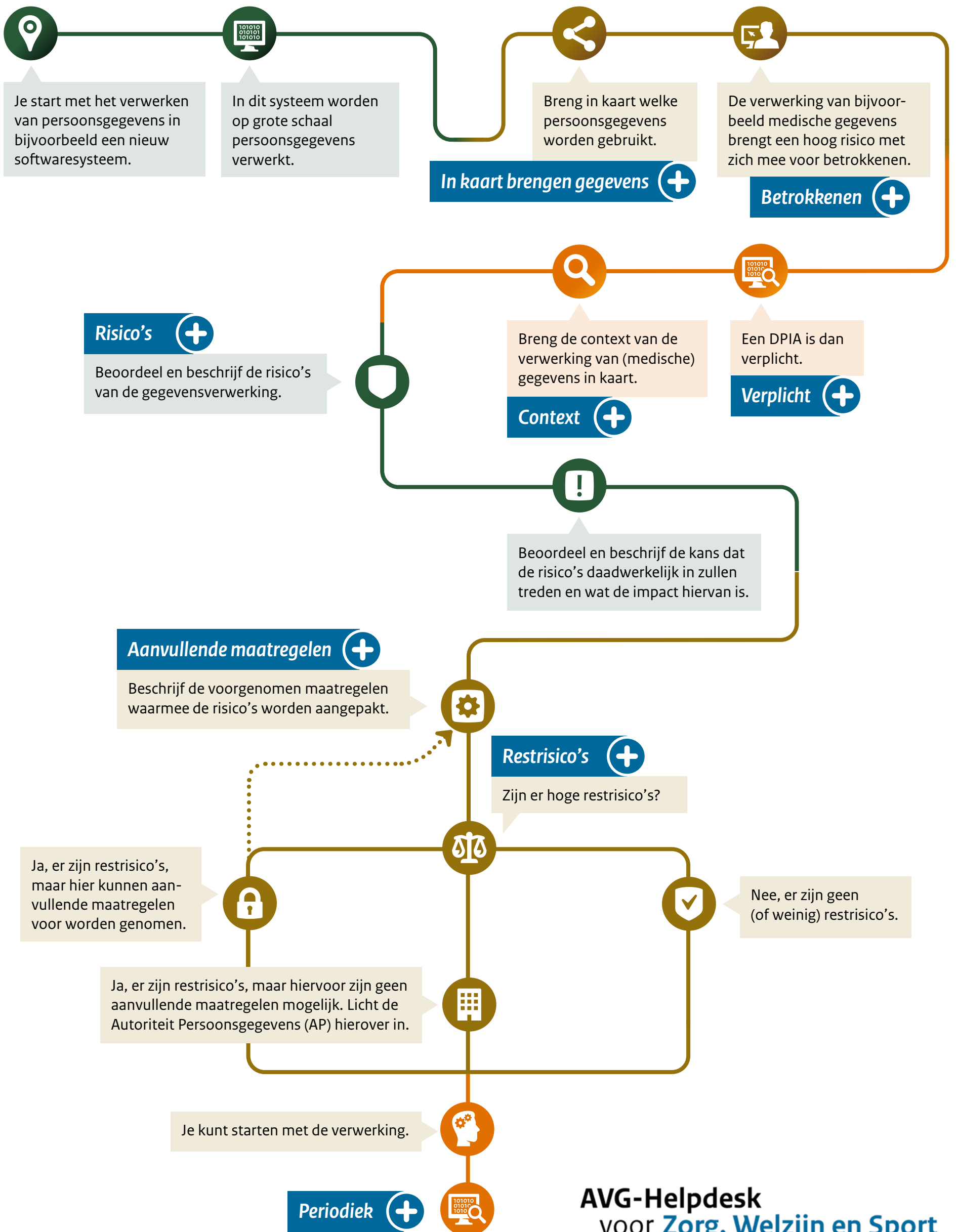




Stappenplan DPIA

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.

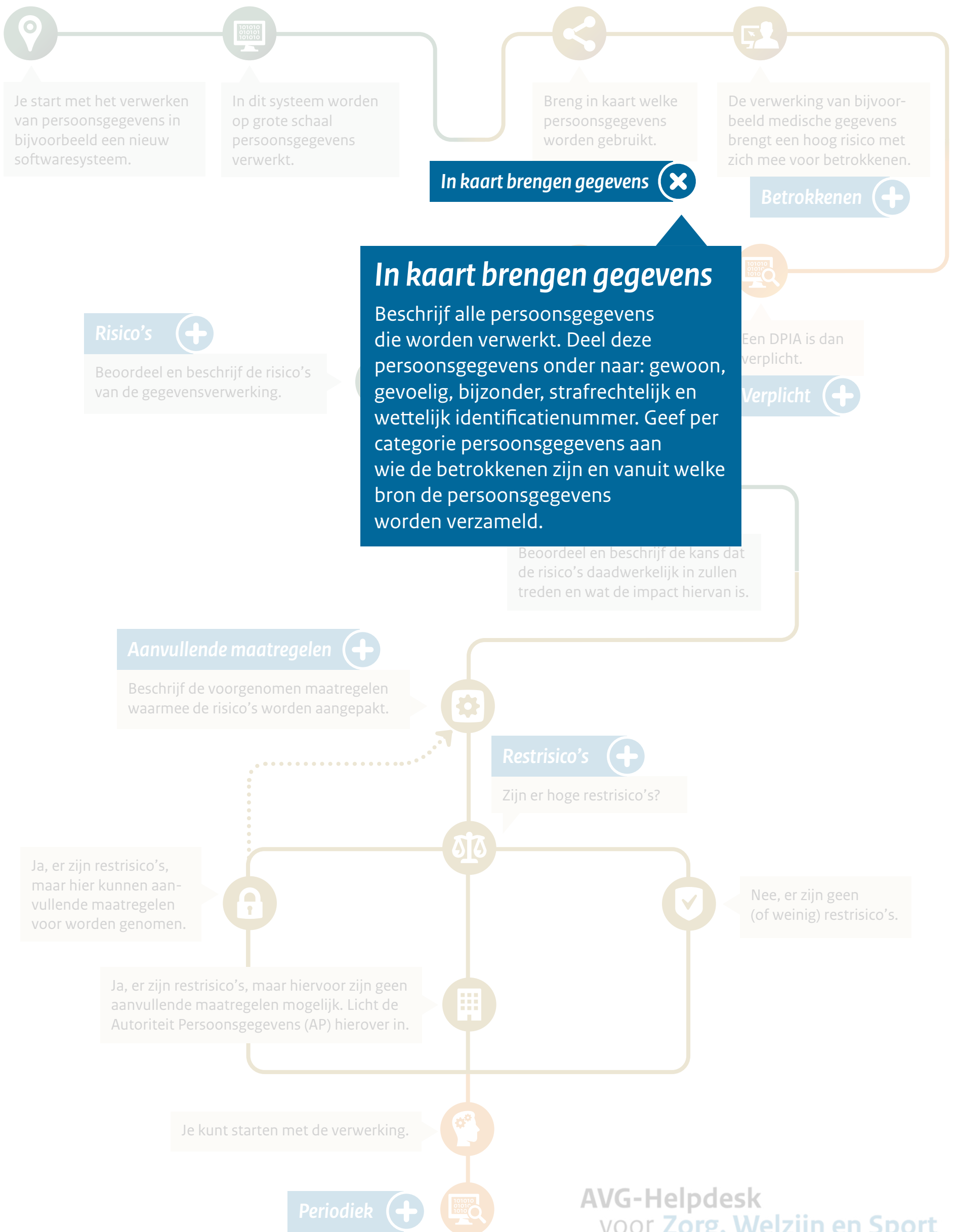
Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.



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.

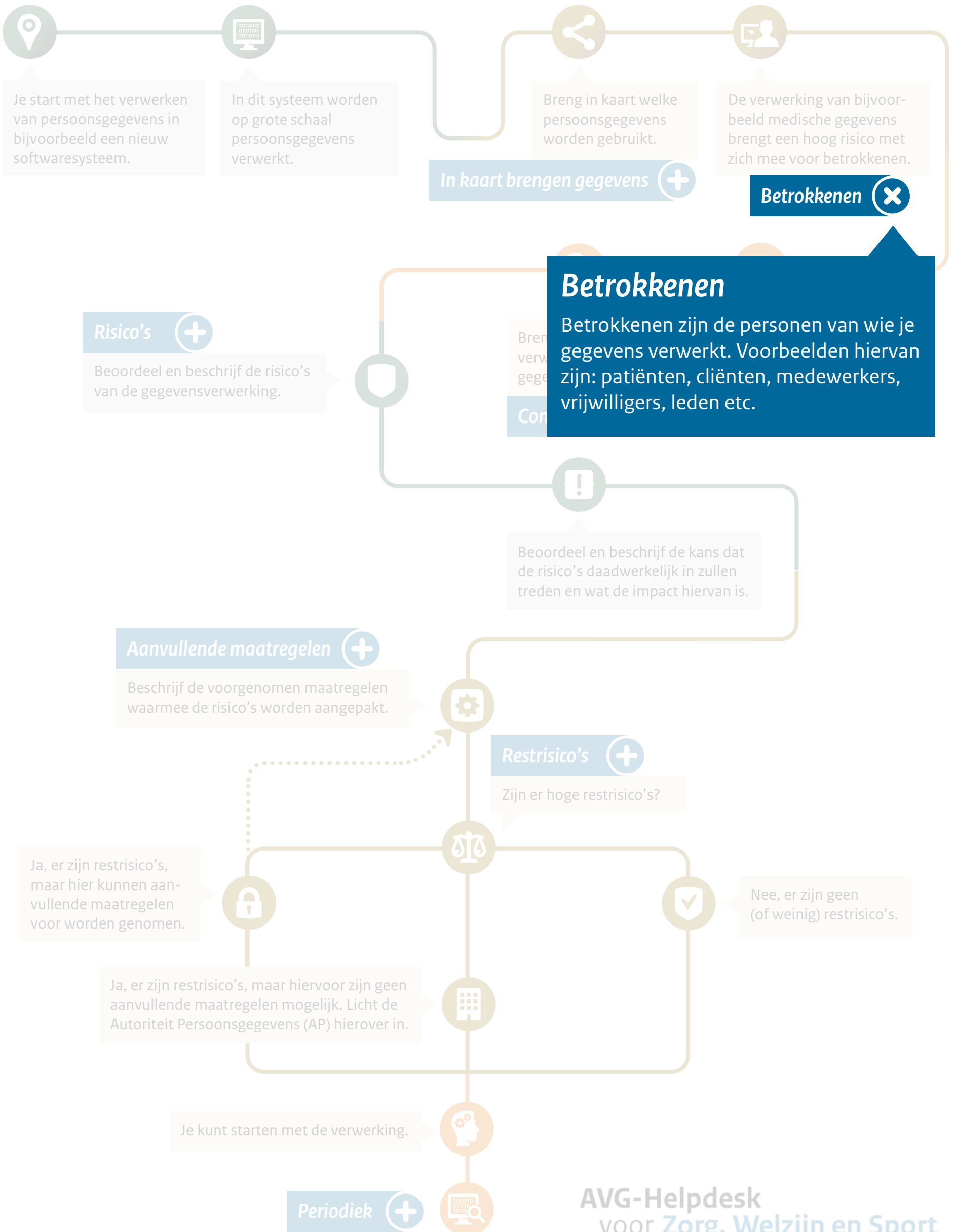
Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.



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.



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.

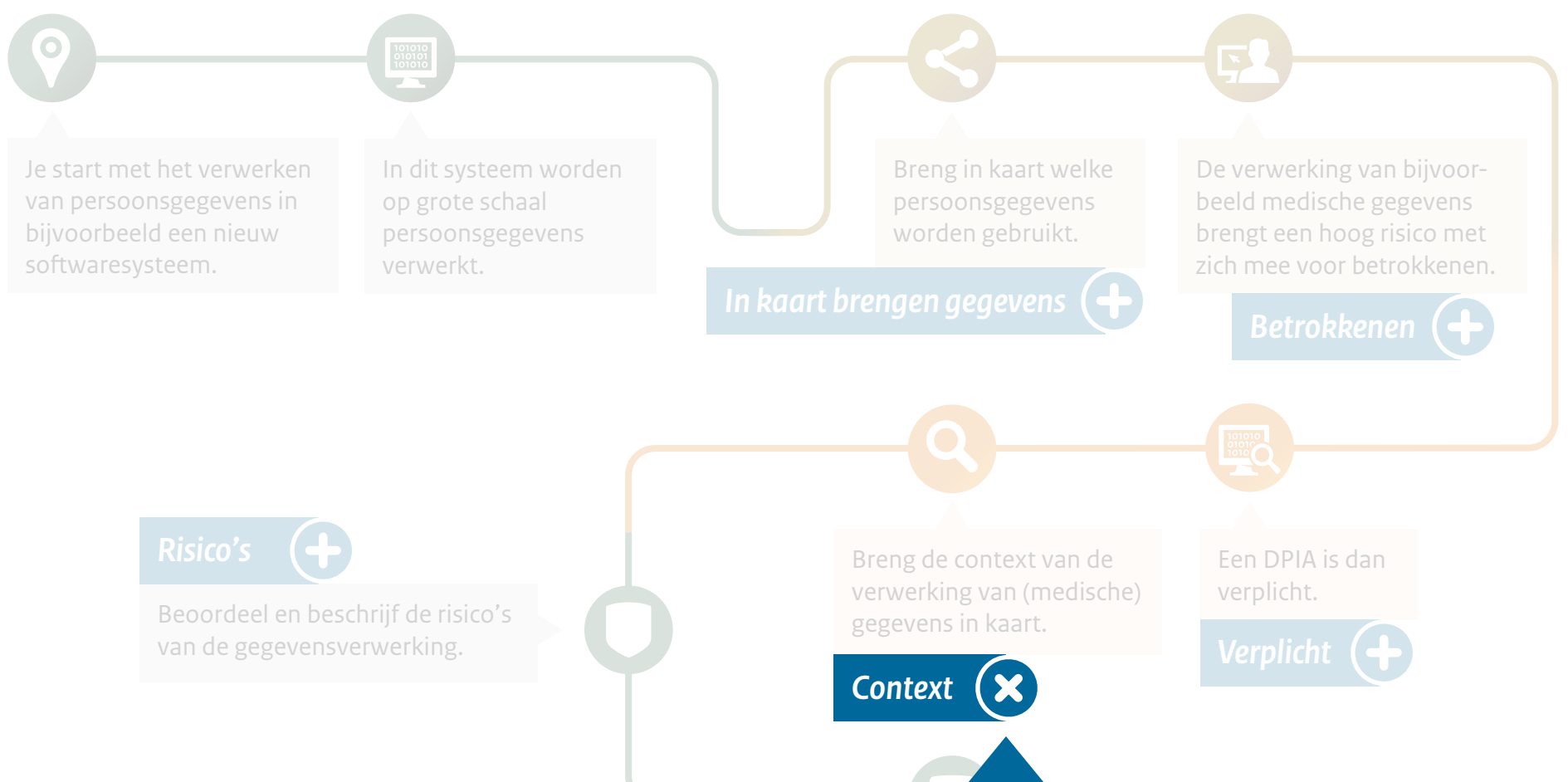
Op www.avghelpdeskzorg.nl vind je nog meer informatie over de AVG en privacy gerelateerde onderwerpen.



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.



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.

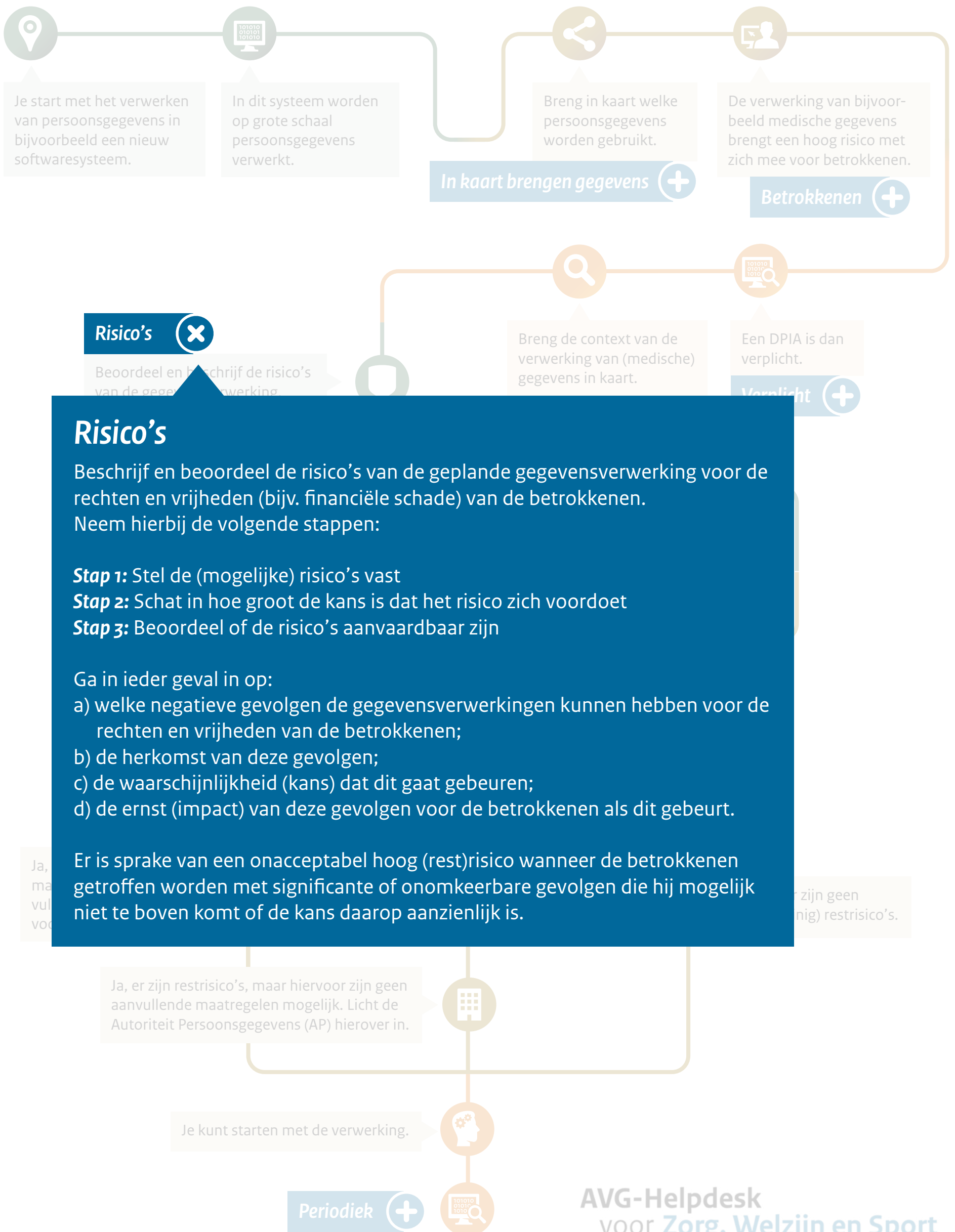
Periodiek +



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.



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:

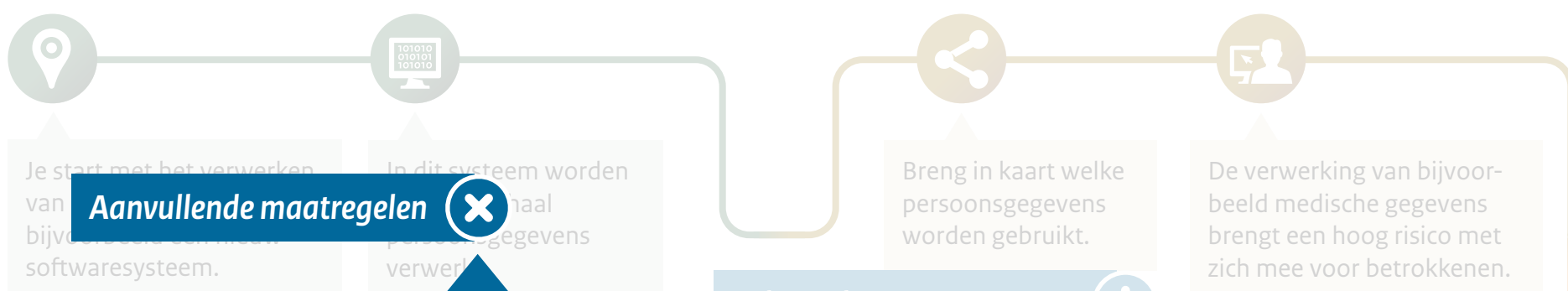
- a) welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
- b) de herkomst van deze gevolgen;
- c) de waarschijnlijkheid (kans) dat dit gaat gebeuren;
- d) de ernst (impact) van deze gevolgen voor de betrokkenen als dit gebeurt.

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.

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.



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:

- pseudonimiseren en versleutelen van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- 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.

Risico's

Beoordeel en beschrijf de risico's van de gegevensverwerking.

Aanvullende maatregelen

Beschrijf de aanvullende maatregelen waarmee de risico's worden verkleind.

Ja, er zijn restrycties, maar hier kunnen aanvullende maatregelen voor worden genomen.

Ja, er zijn restrycties, maar hier kunnen aanvullende maatregelen worden genomen. Autoriteit Persoonsgegevens

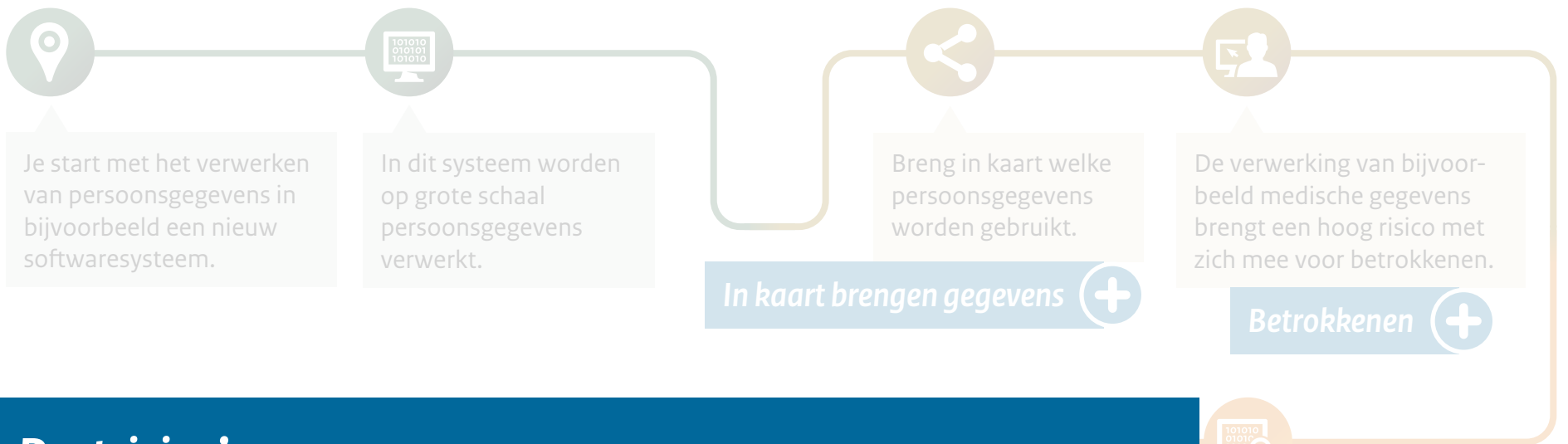
Je kunt...



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.



Restrisico's

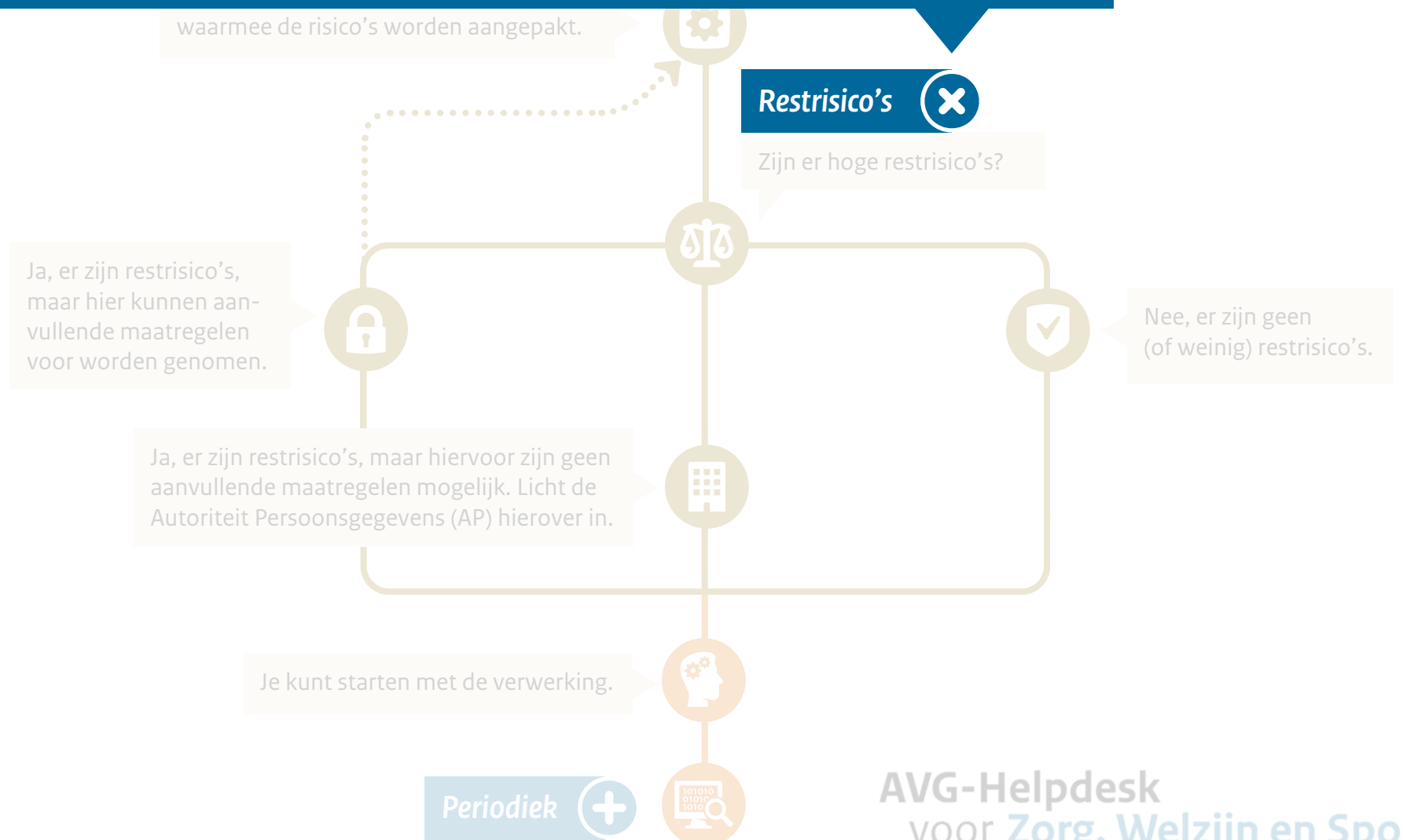
Na beoordeling en beschrijving van de risico's en voorgenomen maatregelen om deze risico's te beperken blijven er nog zogenaamde restrisico's over. Het is namelijk niet mogelijk om risico's volledig uit te sluiten.

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.



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.

