

Stichting Bureau Kredietregistratie (BKR)

Teisterbantlaan 2a  
4006 EB TIEL

## Assurancerapport met betrekking tot de bescherming van persoonsgegevens

Geachte heer Van den Bosch,

### Opdracht en object van onderzoek

Ingevolge uw opdracht hebben wij (Ernst & Young Accountants LLP) de opzet en het bestaan van het stelsel van interne maatregelen en procedures gericht op de bescherming van de verwerking van persoonsgegevens met behulp van het Centraal Krediet Informatiesysteem onderzocht. Tevens hebben wij onderzoek uitgevoerd naar de werking van genoemd stelsel over het jaar 2015. De rapportage van de Stichting Bureau Kredietregistratie (BKR) daaromtrent in de Privacyparagraaf van het jaarverslag is onderdeel van het object van onderzoek. De betreffende verwerking is gemeld bij de Autoriteit Persoonsgegevens onder meldingsnummer 1016265.

### Verantwoordelijkheden

De leiding van BKR is verantwoordelijk voor de opzet en voortdurend goede werking van het genoemde stelsel gericht op de bescherming van de persoonlijke levenssfeer van de geregistreerden, zoals bedoeld in de Wet bescherming persoonsgegevens en de mede daartoe opgestelde interne richtlijnen en reglementen. De leiding van BKR is tevens verantwoordelijk voor de inhoud van de Privacyparagraaf. Het is onze verantwoordelijkheid om op basis van gedegen werkzaamheden een assurancerapport inclusief onze conclusie met betrekking tot dit stelsel en de in de jaarrekening opgenomen Privacyparagraaf te verstrekken.

### Doelstelling van het onderzoek

Doel van het onderzoek is te komen tot een uitspraak in hoeverre dit stelsel:

- In opzet voldoet aan de gestelde normen;
- Bij voortduring in stand blijft op het, gezien de Wet bescherming persoonsgegevens en de binnen BKR bestaande regelgeving, minimaal noodzakelijk geachte niveau;
- In het kader van de naleving van deze regelgeving stelselmatig en bij voortduring voldoende heeft gewerkt in 2016.

Het onderzoek is gericht op het verkrijgen van een redelijke mate van zekerheid.

## Verrichte werkzaamheden en gehanteerde criteria

Het onderzoek is uitgevoerd in overeenstemming met de door het Nederlandse Beroepsgroep voor Accountants (NBA) en de Nederlandse Orde van Register EDP auditors (NOREA) uitgegeven richtlijn voor Privacy Audits (3600N). In het bijzonder hebben wij bij de uitvoering van onze werkzaamheden gebruik gemaakt van de volgende normen en criteria (gezamenlijk verder aangeduid als normenkader):

- De Wet bescherming persoonsgegevens, de wet van 6 juli 2000, Staatsblad 302, houdende regels inzake de bescherming van persoonsgegevens, inclusief alle onderliggende besluiten en regelingen geldend tot en met 31 december 2016 waaronder de meldplicht datalekken;
- Richtsnoeren beveiliging van persoonsgegevens als opvolger van de in de standaard benoemde Achtergrondstudies & Verkenningen 23 "Beveiliging van persoonsgegevens";
- Richtlijn 3600N inclusief het in 2017 uitgegeven Addendum Privacy Audit, waarin onder andere wordt verwezen naar de "Contouren voor Compliance", "Raamwerk Privacy Audit" en "Handreiking bij het Raamwerk Privacy Audit";
- De door BKR opgestelde interne richtlijnen en reglementen met betrekking tot privacybescherming;
- De formeel van toepassing zijnde sectorale wetgeving, andere wetgeving, gedragscodes, jurisprudentie en publieke afspraken voor zover het betrekking heeft op de verwerking van persoonsgegevens.

## Werkzaamheden

Hiertoe hebben wij:

- Kennisgenomen van de interne analyses van het hiervoor genoemde normenkader in verhouding tot het bij BKR getroffen stelsel van maatregelen en procedures;
- De opzet onderzocht van interne, in het bijzonder de administratieve, organisatie inclusief automatisering van BKR. Dit met name ter zake van de daarin besloten maatregelen van interne beheersing;
- De stelselmatig goede werking van deze beheersingsmaatregelen getoetst;
- Waar nodig overige werkzaamheden uitgevoerd, waaronder mede te rekenen eigen acties, die wij in het kader van ons onderzoek noodzakelijk achtten;
- In opdracht van het dagelijks bestuur aanvullende werkzaamheden uitgevoerd.

Bij ons onderzoek is mede gebruikgemaakt van de werkzaamheden van de binnen BKR bestaande afdeling Audit & Riskmanagement. Wij zijn van mening dat de door ons verkregen informatie voldoende en geschikt is als basis voor onze conclusie.

## Conclusie

Op grond van ons onderzoek concluderen wij dat de opzet en het bestaan van het binnen BKR bestaande stelsel van maatregelen en procedures gericht op de bescherming van de verwerking van persoonsgegevens met behulp van het Centraal Krediet Informatiesysteem naar de stand van 31 december 2016 heeft voldaan aan het normenkader en dat dit stelsel gedurende 2016 als zodanig heeft gewerkt.

### Toelichting op het oordeel

Het door ons uitgevoerde onderzoek brengt, naar zijn aard, inherente beperkingen met zich mee. Dit heeft tot gevolg dat incidenten, ondanks een effectieve uitvoering van ons onderzoek, niet altijd (kunnen) worden ontdekt. Bovendien heeft ons onderzoek niet betrekking op toekomstige perioden, omdat het stelsel van maatregelen en procedures onderhevig kan zijn aan gewijzigde omstandigheden of verandering van naleving in gedragslijnen en/of procedures.

Amsterdam, 26 april 2017

Ernst & Young Accountants LLP  
Namens deze,

w.g.

drs. S.J. Hartjes RE RA  
Partner