rechten zij hebben en hoe zij deze kunnen uitoefenen?

De informatie die aan de betrokkenen wordt verstrekt is ons privacy beleid wat naar voren komt in elke aanvraag die wordt verstuurd.

Hoe is het recht op inzage gewaarborgd?

Het recht op inzage is gewaarborgd door te e-mailen naar onze privacy officer op info@touristdoc.com.

Hoe is het recht op rectificatie gewaarborgd?

Het recht op rectificatie is gewaarborgd door te e-mailen naar onze privacy officer op info@touristdoc.com.

Hoe is het recht op verwijdering gewaarborgd?

Het recht op verwijdering is gewaarborgd doortet e-mailen naar onze privacy officer op inf@touristdoc.com.

Hoe is het recht op overdraagbaarheid van gegevens gewaarborgd?

Het recht op overdraagbaarheid van gegevens is gewaarborgd door te e-mailen naar onze privacy officer op info@touristdoc.com.

Beoordeling van de privacyrisico's

Inschatting risico's

Hoe schat u de kans en impact van de volgende risico's:

Risico	Hoe kan dit risico zich voordoen?	Kans dat dit in een jaar gebeurt	Impact op betrokkenen
Onrechtmatige toegang – interne medewerkers	Dit kan wanneer de interne medewerkers toegang krijgen tot de e-mailadressen van doktoren, geregistreerde gebruikers van de app en/of van collega's binnen de organisatie waar de aangemaakte inlogcodes van accounts op binnenkomt.	Laag want deze codes worden elke keer opnieuw gegenereerd waardoor de medewerker stelselmatige toegang moet krijgen van de e-mailadressen van de beheerders.	Laag want de informatie wordt versleuteld opgeslagen en ook gegevens worden versnipperd opgeslagen waardoor er geen coherent informatie uit te vallen haalt.
Onrechtmatige toegang – door buitenstaanders	Als er wordt ingebroken op de clouddienst en ISP van Touristdoc.	Laag want door een twee staps verificatie is de kans op inbraak kleiner.	Laag want de informatie wordt versleuteld opgeslagen en ook gegevens worden versnipperd opgeslagen waardoor er geen coherent informatie uit te vallen haalt en aan te passen.
Ongewenste wijziging van gegevens – interne medewerkers	Als een medewerker de informatie van gebruikers wijzigt in het admin paneel van de website en app.	Laag want door een twee staps verificatie is de kans op inbraak kleiner.	Laag want de informatie wordt versleuteld opgeslagen en ook gegevens worden versnipperd opgeslagen waardoor er geen coherent informatie uit te vallen haalt en aan te passen.

Ongewenste wijziging van gegevens – door buitenstaanders	Als er wordt ingebroken in het admin paneel van de website en app.	Laag want door een twee staps verificatie is de kans op inbraak kleiner.	Laag want de informatie wordt versleuteld opgeslagen en ook gegevens worden versnipperd opgeslagen waardoor er geen coherent informatie uit te vallen haalt en aan te passen.
Verdwijnen / zoekraken van gegevens	Wanneer de website of app crasht	Laag want er is sprake van een dagelijkse backup	Laag want de informatie wordt versleuteld opgeslagen en ook gegevens worden versnipperd opgeslagen waardoor er geen coherent informatie uit te vallen haalt en aan te passen.

Wat is de exacte impact van uitlekken van gegevens op betrokkenen?

- Heeft dit nadelige gevolgen voor de persoon?
- Is er kans op financiële schade?
- Is er kans op identiteitsdiefstal of fraude?

Maatregelen

Kunt u per risico aangeven welke maatregelen u neemt om de gegevens te beschermen:

Onrechtmatige toegang – interne medewerkers	Wij hebben twee staps verificatie en een dagelijkse backup waardoor informatie teruggehaald kan worden en de essentiële onderdelen altijd na een reset van de server weer terecht is. Daardoor kan een inbraak verholpen worden en wachtwoorden gereset worden.
Onrechtmatige toegang – door buitenstaanders	Wij hebben twee staps verificatie en een dagelijkse backup waardoor informatie teruggehaald kan worden en de essentiële onderdelen altijd na een reset van de server weer terecht is. Daardoor kan een inbraak verholpen worden en wachtwoorden gereset worden.
Ongewenste wijziging van gegevens – interne medewerkers	Wij hebben twee staps verificatie en een dagelijkse backup waardoor informatie teruggehaald kan worden en de essentiële onderdelen altijd na een reset van de server weer terecht is. Daardoor kan een inbraak verholpen worden en wachtwoorden gereset worden.
Ongewenste wijziging van gegevens – door	Wij hebben twee staps verificatie en een dagelijkse backup waardoor informatie teruggehaald kan worden en de essentiële onderdelen altijd na een reset van de server weer terecht is.

buitenstaanders	Daardoor kan een inbraak verholpen worden en wachtwoorden gereset worden.
Verdwijnen / zoekraken van gegevens	Wij hebben twee staps verificatie en een dagelijkse backup waardoor informatie teruggehaald kan worden en de essentiële onderdelen altijd na een reset van de server weer terecht is. Daardoor kan een inbraak verholpen worden en wachtwoorden gereset worden.

Zijn er nog aanvullende organisatorische maatregelen die u neemt?

Nee wij hebben nog geen aanvullende organisatorische maatregelen die wij nemen.

Zijn er nog aanvullende technische maatregelen die u neemt?

Nee wij hebben nog geen aanvullende organisatorische maatregelen die wij nemen.

Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen? Wie is dit:

Dit is Guido Terhorst

Advies van de FG

Heeft u een Functionaris voor de Gegevensbescherming (FG) benoemd? Dan is het verplicht om deze persoon om advies te vragen. Leg het advies van de FG hieronder vast:

Een FG is nog niet bepaald en wordt t.z.t. nog vastgesteld.

Naam FG:
Datum van advies:

Antwoorden van FG:

Zijn de gegevensverwerking en doeleinden duidelijk omschreven?

Is er de verwerking van de persoonsgegevens noodzakelijk of proportioneel voor de doeleinden?

Zijn de privacyrisico's voldoende in kaart gebracht? Welke risico's ontbreken nog?

Advies van betrokkenen en vertegenwoordigers

Is er voor deze DPIA gesproken met betrokkenen of vertegenwoordigers? Welke reactie hebben zij gegeven? Hoe is deze reactie verwerkt?

Voorafgaande raadpleging

Komt er uit de DPIA dat de verwerking een hoog risico oplevert als u geen risicobeperkende maatregelen neemt? Geef antwoord en motivatie hieronder:

Nee want de architectuur van onze website, clouddiensten en app is zo gemaakt dat er geen hoog risico is als er geen risicobeperkende maatregelen worden genomen.

Indien ja, dan moet u een voorafgaande raadpleging aanvragen bij de Autoriteit Persoonsgegevens (AP). Hierbij moet u de DPIA aan de AP verstrekken.