Ministerie van Volksgezondheid, Welzijn en Sport

Stappenplan DPIA

Voor de start van het verwerken van (medische) gegevens is het nodig om alle privacyrisico's in kaart te brengen en maatregelen te nemen om deze risico's te verkleinen. Een Data Protection Impact Assessment (DPIA) helpt hierbij. Hoe zo'n DPIA-proces verloopt en welke stappen je tijdens dit proces moet doorlopen, staat in onderstaand schema.

Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.

Je start met het verwerken van persoonsgegevens in bijvoorbeeld een nieuw softwaresysteem.

In dit systeem worden op grote schaal persoonsgegevens verwerkt.

Breng in kaart welke persoonsgegevens worden gebruikt.

In kaart brengen gegevens

De verwerking van bijvoorbeeld medische gegevens brengt een hoog risico met zich mee voor betrokkenen.

Betrokkenen

Een DPIA is dan verplicht.

Verplicht

Breng de context van de verwerking van (medische) gegevens in kaart.

Context

Risico's

Beoordeel en beschrijf de risico's van de gegevensverwerking.

Beoordeel en beschrijf de kans dat de risico's daadwerkelijk in zullen treden en wat de impact hiervan is.

Aanvullende maatregelen

Beschrijf de voorgenomen maatregelen waarmee de risico's worden aangepakt.

Restrisico's

Zijn er hoge restrisico's?

Ja, er zijn restrisico's, maar hier kunnen aanvullende maatregelen voor worden genomen.

Ja, er zijn restrisico's, maar hiervoor zijn geen aanvullende maatregelen mogelijk. Licht de Autoriteit Persoonsgegevens (AP) hierover in.

Nee, er zijn geen (of weinig) restrisico's.

Je kunt starten met de verwerking.

Periodiek

Samen gezond, fit en veerkrachtig

AVG-Helpdesk voor Zorg, Welzijn en Sport

Ministerie van Volksgezondheid,
Welzijn en Sport

Stappenplan DPIA

Voor de start van het verwerken van (medische) gegevens is het nodig om alle privacyrisico's in kaart te brengen en maatregelen te nemen om deze risico's te verkleinen. Een Data Protection Impact Assessment (DPIA) helpt hierbij. Hoe zo'n DPIA-proces verloopt en welke stappen je tijdens dit proces moet doorlopen, staat in onderstaand schema.

Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.

Je start met het verwerken van persoonsgegevens in bijvoorbeeld een nieuw softwaresysteem.

In dit systeem worden op grote schaal persoonsgegevens verwerkt.

Breng in kaart welke persoonsgegevens worden gebruikt.

De verwerking van bijvoorbeeld medische gegevens brengt een hoog risico met zich mee voor betrokkenen.

In kaart brengen gegevens

Betrokkenen

In kaart brengen gegevens

Beschrijf alle persoonsgegevens die worden verwerkt. Deel deze persoonsgegevens onder naar: gewoon, gevoelig, bijzonder, strafrechtelijk en wettelijk identificatienummer. Geef per categorie persoonsgegevens aan wie de betrokkenen zijn en vanuit welke bron de persoonsgegevens worden verzameld.

Risico's

Beoordeel en beschrijf de risico's van de gegevensverwerking.

Beoordeel en beschrijf de kans dat de risico's daadwerkelijk in zullen treden en wat de impact hiervan is.

Aanvullende maatregelen

Beschrijf de voorgenomen maatregelen waarmee de risico's worden aangepakt.

Restrisico's

Zijn er hoge restrisico's?

Ja, er zijn restrisico's, maar hier kunnen aanvullende maatregelen voor worden genomen.

Nee, er zijn geen (of weinig) restrisico's.

Ja, er zijn restrisico's, maar hiervoor zijn geen aanvullende maatregelen mogelijk. Licht de Autoriteit Persoonsgegevens (AP) hierover in.

Je kunt starten met de verwerking.

Periodiek

Samen gezond, fit en veerkrachtig

AVG-Helpdesk
voor Zorg, Welzijn en Sport

Ministerie van Volksgezondheid,
Welzijn en Sport

Stappenplan DPIA

Voor de start van het verwerken van (medische) gegevens is het nodig om alle privacyrisico's in kaart te brengen en maatregelen te nemen om deze risico's te verkleinen. Een Data Protection Impact Assessment (DPIA) helpt hierbij. Hoe zo'n DPIA-proces verloopt en welke stappen je tijdens dit proces moet doorlopen, staat in onderstaand schema.

Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.

Je start met het verwerken van persoonsgegevens in bijvoorbeeld een nieuw softwaresysteem.

In dit systeem worden op grote schaal persoonsgegevens verwerkt.

Breng in kaart welke persoonsgegevens worden gebruikt.

In kaart brengen gegevens +

De verwerking van bijvoorbeeld medische gegevens brengt een hoog risico met zich mee voor betrokkenen.

Betrokkenen ×

Betrokkenen

Betrokkenen zijn de personen van wie je gegevens verwerkt. Voorbeelden hiervan zijn: patiënten, cliënten, medewerkers, vrijwilligers, leden etc.

Risico's +

Beoordeel en beschrijf de risico's van de gegevensverwerking.

Breng de verwerki gegeven

Context +

Beoordeel en beschrijf de kans dat de risico's daadwerkelijk in zullen treden en wat de impact hiervan is.

Aanvullende maatregelen +

Beschrijf de voorgenomen maatregelen waarmee de risico's worden aangepakt.

Restrisico's +

Zijn er hoge restrisico's?

Ja, er zijn restrisico's, maar hier kunnen aanvullende maatregelen voor worden genomen.

Nee, er zijn geen (of weinig) restrisico's.

Ja, er zijn restrisico's, maar hiervoor zijn geen aanvullende maatregelen mogelijk. Licht de Autoriteit Persoonsgegevens (AP) hierover in.

Je kunt starten met de verwerking.

Periodiek +

Samen gezond, fit en veerkrachtig

AVG-Helpdesk
voor Zorg, Welzijn en Sport

Ministerie van Volksgezondheid,
Welzijn en Sport

Stappenplan DPIA

Voor de start van het verwerken van (medische) gegevens is het nodig om alle privacyrisico's in kaart te brengen en maatregelen te nemen om deze risico's te verkleinen. Een Data Protection Impact Assessment (DPIA) helpt hierbij. Hoe zo'n DPIA-proces verloopt en welke stappen je tijdens dit proces moet doorlopen, staat in onderstaand schema.

Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.

Je start met het verwerken van persoonsgegevens in bijvoorbeeld een nieuw softwaresysteem.

In dit systeem worden op grote schaal persoonsgegevens verwerkt.

Breng in kaart welke persoonsgegevens worden gebruikt.

In kaart brengen gegevens +

De verwerking van bijvoorbeeld medische gegevens brengt een hoog risico met zich mee voor betrokkenen.

Betrokkenen +

Verplicht

Een DPIA is verplicht als het verwerken van gegevens een hoog privacyrisico heeft. Door het gebruik van een grote hoeveelheid aan gegevens en het soort gegevens, die voor een langere tijd worden gebruikt, is er in de gezondheidszorg vaak sprake van een hoog privacyrisico. De Autoriteit Persoonsgegevens (AP) heeft een lijst van verwerkingen samengesteld. Staat de verwerking op deze lijst dan is een DPIA verplicht:

1. Heimelijk onderzoek
2. Zwarte lijsten
3. Fraudebestrijding
4. Creditscores
5. Financiële situatie
6. Genetische persoonsgegevens
7. Gezondheidsgegevens
8. Samenwerkingsverbanden
9. Cameratoezicht
10. Flexibel cameratoezicht (bijvoorbeeld camera's op de kleding of helm van brandweer- of ambulancepersoneel, of het gebruik van dashcams door hulpdiensten)
11. Controle werknemers (bijvoorbeeld door het monitoren van internetgebruik)
12. Locatiegegevens
13. Communicatiegegevens
14. Internet of Things
15. Profilering
16. Observatie en beïnvloeding van gedrag (bijvoorbeeld bij online behavioral advertising)
17. Biometrische gegevens

Let op: het kan zijn dat de verwerking van persoonsgegevens die je voor ogen hebt, niet op deze lijst staat. In dat geval zal je zelf moeten bepalen of de verwerking van persoonsgegevens een hoog risico oplevert voor de betrokkenen.

→ Data protection impact assessment (DPIA)
→ autoriteitpersoonsgegevens.nl
→ Staatscourant 2019 nr. 64418

Een DPIA is dan verplicht.

Verplicht ×

s dat de
n treden en

Ja, er zijn restrisico's, maar hier kunnen aanvullende maatregelen voor worden genomen.

Nee, er zijn geen (of weinig) restrisico's.

Ja, er zijn restrisico's, maar hiervoor zijn geen aanvullende maatregelen mogelijk. Licht de Autoriteit Persoonsgegevens (AP) hierover in.

Je kunt starten met de verwerking.

Periodiek +

Samen gezond, fit en veerkrachtig

AVG-Helpdesk
voor Zorg, Welzijn en Sport

Ministerie van Volksgezondheid, Welzijn en Sport

Stappenplan DPIA

Voor de start van het verwerken van (medische) gegevens is het nodig om alle privacyrisico's in kaart te brengen en maatregelen te nemen om deze risico's te verkleinen. Een Data Protection Impact Assessment (DPIA) helpt hierbij. Hoe zo'n DPIA-proces verloopt en welke stappen je tijdens dit proces moet doorlopen, staat in onderstaand schema.

Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.

Je start met het verwerken van persoonsgegevens in bijvoorbeeld een nieuw softwaresysteem.

In dit systeem worden op grote schaal persoonsgegevens verwerkt.

Breng in kaart welke persoonsgegevens worden gebruikt.

In kaart brengen gegevens +

De verwerking van bijvoorbeeld medische gegevens brengt een hoog risico met zich mee voor betrokkenen.

Betrokkenen +

Risico's +

Beoordeel en beschrijf de risico's van de gegevensverwerking.

Breng de context van de verwerking van (medische) gegevens in kaart.

Context ×

Een DPIA is dan verplicht.

Verplicht +

Beoordeel en beschrijf de kans dat de risico's daadwerkelijk in zullen treden en wat de impact hiervan is.

Context

Beantwoord de volgende vragen om de context, waarbinnen de gegevens worden verwerkt, in kaart te brengen.

- In welke context wordt de verwerking uitgevoerd? Beschrijf het voorstel van gegevensverwerking waar de DPIA op toeziet op hoofdlijnen en benoem hoe dit tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming hiervan.
- Wat is het doel van de verwerking?
- Welke gegevens worden er van een patiënt verzameld?
- Zijn de verzamelde gegevens noodzakelijk voor het proces?
- Wie zijn er allemaal betrokken bij de gegevensverwerking? Wie heeft er toegang tot de gegevens?
- Wat zijn de belangen van de betrokken partijen?
- In welke landen vinden de gegevensverwerkingen plaats? Geef aan of en welke aanvullende maatregelen van toepassing zijn wanneer verwerkingslocaties zich buiten de Europese Economische Ruimte bevinden.
- Welke technieken en methoden van gegevensverwerking worden er gebruikt?
- Welke wet- en regelgeving is van toepassing op de gegevensverwerking?
- Wat zijn de bewaartermijnen van de persoonsgegevens?
- Wordt er rekening gehouden met de rechten van de betrokkene?

Nee, er zijn geen (of weinig) restrisico's.

Je kunt starten met de verwerking.

Periodiek +

Samen gezond, fit en veerkrachtig

AVG-Helpdesk voor Zorg, Welzijn en Sport

Ministerie van Volksgezondheid,
Welzijn en Sport

Stappenplan DPIA

Voor de start van het verwerken van (medische) gegevens is het nodig om alle privacyrisico's in kaart te brengen en maatregelen te nemen om deze risico's te verkleinen. Een Data Protection Impact Assessment (DPIA) helpt hierbij. Hoe zo'n DPIA-proces verloopt en welke stappen je tijdens dit proces moet doorlopen, staat in onderstaand schema.

Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.

Je start met het verwerken van persoonsgegevens in bijvoorbeeld een nieuw softwaresysteem.

In dit systeem worden op grote schaal persoonsgegevens verwerkt.

Breng in kaart welke persoonsgegevens worden gebruikt.

In kaart brengen gegevens +

De verwerking van bijvoorbeeld medische gegevens brengt een hoog risico met zich mee voor betrokkenen.

Betrokkenen +

Breng de context van de verwerking van (medische) gegevens in kaart.

Een DPIA is dan verplicht.

Verplicht +

Risico's ×

Beoordeel en beschrijf de risico's van de

Risico's

Beschrijf en beoordeel de risico's van de geplande gegevensverwerking voor de rechten en vrijheden (bijv. financiële schade) van de betrokkenen. Neem hierbij de volgende stappen:

Stap 1: Stel de (mogelijke) risico's vast

Stap 2: Schat in hoe groot de kans is dat het risico zich voordoet

Stap 3: Beoordeel of de risico's aanvaardbaar zijn

Ga in ieder geval in op:

a) welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
b) de herkomst van deze gevolgen;
c) de waarschijnlijkheid (kans) dat dit gaat gebeuren;
d) de ernst (impact) van deze gevolgen voor de betrokkenen als dit gebeurt.

Er is sprake van een onacceptabel hoog (rest)risico wanneer de betrokkenen getroffen worden met significante of onomkeerbare gevolgen die hij mogelijk niet te boven komt of de kans daarop aanzienlijk is.

Ja, er zijn restrisico's, maar hier kunnen aanvullende maatregelen voor worden genomen.

Nee, er zijn geen (of weinig) restrisico's.

Ja, er zijn restrisico's, maar hiervoor zijn geen aanvullende maatregelen mogelijk. Licht de Autoriteit Persoonsgegevens (AP) hierover in.

Je kunt starten met de verwerking.

Periodiek +

Samen gezond, fit en veerkrachtig

AVG-Helpdesk
voor Zorg, Welzijn en Sport

Ministerie van Volksgezondheid,
Welzijn en Sport

Stappenplan DPIA

Voor de start van het verwerken van (medische) gegevens is het nodig om alle privacyrisico's in kaart te brengen en maatregelen te nemen om deze risico's te verkleinen. Een Data Protection Impact Assessment (DPIA) helpt hierbij. Hoe zo'n DPIA-proces verloopt en welke stappen je tijdens dit proces moet doorlopen, staat in onderstaand schema.

Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.

Je start met het verwerken van persoonsgegevens in bijvoorbeeld een nieuw softwaresysteem.

In dit systeem worden op grote schaal persoonsgegevens verwerkt.

Breng in kaart welke persoonsgegevens worden gebruikt.

In kaart brengen gegevens +

De verwerking van bijvoorbeeld medische gegevens brengt een hoog risico met zich mee voor betrokkenen.

Betrokkenen +

Risico's +

Beoordeel en beschrijf de risico's van de gegevensverwerking.

Breng de context van de verwerking van (medische) gegevens in kaart.

Context +

Een DPIA is dan verplicht.

Verplicht +

Beoordeel en beschrijf de kans dat de risico's daadwerkelijk in zullen treden en wat de impact hiervan is.

Aanvullende maatregelen ×

Aanvullende maatregelen

Voor het nemen van aanvullende maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, 'beste praktijken' en goedgekeurde gedragscodes en certificeringsmechanismen.

Ter illustratie noemt de AVG de volgende maatregelen:

a. pseudonimiseren en versleutelen van persoonsgegevens;
b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- opslag van gegevens in een kluis;
- project-, risico- en incidentenmanagement;
- data opsplitsen;
- dataminimalisatie;
- back-ups;
- integriteitscontroles;
- meerfactor-authenticatie;
- monitoring en logging;
- controle van toegekende bevoegdheden;
- privacybewustzijn- en beveiligingstrainingen;
- managementrapportages over risicobeheer;
- beperken inzageniveau;
- periodiek een audit of hack- of penetratietest uitvoeren;
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- responsible-disclosurebeleid;
- geheimhoudingsverklaringen;
- service level agreements (met boeteclausules);
- verwerkersovereenkomsten;
- screening personeel en VOG-verklaring.

Ministerie van Volksgezondheid,
Welzijn en Sport

Stappenplan DPIA

Voor de start van het verwerken van (medische) gegevens is het nodig om alle privacyrisico's in kaart te brengen en maatregelen te nemen om deze risico's te verkleinen. Een Data Protection Impact Assessment (DPIA) helpt hierbij. Hoe zo'n DPIA-proces verloopt en welke stappen je tijdens dit proces moet doorlopen, staat in onderstaand schema.

Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.

Je start met het verwerken van persoonsgegevens in bijvoorbeeld een nieuw softwaresysteem.

In dit systeem worden op grote schaal persoonsgegevens verwerkt.

Breng in kaart welke persoonsgegevens worden gebruikt.

In kaart brengen gegevens +

De verwerking van bijvoorbeeld medische gegevens brengt een hoog risico met zich mee voor betrokkenen.

Betrokkenen +

Risico's +

Beoordeel en beschrijf de risico's van de

Breng de context van de verwerking van (medische) gegevens in kaart.

Een DPIA is dan verplicht.

Verplicht +

Restrisico's

Na beoordeling en beschrijving van de risico's en voorgenomen maatregelen om deze risico's te beperken blijven er nog zogenaamde restrisico's over. Het is namelijk niet mogelijk om risico's volledig uit te sluiten.

Besteed aandacht aan de volgende punten bij beoordeling van de restrisico's:

- Geef aan welke risico's niet volledig door de genomen maatregelen voorkomen worden.
- Vermeld specifiek in welke situatie met welke persoonsgegevens een restrisico aanwezig is.
- Schat de restrisico's in met de formule kans x impact. Kortom, beoordeel en beschrijf de kans dat dit restrisico op zal treden en beoordeel en beschrijf de impact van deze restrisico's.
- Beschrijf helder en duidelijk waarom deze restrisico's na het nemen van de maatregelen acceptabel zijn.

waarmee de risico's worden aangepakt.

Restrisico's ×

Zijn er hoge restrisico's?

Ja, er zijn restrisico's, maar hier kunnen aanvullende maatregelen voor worden genomen.

Nee, er zijn geen (of weinig) restrisico's.

Ja, er zijn restrisico's, maar hiervoor zijn geen aanvullende maatregelen mogelijk. Licht de Autoriteit Persoonsgegevens (AP) hierover in.

Je kunt starten met de verwerking.

Periodiek +

Samen gezond, fit en veerkrachtig

AVG-Helpdesk
voor Zorg, Welzijn en Sport

Ministerie van Volksgezondheid,
Welzijn en Sport

Stappenplan DPIA

Voor de start van het verwerken van (medische) gegevens is het nodig om alle privacyrisico's in kaart te brengen en maatregelen te nemen om deze risico's te verkleinen. Een Data Protection Impact Assessment (DPIA) helpt hierbij. Hoe zo'n DPIA-proces verloopt en welke stappen je tijdens dit proces moet doorlopen, staat in onderstaand schema.

Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.

Je start met het verwerken van persoonsgegevens in bijvoorbeeld een nieuw softwaresysteem.

In dit systeem worden op grote schaal persoonsgegevens verwerkt.

Breng in kaart welke persoonsgegevens worden gebruikt.

In kaart brengen gegevens +

De verwerking van bijvoorbeeld medische gegevens brengt een hoog risico met zich mee voor betrokkenen.

Betrokkenen +

Risico's +

Beoordeel en beschrijf de risico's van de gegevensverwerking.

Breng de context van de verwerking van (medische) gegevens in kaart.

Context +

Een DPIA is dan verplicht.

Verplicht +

Beoordeel en beschrijf de kans dat de risico's daadwerkelijk in zullen treden en wat de impact hiervan is.

Aanvullende maatregelen +

Beschrijf de voorgenomen maatregelen waarmee de risico's worden aangepakt.

Restrisico's +

Zijn er hoge restrisico's?

Ja, er zijn restrisico's, maar hier kunnen aanvullende maatregelen voor worden genomen.

Nee, er zijn geen (of weinig) restrisico's.

Ja, er zijn restrisico
aanvullende maat
Persoonsgegevens

Je kur

Periodiek

Een DPIA kan meerdere keren en op verschillende momenten worden uitgevoerd en geactualiseerd. Bij een wijziging van de regelgeving of project waarbij de verwerkingen van persoonsgegevens een rol spelen, wordt opnieuw een DPIA uitgevoerd. De DPIA wordt opnieuw beoordeeld om te controleren of de manier van gegevensverwerking of de effecten van gegevensverwerking is veranderd. Het advies is om een DPIA elke drie jaar te evalueren.

Periodiek ×

Samen gezond, fit en veerkrachtig

AVG-Helpdesk
voor Zorg, Welzijn en Sport