<Klantnaam>

PRIVACY ASSURANCE-RAPPORTAGE VERWERKING PERSOONSGEGEVENS IN <OBJECT>

Over periode van <start verslagperiode>

tot en met <einde verslagperiode>

<Datum rapportage>

Logo «Klantnaam»

1. VERMELDING VAN <KLANTNAAM>

Wij, <klantnaam>, zijn verantwoordelijk voor het beheer van het <object> en het opzetten, implementeren en effectief laten werken van interne beheersingsmaatregelen rondom de verwerking van de persoonsgegevens in het <object>.

Wij hebben hiertoe interne beheersingsmaatregelen opgezet, geïmplementeerd en toegepast om de privacy-beheersingsdoelstellingen zoals vermeld in het hoofdstuk 'Beheersingsraamwerk' te bereiken. De privacy-beheersingsdoelstellingen zijn afkomstig uit het Privacy Control Framework versie 2.0 van NOREA[1].

Wij bevestigen dat:

a) De interne beheersingsmaatregelen die verband houden met de privacy-beheersingsdoelstellingen die afkomstig zijn uit het Privacy Control Framework van NOREA versie 2.0 op afdoende wijze zijn opgezet, geïmplementeerd en effectief werkten gedurende de verslagperiode van <start verslagperiode> tot en met <einde verslagperiode>, met uitzondering van de beheersingsmaatregelen beschreven onder punt b. De criteria waarvan bij het maken van deze vermelding gebruik werd gemaakt hielden in dat:
   i. De risico's die het bereiken van de privacy beheersingsdoelstellingen uit het Privacy Control Framework in gevaar brengen, werden geïdentificeerd.
   ii. De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de privacy-beheersingsdoelstellingen uit het Privacy Control Framework niet zouden verhinderen.
   iii. Het beheersingsraamwerk geeft weer welke beheersingsmaatregelen zijn geïmplementeerd en als zodanig bestaan binnen onze organisatie.
   iv. De interne beheersingsmaatregelen gedurende de verslagperiode van <start verslagperiode> tot <einde verslagperiode> consistent zijn toegepast zoals opgezet, met inbegrip ervan dat handmatige interne beheersingsmaatregelen zijn toegepast door personen die de geschikte competentie en bevoegdheid hebben.

b) De volgende beheersingsmaatregelen hebben niet gewerkt gedurende de verslagperiode
   - Beheersingsmaatregel [naam]

<klantnaam>
<naam tekenend persoon klant>
<functie tekenend persoon klant>

<plaats tekenen klant>, [datum rapportage]

[1] https://www.norea.nl/download/?id=6038

2. ASSURANCE-RAPPORT VAN ONAFHANKELIJKE IT-AUDITOR

Aan: de directie van <klantnaam>.

Wij hebben het beheersingsraamwerk zoals opgenomen in hoofdstuk 3 onderzocht om te rapporteren over de opzet, het bestaan en de werking van de interne beheersingsmaatregelen die verband houden met de privacy-beheersingsdoelstellingen afkomstig uit het Privacy Control Framework versie 2.0 van NOREA gedurende de periode van <start verslagperiode> tot en met <einde verslagperiode> voor de verwerking van persoonsgegevens in <object>.

2.1 Ons oordeel [met beperking]

Naar ons oordeel, in alle van materieel belang zijnde aspecten [uitgezonderd de aangelegenheden die staan beschreven in de paragraaf 'Basis voor ons oordeel met beperking']:

a) Zijn de interne beheersingsmaatregelen die verband houden met de privacy-beheersingsdoelstellingen van <start verslagperiode> tot en met <einde verslagperiode> op afdoende wijze opgezet om de privacy-beheersingsdoelstellingen te bereiken indien de beheersingsmaatregelen effectief werkten gedurende de periode van <start verslagperiode> tot en met <einde verslagperiode>;
b) Bestaan de interne beheersingsmaatregelen binnen de organisatie zoals beschreven in het beheersingsraamwerk gedurende de periode van <start verslagperiode> tot en met <einde verslagperiode>; en
c) Hebben de getoetste interne beheersingsmaatregelen effectief gewerkt om de privacy-beheersingsdoelstellingen te bereiken gedurende de periode van <start verslagperiode> tot en met <einde verslagperiode>.

De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die in de vermelding van <klantnaam> staan beschreven voor de verwerking van persoonsgegevens in <object> voor belanghebbenden van <klantnaam>.

Ons oordeel is gevormd op basis van de aangelegenheden die in deze rapportage zijn uiteengezet. De specifieke, getoetste interne beheersingsmaatregelen en de aard, timing en resultaten van die toetsingen zijn opgenomen in 3.2 Beheersingsraamwerk inclusief testwerkzaamheden en resultaten (hierna: de 'beschrijving van toetsingen').

2.2 De basis voor ons oordeel [met beperking]

Wij hebben vastgesteld van de hieronder genoemde beheersingsmaatregelen dat deze niet op afdoende wijze zijn opgezet en/of de gehele periode effectief hebben gewerkt:

a) Toelichting bevinding 1

b) Toelichting bevinding 2

Wij hebben onze opdracht uitgevoerd overeenkomstig Richtlijn 3000A 'Attest-opdrachten' van NOREA, de beroepsorganisatie van IT-auditors in Nederland. Deze opdracht is gericht

op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van <klantnaam> en hebben de vereisten nageleefd van het NOREA Reglement Gedragscode ('Code of Ethics', een reglement met betrekking tot integriteit, objectiviteit, vakbekwaamheid en zorgvuldigheid, geheimhouding en professioneel gedrag).

Wij vinden dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor ons oordeel [met beperking].

Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

<optionele nadere duiding van reikwijdte>

Ons oordeel is niet aangepast als gevolg van deze aangelegenheden.

2.3 Beperkingen van interne beheersingsmaatregelen

Het bereiken van de privacy-beheersingsdoelstellingen uit het Privacy Control Framework is geen garantie voor volledige compliance met de geldende Algemene Verordening Gegevensbescherming (AVG).

Interne beheersingsmaatregelen bij een organisatie kunnen, vanwege hun aard, niet alle fouten of omissies bij het verwerken van persoonsgegevens voorkomen of ontdekken, waaronder de mogelijkheid van menselijke fouten en het omzeilen van interne beheersingsmaatregelen. Vanwege deze inherente beperkingen kan een entiteit redelijke, maar niet absolute zekerheid verkrijgen dat alle privacy-incidenten die leiden tot beschadiging van de belangen van individuele personen of het niet naleven van de op de bescherming van persoonsgegevens betrekking hebbende wet- en regelgeving worden voorkomen en, voor degenen die niet worden voorkomen, tijdig worden gedetecteerd.

Ons onderzoek heeft geen betrekking op toekomstige perioden. Derhalve kunnen wij niet uitsluiten dat zich in de toekomst gebeurtenissen voordoen die kunnen leiden tot een afwijking van het stelsel van maatregelen en procedures of kunnen leiden dat de beheersingsmaatregelen ontoereikend worden als gevolg van veranderingen in de omstandigheden.

2.4 Doeleinden assurance rapport en beoogde gebruikers

Ons assurance rapport heeft als doel om de mate van vertrouwen te versterken met betrekking tot het stelsel van maatregelen en procedures van <klantnaam> gericht op de bescherming van persoonsgegevens in <object>. Deze rapportage en de beschrijving van toetsingen van de privacy-beheersingsdoelstellingen zijn voor belanghebbenden van <klantnaam> voor de verwerking van persoonsgegevens in <object>.

2.5 Verantwoordelijkheden van het bestuur van <klantnaam>

Het bestuur van <klantnaam> is verantwoordelijk voor:

a) het opstellen van de vermelding, met inbegrip van de volledigheid en nauwkeurigheid van de vermelding;
b) het verwerken van persoonsgegevens in <object>;
c) het identificeren van de risico's die een bedreiging vormen voor het bereiken van de privacy-beheersingsdoelstellingen;
d) het opstellen van interne beheersingsmaatregelen om de privacy-beheersingsdoelstellingen te bereiken en de mapping van interne beheersingsmaatregelen aan privacy-beheersingsdoelstellingen; en
e) het opzetten, implementeren en effectief laten werken van interne beheersingsmaatregelen om de privacy-beheersingsdoelstellingen afkomstig uit het Privacy Control Framework versie 2.0 van NOREA te bereiken.

Het bestuur is tevens verantwoordelijk voor het monitoren van interne beheersingsmaatregelen teneinde hun effectiviteit vast te stellen, tekortkomingen te identificeren en corrigerende acties te nemen.

2.6 Verantwoordelijkheden van de IT-auditor

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel over de opzet en werking van interne beheersingsmaatregelen die verband houden met de privacy-beheersingsdoelstellingen in overeenstemming met de criteria die zijn beschreven in de Vermelding van <klantnaam> en die in het hoofdstuk 'Beheersingsraamwerk inclusief testwerkzaamheden en resultaten' staan vermeld..

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële fouten en fraude ontdekken.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhouden een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.

Ons onderzoek van de opzet en effectieve werking van interne beheersingsmaatregelen, bestond onder andere uit:

a) het identificeren en inschatten van de risico's dat interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet of effectief werken om de privacy beheersingsdoelstellingen afkomstig uit het Privacy Control Framework versie 2.0 van NOREA te bereiken gedurende de periode van <start verslagperiode> tot en met <einde verslagperiode> als gevolg van fouten of fraude, het in reactie op deze risico's bepalen van assurance werkzaamheden voor het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel;

b) het evalueren van de geschiktheid van de privacy-beheersingsdoelstellingen en de geschiktheid van de criteria die door de serviceorganisatie zijn beschreven in de Vermelding van <klantnaam>;

c) het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de opzet van interne beheersingsmaatregelen om de privacy-beheersingsdoelstellingen te bereiken;

d) het toetsen van de werking van de interne beheersingsmaatregelen die noodzakelijk zijn voor het verschaffen van een redelijke mate van zekerheid dat de privacy-beheersingsdoelstellingen werden bereikt.

<plaats>, <datum rapportage>

<organisatie>

Namens deze,

<naam>

<functie>

3 BEHEERSINGSRAAMWERK

3.1 Informatie van de IT-auditor

Ons onderzoek is uitgevoerd in overeenstemming met de Richtlijn 3000A 'Attest-opdrachten' van NOREA

3.1.1 Testprocedures

Wij hebben bepaald welke van de interne beheersingsmaatregelen van <klantnaam> noodzakelijk zijn om de privacy-beheersingsdoelstellingen te bereiken en wij hebben beoordeeld of die interne beheersingsmaatregelen op afdoende wijze zijn opgezet, bestaan en effectief werken. Per onderdeel is een daarop gerichte testprocedure toegepast:

- **Het verzoeken om Inlichtingen:** het trachten te verkrijgen van informatie bij goed ingelichte personen binnen of buiten de entiteit. Het verzoeken om inlichtingen kan gaan van het formeel schriftelijk verzoeken om inlichtingen tot het informeel mondeling verzoeken.
- **Inspectie:** het onderzoeken van interne of externe vastleggingen of documenten op papier, in elektronische vorm of op andere gegevensdragers vastgelegd, dan wel het fysiek onderzoeken van een actief.
- **Waarneming:** het gadeslaan van een proces dat of een procedure die door anderen wordt uitgevoerd
- **Het opnieuw uitvoeren (reperformance):** het op onafhankelijke wijze procedures of interne beheersingsmaatregelen uitvoeren die oorspronkelijk in het kader van de interne beheersing van de entiteit werden uitgevoerd.

De omvang van de deelwaarnemingen die zijn geselecteerd voor het toetsen van de effectieve werking van beheersingsmaatregelen is onder meer afhankelijk van de aard en de frequentie van de beheersingsmaatregel.

Frequentie	Omvang deelwaarneming
Meer dan dagelijks	XX-XX
Dagelijks	XX-XX
Wekelijks	XX-XX
Maandelijks	XX-XX
Ieder kwartaal	XX-XX
Jaarlijks	1

3.1.2 Testresultaten

De privacy-beheersingsdoelstellingen wordt bereikt door het bestaan en de effectieve werking van de gerelateerde beheersingsmaatregelen.. Een beheersingsmaatregel wordt als effectief beschouwd als er geen uitzonderingen zijn geconstateerd. Indien relevante uitzonderingen zijn geconstateerd, hebben wij deze gerapporteerd.

Wanneer een beheersingsmaatregel niet effectief heeft gewerkt gedurende de verslagperiode, hebben wij vastgesteld of deze beheersingsmaatregel wordt gecompenseerd door andere beheersingsmaatregelen ten einde de vermelde beheersingsdoelstelling(en) te bereiken. In het geval dat de ineffectiviteit van een beheersingsmaatregel niet wordt gecompenseerd, concluderen wij dat de beheersingsdoelstelling waar de betreffende beheersingsmaatregel betrekking op heeft niet wordt bereikt.

Onze conclusies per beheersingsmaatregel zijn onder te verdelen in de volgende categorieën:

- Geen relevante uitzonderingen geconstateerd;
- Uitzonderingen met compenserende maatregel: de beheersingsmaatregel heeft niet effectief gewerkt gedurende de verslagperiode, echter de uitzonderingen worden gecompenseerd door een andere beheersingsmaatregel; derhalve wordt de beheersingsdoelstelling wel gerealiseerd;
- Uitzonderingen geconstateerd: de beheersingsmaatregel heeft niet effectief gewerkt gedurende de verslagperiode en compenserende maatregelen zijn niet aanwezig; de uitzonderingen hebben impact op de realisatie van de beheersingsdoelstelling;
- Geen waarneming: er hebben geen activiteiten voorgedaan waarvoor de beheersingsmaatregel uitgevoerd had moeten worden.

In het hiernavolgende beheersingsraamwerk zijn de beheersingsdoelstelling uit het Privacy Control Framework versie 2.0 van NOREA opgenomen en heeft <klant> beheersingsmaatregelen per beheersingsdoelstelling gedefinieerd. Wij hebben de door ons verrichte testprocedures en de daaruit voortkomende testresultaten opgenomen in het beheersingsraamwerk (kolom ‘Testwerkzaamheden’ en ‘Testresultaten’).

3.2 Beheersingsraamwerk inclusief testwerkzaamheden en resultaten

3.2.1 Proces 1: Management

Beheersingsdoelstelling A: Privacy beleid De entiteit stelt een privacy beleid vast en communiceert dit. Dit beleid bevat de doelstellingen en verantwoordelijkheden met betrekking tot privacy en is in overstemming met geaccepteerde privacy principes en de van toepassing zijnde wet- en regelgeving.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling B: Afbakening van rollen en verantwoordelijkheden De entiteit definieert duidelijke rollen en verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens en het behalen van privacy doelstellingen, en implementeert deze.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling C: Identificatie en classificatie van persoonsgegevens De entiteit heeft een duidelijk beeld van en documenteert welke persoonsgegevens worden opgeslagen en verwerkt. Persoonsgegevens worden geïdentificeerd en er wordt op de juiste wijze mee omgegaan. In de maatregelen voor bescherming van persoonsgegevens wordt rekening gehouden met verschillen in de gevoeligheid van persoonsgegevens. Dit leidt tot identificatie van risico's en compliance met wet- en regelgeving.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling D: Risicomanagement De entiteit identificeert, beoordeelt en beperkt systematisch en periodiek de factoren die het behalen van de privacy doelstellingen in gevaar kunnen brengen.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling E: Data Protection Impact Assessments De privacy-gerelateerde effecten van nieuwe producten en diensten en het gebruik ervan binnen de entiteit worden op systematische wijze geïdentificeerd, beoordeeld en aangepakt.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling F: Beheer van privacy incidenten en inbreuken De entiteit detecteert incidenten met betrekking tot privacy en handelt deze af. Op privacy-gerelateerde incidenten wordt adequaat gereageerd met het doel de gevolgen te beperken en er worden maatregelen genomen om toekomstige inbreuken te voorkomen.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling G: Competenties medewerkers Medewerkers die vanuit hun functie toegang hebben tot persoonsgegevens of processen beheren waarin persoonsgegevens worden verwerkt, beschikken over de benodigde competenties met betrekking tot privacy om hun taken naar behoren te kunnen vervullen.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling H: Bewustwording en training medewerkers De medewerkers zijn voldoende op de hoogte van de privacywetgeving en -regelgeving, het privacy beleid en de richtlijnen binnen de organisatie, en hun verantwoordelijkheden met betrekking tot privacy. De entiteit implementeert programma's om bewustwording te bereiken en op peil te houden.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling I: Juridische toets van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten Privacy risico's verbonden aan veranderingen in de entiteit (structuur en strategie) en aan wettelijke vereisten, worden voldoende in overweging genomen.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

3.2.2 Proces 2: Informeren

Beheersingsdoelstelling J: Privacyverklaring De entiteit informeert betrokkenen op transparante wijze over het beleid, de voorwaarden en activiteiten met betrekking tot het verzamelen, gebruiken, bewaren, verstrekken en verwijderen van persoonsgegevens.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

3.2.3 Proces 3: Keuze en Toestemming

Beheersingsdoelstelling K: Toestemmingsraamwerk De entiteit verkrijgt indien vereist of noodzakelijk toestemming van de betrokkene om persoonsgegevens te verwerken.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

3.2.4 Proces 4: Verzamelen

Beheersingsdoelstelling L: Minimale gegevensverwerking De persoonsgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de gerechtvaardigde doeleinden waarvoor zij worden verwerkt.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

3.2.5 Proces 5: Gebruiken, opslaan en verwijderen

Beheersingsdoelstelling M: Doelbinding Persoonsgegevens worden niet verstrekt, beschikbaar gesteld of anderszins voor andere doeleinden gebruikt dan die zijn geformuleerd in de privacyverklaring van de entiteit, tenzij: a) de betrokkene toestemming verleent; b) of dit wettelijk vereist is.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling N: Privacy architectuur (Gegevens-bescherming door ontwerp en door standaard-instellingen) De entiteit neemt bij het ontwikkelen en wijzigen van producten, diensten, bedrijfssystemen of processen het privacy beleid, de privacy principes en/of de van toepassing zijnde wet- en regelgeving in acht.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling O: Bewaren van gegevens Persoonsgegevens worden niet langer bewaard dan noodzakelijk, dan wettelijk is toegestaan of dan noodzakelijk is voor de doeleinden waarvoor zij werden verzameld.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling P: Verwijdering, vernietiging en anonimiseren Persoonsgegevens worden indien nodig geanonimiseerd en/of verwijderd binnen de entiteit. De identiteit van personen kan niet worden herleid en persoonsgegevens zijn niet meer beschikbaar nadat de bewaartermijn is verstreken.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling Q: Gebruik en beperking Persoonsgegevens worden niet verwerkt als de betrokkene een beperking van de verwerking heeft verkregen of wanneer er sprake is van specifieke juridische restricties door lokale autoriteiten. Bezwaren van de betrokkene tegen de verwerking van persoonsgegevens worden op een adequate wijze afgehandeld.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

3.2.6 Proces 6: Inzage en kwaliteit van gegevens

Beheersingsdoelstelling R: Verzoeken om inzage Een inzageverzoek van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen nagaan welke persoonsgegevens van hen worden verwerkt en op welke manier.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling S: Verzoek tot rectificatie Een rectificatieverzoek van de betrokkene wordt op de juiste wijze afgehandeld. Betrokkenen kunnen bepalen of hun persoonsgegevens juist/up to-date en zo nodig geactualiseerd zijn en zij kunnen deze (laten) corrigeren.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling T: Verzoek tot wissen Een verzoek tot het wissen van persoonsgegevens van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen bepalen welke persoonsgegevens zij willen laten wissen, mits aan de geldende criteria wordt voldaan.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling U: Verzoek tot overdracht Een verzoek tot overdracht van persoonsgegevens van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen hun persoonsgegevens laten overdragen aan een andere entiteit, mits aan de geldende criteria wordt voldaan.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling V: Juistheid en volledigheid van gegevens Vastgelegde procedures voor het valideren, aanpassen en bijwerken van persoonsgegevens waarborgen de juistheid en volledigheid van persoonsgegevens.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

3.2.7 Proces 7: Verstrekken

Beheersingsdoelstelling W: Verstrekking aan derden en registratie Persoonsgegevens worden niet aan derden verstrekt zonder wettelijke basis of voor andere doeleinden dan waarover de betrokkene is geïnformeerd.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling X: Overeenkomsten met derden Bij de verwerving van oplossingen en diensten (gerelateerd aan persoonsgegevens) van derden wordt voldoende aandacht besteed aan privacyoverwegingen en -vereisten, waardoor geborgd wordt op de juiste wijze met persoonsgegevens wordt omgegaan en deze worden beschermd.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling Y: Doorgifte van persoonsgegevens Persoonsgegevens worden niet doorgegeven (d.w.z. verplaatst, weergegeven of geprint op een andere locatie) aan landen die geen toereikend rechtskader ten aanzien van privacy hebben.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

3.2.8 Proces 8: Gegevensbeveiliging

Beheersingsdoelstelling Z: Programma informatiebeveiliging Persoonsgegevens worden adequaat beschermd tegen onopzettelijke fouten of verlies, of kwaadwillige handelingen zoals hacken, diefstal, ongeautoriseerde verstrekking of verlies.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling AA: Identiteit en toegangsbeheer Toegangsrechten worden adequaat toegekend, gewijzigd en ingetrokken. Dit verkleint de kans op ongeautoriseerde toegang tot en onjuiste verwerking van persoonsgegevens, of inbreuk in verband met persoonsgegevens door interne medewerkers, derden of hackers.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling AB: Veilige gegevensoverdracht Door beperkte toegang tot persoonsgegevens tijdens verzending wordt op adequate wijze ongeautoriseerde verstrekking, inbreuk, wijziging of verwijdering van persoonsgegevens voorkomen.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling AC: Versleuteling en eindpuntbeveiliging Inbreuk in verband met persoonsgegevens/datalek (onopzettelijk verlies of kwaadwillige handelingen zoals diefstal, ongeautoriseerde verstrekking of verlies) wordt voorkomen door middel van versleuteling.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling AD: Registreren van toegang Toegang of toegangspogingen tot persoonsgegevens door medewerkers en derden worden geregistreerd en onderzocht om (pogingen tot) inbreuk op de beveiliging van persoonsgegevens te detecteren en te voorkomen.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

3.2.9 Proces 9: Monitoren en Handhaven

Beheersingsdoelstelling AE: Beoordeling van compliance met privacywetgeving Adequaat toezicht op de interne organisatie en derden waarborgt dat de entiteit voldoet aan de wet- en regelgeving met betrekking tot privacy en vermindert het risico op inbreuk in verband met persoonsgegevens of verlies hiervan.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			

Beheersingsdoelstelling AF: Periodiek monitoren van privacy-beheersingsmaatregelen Systematische en periodieke evaluatie van privacy processen en beheersingsmaatregelen waarborgt dat deze naar behoren werken, zodat blijvend wordt voldaan aan de van toepassing zijnde wet- en regelgeving.			
1			
Ref.	**Beheersingsmaatregelen**	**Testwerkzaamheden**	**Test resultaten**
1.1			