Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1299

Vragen van het lid **Kuiken** (PvdA) aan de Minister voor Rechtsbescherming over *gestolen data van Übergebruikers* (ingezonden 15 december 2017).

Antwoord van Minister **Dekker** (Rechtsbescherming) (ontvangen 28 februari 2018). Zie ook Aanhangsel Handelingen, vergaderjaar 2017–2018, nr. 840.

Vraag 1
Kent u het bericht «Data 174.000 Nederlandse Ubergebruikers gestolen»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat een bedrijf datalekken bij de Autoriteit Persoonsgegevens moet melden en in het geval het persoonsgegevens betreft ook de getroffen personen daarvan op de hoogte moet stellen? Zo nee, waarom klopt dat niet?

Antwoord 2
Ja, het klopt dat een bedrijf datalekken onmiddellijk moet melden aan de Autoriteit persoonsgegevens als dit leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Dit staat in artikel 34a, eerste lid, van de Wet bescherming persoonsgegevens. De verantwoordelijke voor de verwerking van persoonsgegevens, in dit geval het bedrijf Über, is verplicht de persoonsgegevens die worden verwerkt te beveiligen tegen verlies en onrechtmatige verwerking. Deze verplichting is opgenomen in artikel 13 van de Wet bescherming persoonsgegevens. Een inbreuk op de beveiliging die een ernstig datalek tot gevolg heeft, moet worden gemeld aan de Autoriteit persoonsgegevens.
Een datalek heeft per definitie betrekking op persoonsgegevens. De verantwoordelijke moet ook de getroffen personen onverwijld inlichten als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor hun persoonlijke levenssfeer. Dit zal in ieder geval aan de orde zijn als het persoonsgegevens van gevoelige aard betreft, bijvoorbeeld medische of strafrechtelijke gegevens. De meldplicht aan betrokken personen staat in artikel 34a, tweede

[1] https://www.parool.nl/amsterdam/data-174-000-nederlandse-ubergebruikers-gestolen~a4545073/

ah-tk-20172018-1299
ISSN 0921 - 7398
's-Gravenhage 2018

lid, van de Wet bescherming persoonsgegevens. Volgens het zesde lid van dit artikel geldt de meldplicht aan betrokkenen niet in het geval dat de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de betreffende persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van die gegevens. Door de wettelijke meldplicht wordt dus veiliggesteld dat de Autoriteit persoonsgegevens en getroffen personen in kennis worden gesteld van ernstige datalekken. Volledigheidshalve wijs ik erop dat de meldplicht voor datalekken ook zal gelden na de inwerkingtreding van de Algemene Verordening Gegevensbescherming op 25 mei 2018.
Zoals uw Kamer bekend is, heeft de Autoriteit persoonsgegevens op haar website aangegeven op 22 november 2017 een datalekmelding van Über te hebben ontvangen. De melding wordt op dit moment onderzocht.

Vraag 3
In hoeverre is het aan een bedrijf zelf om vast te stellen of er sprake is van een datalek dat bij de Autoriteit Persoonsgegevens moet worden gemeld?

Antwoord 3
De wettelijke meldplicht inzake datalekken richt zich tot de verantwoordelijke voor de verwerking van persoonsgegevens. De verantwoordelijke is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1, onderdeel d, van de Wet bescherming persoonsgegevens). Een bedrijf dat persoonsgegevens verwerkt, dient dus zelf vast te stellen of er sprake is van een datalek dat bij de Autoriteit persoonsgegevens moet worden gemeld.

Vraag 4
Hoe kan worden voorkomen dat een bedrijf vanwege bedrijfsbelangen datalekken niet meldt?

Antwoord 4
De wettelijke verplichting tot het melden van ernstige datalekken, zoals beschreven onder antwoord 2), geldt onverkort voor alle bedrijven en organisaties die persoonsgegevens verwerken. Zij zijn derhalve verplicht melding te doen van ernstige datalekken.
Het is de taak van de Autoriteit persoonsgegevens toezicht te houden op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens. De Autoriteit persoonsgegevens is bevoegd om onderzoek te doen naar mogelijke overtredingen van de wet. Dit is geregeld in artikel 60 van de Wet bescherming persoonsgegevens. In het geval de Autoriteit persoonsgegevens van oordeel is dat er sprake is van overtreding van de wet, is zij bevoegd om handhavend op te treden. De Autoriteit persoonsgegevens kan een last onder bestuursdwang opleggen die gericht is op het beëindigen van de overtreding. De Autoriteit persoonsgegevens is ook bevoegd een bestuurlijke boete op te leggen, waaraan in bepaalde gevallen een bindende aanwijzing vooraf kan gaan.
Dit handhavingsinstrumentarium is neergelegd in de artikelen 65 en 66 van de Wet bescherming persoonsgegevens.

Vraag 5
Deelt u de mening dat een bedrijf waarvan persoonsgegevens van klanten gestolen worden, ter wille van de bescherming van hun klanten, melding zou moeten maken, zelfs al zouden zij daartoe volgens wet- of regelgeving niet toe verplicht zijn? Zo ja, waarom? Zo nee, waarom niet?

Antwoord 5
De Wet bescherming persoonsgegevens, en straks de Algemene Verordening Gegevensbescherming en de bijbehorende uitvoeringswetgeving, biedt een hoog beschermingsniveau ter zake van de verwerking van persoonsgegevens en het beschermen van individuen tegen de onrechtmatige verwerking van hun gegevens.
Zoals vermeld in het antwoord op vraag 2), moet de verantwoordelijke ernstige datalekken die waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van betrokkenen, melden aan de Autoriteit persoonsgegevens en aan getroffen personen.

Mocht een bedrijf een ernstig datalek niet melden aan getroffen personen, voorziet de Wet bescherming persoonsgegevens (artikel 34a, zevende lid) in een mogelijkheid voor de Autoriteit persoonsgegevens om – indien zij van oordeel is dat het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van betrokkenen zal hebben – van het bedrijf te verlangen dat het getroffenen alsnog in kennis stelt van het datalek. Getroffen personen dienen in beginsel op individuele basis te worden geïnformeerd over het datalek en wat zij kunnen doen om de negatieve gevolgen van het datalek te beperken, zoals het wijzigen van gebruikersnamen en wachtwoorden. Daarnaast kan er aanvullend een algemene voorlichting worden gegeven, bijvoorbeeld op de website van het bedrijf.
De wettelijke regeling over het melden van datalekken aan getroffen personen waarbij hun persoonlijke levenssfeer in negatieve zin kan worden beïnvloed, zorgt ervoor dat betrokkenen zo snel mogelijk en zo volledig mogelijk worden geïnformeerd.

Vraag 6
Kunt u de Kamer op de hoogte stellen van de uitkomst van het onderzoek van de Autoriteit Persoonsgegevens naar Über?

Antwoord 6
Gelet op de onafhankelijke positie van de Autoriteit persoonsgegevens rapporteert zij uit eigen beweging over de uitkomsten van haar onderzoek. De Autoriteit persoonsgegevens maakt de definitieve bevindingen, met uitzondering van bevindingen in het kader van een boeteonderzoek, na vaststelling daarvan openbaar. De handelwijze over de openbaarmaking van de uitkomst van onderzoeken, is terug te vinden in de Beleidsregels openbaarmaking Autoriteit persoonsgegevens die zijn gepubliceerd op haar website.