<Klantnaam>

SOC 3® RAPPORT

Rapportage over <object> relevant voor <van toepassing zijnde criteria>

<start verslagperiode> tot en met <einde verslagperiode>

MANAGEMENTBEWERING VAN <KLANTNAAM>

Wij zijn verantwoordelijk voor het opzetten, implementeren, en het effectief laten werken van interne beheersingsmaatregelen met betrekking tot <object> gedurende de periode <start verslagperiode> tot en met <einde verslagperiode>, om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereistenrelevant voor beveiliging, beschikbaarheid, verwerking van integriteit, vertrouwelijkheid en privacy werden bereikt. Onze beschrijving van de grenzen van <object> is opgenomen in bijlage A en identificeert de aspecten van het <object>die onderdeel zijn van onze bewering.

Wij hebben een evaluatie uitgevoerd van de effectieve werking van de interne beheersingsmaatregelen met betrekking tot <object> gedurende de periode <start verslagperiode> tot en met <einde verslagperiode>, om een redelijke mate van zekerheid te verschaffen dat onze serviceverplichtingen en systeemvereistenwerden bereikt. Deze evaluatie is uitgevoerd op basis van op de trust services criteria relevant voor beveiliging, beschikbaarheid, verwerking van integriteit, vertrouwelijkheid en privacy (de van toepassing zijnde 'trust services criteria'), zoals uiteengezet in TSP Sectie 100, 'Trust Services Criteria voor beveiliging, beschikbaarheid, verwerking van integriteit, vertrouwelijkheid en privacy', van het Amerikaanse Instituut van Public Accountants (AICPA) en voor Privacy ook op basis van de privacy-beheersingsdoelstellingen afkomstig uit het Privacy Control Framework versie 2.0 van NOREA. De doelstellingen van <klantnaam> voor <object> bij het toepassen van de van toepassing zijnde trust services criteria zijn opgenomen in de serviceverplichtingen en systeemvereistenvan <klantnaam. De belangrijkste serviceverplichtingen en systeemvereistengerelateerd aan de van toepassing zijnde trust services criteria zijn opgenomen in bijlage B.

Er bestaan inherente beperkingen aan ieder systeem van interne beheersing, waaronder de mogelijkheid tot menselijke fouten en het omzeilen van interne beheersingsmaatregelen. Vanwege deze inherente beperkingen kan een service organisatie redelijke, maar geen absolute zekerheid verschaffen dat de serviceverplichtingen en systeemvereistenworden bereikt.

<Klantnaam> maakt gebruik van sub-serviceorganisatie(s) <subservice organisatie(s)> om <beschrijving diensten>. De beschrijving van de grenzen van <object> (bijlage A van dit rapport) stelt dat bepaalde criteria alleen bereikt kunnen worden indien de beheersingsmaatregelen bij de sub-serviceorganisatie juist zijn opgezet en effectief werken. De beschrijving van de grenzen van <object> geeft ook de aanvullende beheersingsmaatregelen van de subservice organisatie weer die zijn verondersteld bij de opzet van de interne beheersingsmaatregelen van <klantnaam>. De beschrijving van de grenzen van <object> geeft niet de feitelijke interne beheersingsmaatregelen bij de subservice organisatie weer.

De beschrijving van de grenzen van <object> (bijlage A van dit rapport) stelt dat bepaalde criteria alleen bereikt kunnen worden indien de beheersingsmaatregelen bij de gebruikersorganisatie juist zijn opgezet en effectief werken. De beschrijving van de grenzen van <object> geeft ook de aanvullende beheersingsmaatregelen van de gebruikersorganisatie weer die zijn verondersteld bij de opzet van de interne beheersingsmaatregelen van <klantnaam>.

Onze beweringen zijn gevormd op basis van de aangelegenheden die hiervoor zijn uiteengezet.

- Wij beweren dat de interne beheeringsmaatregelen met betrekking tot <object> effectief hebben gewerkt gedurende de periode <start verslagperiode> tot en met <einde verslagperiode>, om een redelijke mate van zekerheid te verschaffen dat de services commitments en system

requirements van <klantnaam> werden bereikt gebaseerd op de van toepassing zijnde trust services criteria.

- Wij beweren tevens dat de interne beheersingsmaatregelen met betrekking tot de Privacy categorie afdoende zijn opgezet, bestaan en effectief zijn uitgevoerd om de privacy-beheersingsdoelstellingen afkomstig uit het Privacy Control Framework versie 2.0 van NOREA[1] te bereiken.

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

Bijlage A – <Klantnaam>'s beschrijving van de grenzen van <object>

De beschrijving van de grenzen van het object betreft een ingekorte versie van de beschrijving uit het SOC 2® rapport. Deze beschrijving dient ten minste de hieronder genoemde onderdelen te bevatten:

- *Geleverde diensten en Scope van de service / afbakening van het systeem / sub-serviceorganisaties*
- *Systeemoverzicht inclusief de paragrafen:*
  - *Infrastructuur*
  - *Software*
  - *Mensen*
  - *Data*
  - *Processen en procedures*
- *Interne beheersingsmaatregelen (inclusief de paragrafen controle-omgeving, risk assessment, controle activiteiten, informatie & communicatie, monitoring activiteiten).*
- *Complementary User Entity Controls*
- *Complementary Subservice Organization Controls*

Bijlage B – Belangrijkste serviceverplichtingen en systeemvereistenservices

Bijlage B geeft een overzicht van de belangrijkste serviceverplichtingen en systeemvereistenservices. Deze kunnen bijvoorbeeld gebaseerd zijn op verantwoordelijkheden die zijn opgenomen in interne beleidsstukken en procedures, Service Level Agreements of op basis van relevante wet- en regelgeving. In het geval van Privacy Audit Proof zal hier ook een toelichting opgenomen worden met betrekking tot de serviceverplichtingen en systeemvereistenservices aangaande de verwerking van persoonsgegevens in het object van onderzoek.

ASSURANCE-RAPPORT VAN DE ONAFHANKELIJKE AUDITOR

Aan: het management van <klantnaam>.

<Introductie>

Reikwijdte

Wij hebben de management bewering van <klantnaam> getiteld "Managementbewering van <klantnaam>" onderzocht. Management van <klantnaam>" beweert hierin dat de interne beheersingsmaatregelen met betrekking tot <object> effectief hebben gewerkt gedurende de periode <start verslagperiode> tot en met <einde verslagperiode>, om een redelijke mate van zekerheid te verschaffen dat de service commitments en system requirements van <klantnaam> werden bereikt. Die evaluatie van het management is uitgevoerd op basis van, de trust services criteria relevant voor beveiliging, beschikbaarheid, verwerking van integriteit, vertrouwelijkheid en privacy (van toepassing zijnde trust services criteria) zoals uiteengezet in TSP sectie 100, 'Trust Services Criteria voor beveiliging, beschikbaarheid, integriteit van verwerking, vertrouwelijkheid en privacy' van het American Institute of Public Accountants (AICPA), en voor Privacy ook op basis van de privacy-beheersingsdoelstellingen afkomstig uit het Privacy Control Framework versie 2.0 van NOREA.

Sub-serviceorganisaties

<Klantnaam> maakt gebruik van sub-serviceorganisatie(s) <subservice organisatie(s)> om <beschrijving diensten>. De beschrijving van de grenzen van <object> (bijlage A van dit rapport) stelt dat bepaalde criteria alleen bereikt kunnen worden indien de beheersingsmaatregelen bij de sub-serviceorganisatie juist zijn opgezet en effectief werken. De beschrijving van de grenzen van <object> geeft ook de aanvullende beheersingsmaatregelen van de subservice organisatie weer die zijn verondersteld bij de opzet van de interne beheersingsmaatregelen van <klantnaam>. De beschrijving van de grenzen van <object> geeft niet de feitelijke interne beheersingsmaatregelen bij de subservice organisatie weer. Onze opdracht bevat geen toetsing van de dienstverlening en de interne beheersingsmaatregelen van de sub-serviceorganisatie.

Beheersingsmaatregelen bij de gebruikersorganisatie (Complementary User Entity Controls)

De beschrijving van de grenzen van <object> (bijlage A van dit rapport) stelt dat bepaalde criteria alleen bereikt kunnen worden indien de beheersingsmaatregelen bij de gebruikersorganisatie juist zijn opgezet en effectief werken. De beschrijving van de grenzen van <object> geeft ook de aanvullende beheersingsmaatregelen van de gebruikersorganisatie weer die zijn verondersteld bij de opzet van de interne beheersingsmaatregelen van <klantnaam>. Wij hebben de opzet of effectieve werking van deze beheersingsmaatregelen bij de gebruikersorganisatie niet geëvalueerd.

Verantwoordelijkheden van de serviceorganisatie

<Klantnaam> is verantwoordelijk voor haar serviceverplichtingen en systeemvereisten, en voor het opzetten, het implementeren en het effectief laten werken van interne beheersingsmaatregelen in het systeem om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten van <klantnaam> werden bereikt. <Klantnaam> heeft tevens de bijgaande bewering gedaan met betrekking tot de effectieve werking van interne beheersingsmaatregelen met betrekking tot <object>. In het opstellen van deze bewering is <klantnaam> verantwoordelijk voor het selecteren en identificeren van de relevante trust services criteria in haar vermelding, en voor het hebben van een redelijke onderbouwing voor het doen van de bewering door het uitvoeren van

een beoordeling van de effectiviteit van de interne beheersingsmaatregelen met betrekking tot <object>.

Verantwoordelijkheden van de service auditor

Onze verantwoordelijkheid is het verschaffen van een oordeel, gebaseerd op ons onderzoek, of de beweringen van het management dat interne beheersingsmaatregelen met betrekking tot <object> effectief werkten gedurende de periode om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten van de service organisatie werden bereikt gebaseerd op de van toepassing zijnde trust services criteria en het Privacy Control Framework, getrouw is weergegeven.

Wij hebben onze assurance-opdracht uitgevoerd conform Nederlandse wetgeving en NOREA Richtlijn Assurance-opdrachten door IT-Auditors (3000A). Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid voor ons oordeel.

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

De auditeenheid past het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhoudt het een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en procedures voor de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.

Naar onze mening hebben we voldoende assurance-informatie verkregen om te komen tot een oordeel met een redelijke mate van zekerheid.

Ons onderzoek omvatte onder andere:

- Het verkrijgen van inzicht in het <object> en de serviceverplichtingen en systeemvereisten van de service organisatie.
- Het maken van een inschatting van de risico's dat interne beheersingsmaatregelen niet effectief werkten om de serviceverplichtingen en systeemvereisten van <klantnaam> te bereiken, gebaseerd op de van toepassing zijnde trust services criteria.
- Het uitvoeren van procedures om assurance-informatie te verkrijgen over de vraag of interne beheersingsmaatregelen met betrekking tot <object> effectief werkten om de s serviceverplichtingen en systeemvereisten van <klantnaam> te bereiken, gebaseerd op de van toepassing zijnde trust services criteria.

Ons onderzoek omvatte ook het uitvoeren van overige procedures die wij noodzakelijk achtten op basis van de omstandigheden.

Inherente beperkingen

De beschrijving van de grenzen van <object> van <klantnaam> is opgesteld voor de algemene informatiebehoefte van een brede groep gebruikers en hun auditors. De beschrijving van de grenzen van <object> dekt daarom niet alle aspecten af die een individuele gebruiker belangrijk acht. Vanwege hun aard en inherente beperkingen is het mogelijk dat interne beheersingsmaatregelen niet altijd effectief werkten om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten van <klantnaam> werden bereikt gebaseerd op de van toepassing zijnde trust services criteria. Bovendien is de projectie van de conclusies omtrent de effectieve werking van interne beheersingsmaatregelen naar toekomstige periodes onderhevig aan

het risico dat <object> wordt gewijzigd of dat interne beheersingsmaatregelen bij een serviceorganisatie inadequaat worden of tekortschieten.

Ons oordeel

Ons oordeel is gebaseerd op de aangelegenheden die in dit assurance-rapport zijn uiteengezet. Naar ons oordeel zijn de beweringen van het management, waarin is vermeld dat de interne beheersingsmaatregelen met betrekking tot <object> effectief werkten gedurende de periode <start verslagperiode> tot en met <einde verslagperiode> om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten van <klantnaam> werden bereikt gebaseerd op de van toepassing zijnde trust services criteria en het Privacy Control Framework, in alle materiële opzichten, getrouw weergegeven.

<plaats>, <datum rapportage>

<organisatie>

Namens deze,

<naam>

<functie>