**KPMG Advisory N.V.**
Postbus 74500
1070 DB Amsterdam

Laan van Langerhuize 1
1186 DS Amstelveen
Telefoon (020) 656 7890
www.kpmg.nl

Liander N.V.
De heer M.J.W. Kempkes
Postbus 50
6920 AB DUIVEN

Onze ref. A1700010367 RA
KML/LdB/jmh
Contact Léon de Beer
(06-46748568)

Amstelveen, 11 december 2017

**Betreft:** Assurancerapport inzake Privacy “verwerking van persoonsgegeves uit de slimme meter ten behoeve van wettelijke taken (Richtlijn 3000A/Richtlijn 3600n)”

Geachte heer Kempkes,

Liander heeft de afgelopen jaren intensief gewerkt aan het inrichten en beheersen van de verwerking van gegevens uit de slimme meterketen. Deze werkzaamheden hebben geresulteerd in het behalen van het Privacy-Audit-Proof keurmerk dat aantoont dat Liander N.V. voor de verwerking van persoonsgegevens voldoet aan de van toepassing zijnde wettelijke vereisten op basis van de Wet bescherming persoonsgegevens en nader gespecificeerde relevante wet- en regelgeving.

Wij hebben de privacy-audit uitgevoerd conform onze opdrachtbrief d.d. 24 april jl. (kenmerk: A1700010367 KML/LdB/jmh).

## *Doelstelling en reikwijdte van de privacy-audit*

De doelstelling van deze privacy-audit is het uitvoeren van een onderzoek naar de opzet, het bestaan en de effectieve werking van het stelsel van maatregelen rondom de verwerking van persoonsgegevens over de periode 1 oktober 2016 tot en met 30 september 2017. Hierbij gaat het om de verwerking van persoonsgegevens die verband houden met het uitlezen, gebruiken en doorgeven van gegevens uit de slimme meters van Liander ten behoeve van de wettelijke taken.

### *Verantwoordelijkheden*

De leiding van Liander is verantwoordelijk voor de opzet en voortdurend goede werking van het genoemde stelsel gericht op de bescherming van persoonsgegevens in overeenstemming met het normenkader.

Het is onze verantwoordelijkheid om op basis van onze werkzaamheden een assurancerapport, inclusief onze conclusie met betrekking tot dit stelsel, te verstrekken.

### *Doelgroep*

Het assurancerapport is bestemd voor het maatschappelijk verkeer. De afzonderlijke rapportage van bevindingen is bestemd voor intern Liander-gebruik en mag alleen met expliciete toestemming van KPMG en Liander worden verspreid aan derden.

### *Object van onderzoek*

Het object van het onderzoek betreft de verwerkingen van persoonsgegevens die verband houden met het:

— uitlezen;

— gebruiken en

— doorgeven.

van gegevens uit de slimme meter voor kleinverbruik, om invulling te geven aan de wettelijke taken van netbeheer die vallen onder de AP-melding 1511611.

Onderstaande onderwerpen vallen niet in de scope van ons onderzoek:

— verwerkingen die samenhangen met het verwerken van persoonsgegevens uit conventionele meters;

— verwerkingen welke Liander uitvoert onder AP-meldingnummer 1511621 'Verwerking van persoonsgegevens uit de slimme meter t.b.v. overige activiteiten';

— overige verwerkingen van persoonsgegevens die niet gerelateerd zijn aan de slimme meter.

### *Criteria*

De opdracht is uitgevoerd in overeenstemming met Nederlands recht, waaronder Richtlijn 3000A 'Assurance-opdrachten door IT-Auditors'.

Tevens is gebruikgemaakt van de richtlijn voor privacy-audits (Richtlijn 3600n) van NBA/NOREA. Conform artikel 12 van Richtlijn 3600n zijn de volgende criteria toegepast:

— Wet bescherming persoonsgegevens, de wet van 6 juli 2000, Staatsblad 302, houdende regels inzake de bescherming van persoonsgegevens, inclusief alle onderliggende besluiten en regelingen, waaronder de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp, de wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens, Staatsblad 230, en het inwerkingstredingsbesluit, staatsblad 281.

— Richtsnoeren beveiliging persoonsgegevens van 2013. Deze zijn in 2013 in de plaats gekomen van Achtergrondstudies en Verkenning nummer 23, "Beveiliging van persoonsgegevens", CBP 2001.

— Raamwerk Privacy Audit, uitgegeven door het samenwerkingsverband Audit Aanpak, 2001 (hoofdstuk V).

— Contouren voor Compliance, Handreiking bij het Raamwerk Privacy Audit, CBP 2005. (hoofdstuk 3, V1 t/m V9, E1 en E2).

— De formeel van toepassing zijnde sectorale wetgeving, andere wetgeving, gedragscodes jurisprudentie en publieke afspraken, te weten:

- Elektriciteits- en gaswet 1998.
- Privacy en Security Sectoreisen versie 2.0, opgesteld door de Beleidscommissie Privacy & Security.
- Meetcode Elektriciteit, opgesteld door NMa, 16 april 2013, artikelen 1.6.1., 2.3.4, 3.1.1, 3.1.2, 3.1.4 en 4.5, voor zover van toepassing op de datacommunicatie en het opslaggedeelte van de slimme meter en niet op het metereologische gedeelte van de meter.
- Besluit op afstand uitleesbare meetinrichtingen, 10 maart 2014.
- Regeling gegevensbeheer en afdracht elektriciteit en gas, 14 juni 2011.
- Gedragscode "Verwerking van Persoonsgegevens door Netbeheerders in het kader van Installatie en Beheer van Slimme Meters bij Kleinverbruikers", Netbeheer Nederland, 19 mei 2012.

### *Mate van zekerheid*

Volgens de beroepsvoorschriften mogen er twee soorten assurance-opdrachten worden uitgevoerd: een assurance-opdracht tot het verkrijgen van een redelijke mate van zekerheid en een assurance-opdracht tot het verkrijgen van een beperkte mate van zekerheid.

Ons onderzoek heeft tot doel ten behoeve van belanghebbenden met een redelijke mate van zekerheid een oordeel te geven of het door Liander ingerichte stelsel van maatregelen en de procedures, gericht op de bescherming van persoonsgegevens, bij de verwerking voldoet aan de eisen zoals opgenomen in het normenkader. Dit betreft een onderzoek naar opzet, bestaan en werking van de ingerichte maatregelen en procedures en omvatte die werkzaamheden die wij nodig achtten voor het signaleren van materiële afwijkingen en het verkrijgen van een deugdelijke grondslag voor het afgeven van ons oordeel met een redelijke mate van zekerheid.

### *Werkzaamheden*

Wij hebben ons onderzoek verricht in overeenstemming met het Nederlands recht, waaronder Richtlijn 3000A 'Richtlijn 3000A 'Assurance-opdrachten door IT-Auditors' en de Richtlijn Privacy Audits (richtlijn 3600n "Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens"). Dit heeft vereist dat wij ons onderzoek zodanig hebben uitgevoerd dat een redelijke mate van zekerheid is verkregen dat opzet, bestaan en werking van het stelsel van maatregelen en procedures gericht op de bescherming van persoonsgegevens geen afwijkingen van materieel belang bevatten, ten opzichte van de van toepassing zijnde criteria.

In het kader van ons onderzoek zijn als belangrijkste werkzaamheden uitgevoerd:

1. Het verkrijgen van inzicht in de kenmerken van de organisatie en de branche waarin deze opereert inclusief relevante maatschappelijke issues en wet- en regelgeving.
2. Het onderkennen van risico's in de externe omgeving en de organisatie zelf, en onderzoeken in hoeverre deze risico's qua opzet en implementatie worden afgedekt door het onderzochte stelsel.
3. Het onderzoeken van het stelsel in opzet, bestaan en werking op basis van een uitgevoerde risicoanalyse. Bij het selecteren van testmethoden is rekening gehouden met de aard van de beheersingsmaatregel, de controledoelstelling en de effectiviteit en efficiëntie van de beheersingsmaatregelen. De volgende testtechnieken zijn gebruikt bij de beoordeling van de werking van de maatregelen:
   - Waarneming ter plaatse: waarnemingen ter plaatse bestaan uit het volgen van de handelingen van anderen bij een proces of procedure om de inrichting en het bestaan van de opgenomen beheersmaatregelen vast te stellen.
   - Inlichtingen inwinnen: het inwinnen van inlichtingen bestaat uit het opvragen van gegevens bij personen die over feitenkennis beschikken om de inrichting en het bestaan van een beheersingsmaatregel vast te stellen.
   - Inspectie/verificatie: verificatie bestaat uit het onderzoeken van interne en externe documenten om de inrichting, het bestaan en de werking van de opgenomen beheersingsmaatregelen vast te stellen.
4. Het wegen van de geconstateerde afwijkingen in relatie tot de eisen zoals opgenomen in het normenkader.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een deugdelijke onderbouwing voor ons oordeel te bieden.

## *Oordeel*

Op grond van onze werkzaamheden zijn wij van oordeel dat in alle van materieel belang zijnde opzichten:

— de opzet van de beheersingsmaatregelen toereikend is om de in het normenkader beschreven risico´s en eisen af te dekken, indien de beschreven beheersingsmaatregelen adequaat worden nageleefd;

— de beschreven beheersingsmaatregelen bestaan per 30 september 2017;

— de beschreven beheersingsmaatregelen gedurende de periode 1 oktober 2016 tot en met 30 september 2017 effectief zijn geweest.

## *Inherente beperkingen*

Ons onderzoek was gericht op het geven van een oordeel met een redelijke, maar geen absolute, mate van zekerheid over de opzet, het bestaan en de werking van het stelsel van maatregelen en de procedures van de aangegeven verwerking. Het door ons uitgevoerde onderzoek brengt, naar zijn aard, inherente beperkingen met zich mee. Dit heeft tot gevolg dat 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, niet altijd (kunnen) worden geconstateerd.

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.

Hoewel het bij de beoordeling gehanteerde normenkader door de AP in samenwerking met marktpartijen is opgesteld, mag een positief oordeel van de privacy-auditor niet worden uitgelegd als een positief oordeel van de AP.

Hoogachtend,
KPMG Advisory N.V.

ir. K.M. Lof RE

partner