<Klantnaam>

PRIVACY ASSURANCE-RAPPORTAGE VERWERKING PERSOONSGEGEVENS IN <OBJECT>

Over periode van<start verslagperiode>

tot en met <einde verslagperiode>

<Datum rapportage>

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 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 en effectief werkten gedurende de verslagperiode van <start verslagperiode> tot en met <einde verslagperiode>. 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.

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

<plaats tekenen klant>, [datum rapportage]

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

ASSURANCE-RAPPORT VAN DE ONAFHANKELIJKE IT-AUDITOR

Aan: de directie van <klantnaam>.

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

Ons oordeel

Naar ons oordeel, in alle van materieel belang zijnde aspecten:

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 basis voor ons oordeel

Wij hebben onze opdracht uitgevoerd overeenkomstig Richtlijn 3000A 'Attest-opdrachten', vastgesteld door de Nederlandse Orde van Register EDP-auditors (NOREA). 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.

Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

<optionele nadere duiding van reikwijdte>

Ons oordeel is niet aangepast als gevolg van deze aangelegenheden.

Beperkingen van interne beheersingsmaatregelen

Het bereiken van de privacy-beheersingsdoelstellingen uit het Privacy Control Framework van NOREA 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.

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>. Tevens kan <klantnaam> dit rapport gebruiken voor het verkrijgen van het logo Privacy Audit Proof van NOREA, waarbij dit rapport bestemd is voor het maatschappelijk verkeer ter onderbouwing hiervan.

Verantwoordelijkheden van het bestuur van <klantnaam>

Het bestuur van<klantnaam> is verantwoordelijk voor:

a) het opstellen van bijgaande 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.

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>.

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>