AH 706
2026Z18649

Antwoord van staatssecretaris Van Bruggen (Justitie en Veiligheid), mede namens de staatssecretaris van Economische Zaken en Klimaat (ontvangen 20 november 2026)

Zie ook Aanhangsel Handelingen, vergaderjaar 2026-2027, nr. 330

Vraag 1
Bent u bekend met het bericht: ‘Smart-tv's van LG bespioneren gebruikers via microfoon’? 1)

Antwoord op vraag 1

Ja.

Vraag 2
Hoe reageert u op dit bericht en het onderliggende onderzoek van Gamers Nexus, Level1Techs en andere professionals?

Antwoord op vraag 2

Volgens berichtgeving en het onderliggende onderzoek van onder andere Gamers Nexus en Level1Techs inventariseren bepaalde LG-smart-tv’s actief het lokale netwerk (apparaten en wifi-informatie) en maken zij gebruik van *automated content recognition* (ACR) om te registreren welke audio- en videoinhoud wordt bekeken; ook worden kwetsbaarheden gemeld, waaronder mogelijk misbruik van de microfoon en remote code execution.[1] Deze bevindingen roepen vragen op over de waarborging van privacy en gegevensbescherming.[2]

Zoals toegelicht bij het antwoord op vraag 4, wordt de bescherming van gegevens en privacy onder meer geregeld in de Algemene verordening gegevensbescherming (AVG) en de e-privacyrichtlijn. Het toezicht op de naleving berust bij de onafhankelijke toezichthouders; in Nederland de Autoriteit Persoonsgegevens (AP) en, waar het de hier relevante e-privacyregels in de Telecommunicatiewet betreft, de Autoriteit Consument & Markt (ACM).

[1] Vgl. LG-smart-tv's lijken gebruikers af te luisteren en netwerken te scannen - Tweakers
[2] LG stelt daartegenover dat spraakgegevens uitsluitend na toestemming worden verwerkt en alleen wanneer de spraakknop wordt ingedrukt of na een ‘wake word’ bij geactiveerde far-field-herkenning, en dat tv’s buiten die gevallen geen omgevingsgeluid opnemen. Tevens geeft LG aan dat scannen/verbinden op het lokale netwerk en ACR op opt-in-basis plaatsvinden en, zonder instemming, niet voor advertentiedoeleinden worden gebruikt. LG ontkent dat televisies gebruikers afluisteren - Tweakers

Vraag 3
Deelt u de mening dat consumenten er redelijkerwijs van uit moeten kunnen gaan dat zij niet afgeluisterd worden door huishoudapparatuur?

Antwoord op vraag 3

Ja. Zoals hieronder uiteengezet in het antwoord op vraag 4, bepaalt de Telecommunicatiewet in samenhang met de AVG dat voor het registreren van gesprekken in beginsel toestemming van betrokkene is vereist.

Vraag 4
Welke wet- en regelgeving beschermt consumenten tegen dit soort spionage door smart-apparaten? Hoe wordt dit in Nederland gehandhaafd?

Antwoord op vraag 4

Bij het auditief registreren van gesprekken via huishoudapparatuur in verband met het gebruik van spraakassistenten zoals in een smart-tv, gelden de gegevensbeschermingsregels uit de AVG en de Telecommunicatiewet. Deze vereisten worden nader toegelicht in de richtsnoeren inzake virtuele spraakassistenten van het Europees Comité voor Gegevensbescherming (EDPB).[3] Een belangrijk vereiste om misbruik te voorkomen, is het vereiste van toestemming voor het gebruik van spraakassistenten. Opslaan van of toegang tot informatie in eindapparatuur (zoals het maken van een geluidsopname via een smart-tv) is in beginsel alleen toegestaan met toestemming van de gebruiker in overeenstemming met de AVG, na duidelijke informatie over alle verwerkingsdoelen.[4] Tevens is voor de (verdere) verwerkingen van persoonsgegevens steeds een verwerkingsgrondslag vereist zoals bedoeld in artikel 6 AVG. Zo zal in voorkomende gevallen bijvoorbeeld na toestemming voor het registreren van de gegevens via de tv, ook specifieke toestemming zijn vereist voor het verwerken van persoonsgegevens voor het doel van gepersonaliseerd adverteren. Waar spraakassistenten *bijzondere* persoonsgegevens verwerken, geldt een verwerkingsverbod, waar alleen onder specifieke voorwaarden zoals *uitdrukkelijke* toestemming van de betrokkene van kan worden afgeweken (zie ook het antwoord op vraag 7).

Een andere essentiële vereiste uit de AVG is de verplichting voor de verwerkingsverantwoordelijke om een passende beveiliging te waarborgen. Zoals uiteengezet in de richtsnoeren van de EDPB, is het voor een veilige verwerking

[3] Richtsnoeren 02/2021 inzake virtuele spraakassistenten. Versie 2.0. Vastgesteld op 7 juli 2021
[4] Behoudens uitzonderingen zoals opgenomen in artikel 11.7a van de Telecommunicatiewet, waaronder de verwerking van gegevens met als uitsluitend doel de communicatie over een elektronisch communicatienetwerk uit te voeren, of die strikt noodzakelijk is om de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren

van persoonsgegeven noodzakelijk dat de spraakassistent de vertrouwelijkheid, de integriteit en beschikbaarheid ervan dient te kunnen waarborgen.

De Richtlijn voor Radioapparatuur (RED) bevat essentiële eisen die betrekking hebben op de cybersecurity van radioapparatuur, die sinds 1 augustus 2025 van toepassing zijn. Een van de vereisten daarin is datradioapparatuur beveiligingen moet bevatten om de bescherming van de persoonsgegevens en de privacy van de gebruiker en de abonnee te waarborgen. De Verordening cyberweerbaarheid (Cyber Resillience Act, CRA) schrijft verder voor dat digitale producten die vanaf 11 december 2027 op de interne markt worden gebracht moeten voldoen aan essentiële cybersecurity-eisen. Onder deze eisen valt ook dat de integriteit van opgeslagen, verzonden of anderszins verwerkte gegevens wordt beschermd, en dat er uitsluitend persoonsgegevens worden verwerkt die noodzakelijk zijn voor het beoogde doel van het product (dataminimalisatie).

De toezichthouders zien toe op de naleving van deze wetgeving. De AP ziet toe op naleving van de AVG, en ACM ziet toe op de naleving van artikel 11.7a van de Telecommunicatiewet. Vanwege de samenhang tussen beide wetten, zijn wanneer persoonsgegevens worden verwerkt beide toezichthouders in de praktijk bevoegd om te handhaven.[5] De AP en de ACM hebben daarvoor ook een samenwerkingsprotocol. De Rijksinspectiedienst Digitale Infrastructuur (RDI) houdt toezicht op de handhaving van de RED en de CRA. Bij niet-naleving kunnen er sancties worden opgelegd, zoals boetes. Ook kunnen producten van de markt worden geweerd door de markttoezichthouder.

Tot slot zijn er bepalingen (art. 139a-b en f en 441b) in het wetboek van Strafrecht die het heimelijk en wederrechtelijk maken van opnamen of afbeeldingen strafbaar stellen, ook in niet-publiek toegankelijke plaatsen.

Vraag 5
Wat zijn de gevolgen voor consumenten als hun privégesprekken heimelijk worden afgeluisterd, opgeslagen en doorverkocht? Welke risico’s draagt dit met zich mee?

Antwoord op vraag 5

De risico’s voor de rechten en vrijheden van natuurlijke personen in verband met het recht op gegevensbescherming kunnen, afhankelijk van het type en de ernst van het incident, qua zwaarte en waarschijnlijkheid sterk uiteenlopen. In algemene zin gelden de risico’s die in de AVG worden genoemd voor de rechten en vrijheden van natuurlijke personen, zoals discriminatie en identiteitsfraude, financiële verliezen of reputatieschade.[6]

[5] Vgl. Advies 5/2019 over de wisselwerking tussen de e privacyrichtlijn en de algemene verordening gegevensbescherming, met name wat betreft de taken en bevoegdheden van gegevensbeschermingsautoriteiten Vastgesteld op 12 maart 2019

[6] overweging 75 AVG, artikel 4 lid 12.

Vraag 6
Kunt u specifiek ingaan op de rechtmatigheid van de dataverzameling door LG, waarbij gesprekken woord voor woord worden opgeslagen, ook zonder internetverbinding, en worden doorgestuurd naar commerciële partijen?

Antwoord op vraag 6

Het woordelijk opslaan van gesprekken met of zonder internetverbinding, evenals het doorsturen van gegevens naar commerciële partijen kan zijn toegestaan als aan de daarvoor geldende voorwaarden uit het wettelijk kader is voldaan (zie ook het antwoord op vraag 4). Het houden van toezicht op en het handhaven van de rechtmatigheid van gegevensverwerkingen in individuele zaken in de private sector is geen taak van het kabinet, maar van de toezichthouder. Deze is onafhankelijk en heeft een ruim mandaat en uitgebreide bevoegdheden om te onderzoeken of partijen voldoen aan hun verplichtingen uit de AVG, de Telecommunicatiewet, de RED en de CRA.

Vraag 7
Wanneer is er sprake van expliciete toestemming voor dataverzameling door smart-apparaten zoals bedoeld onder de Algemene Verordening Gegevensbescherming?

Antwoord op vraag 7

De term “expliciete” toestemming als zodanig wordt niet letterlijk genoemd in de Nederlandse vertaling van de AVG.[7] Wel geldt de eis van “uitdrukkelijke” toestemming voor de verwerking van bijzondere categorieën persoonsgegevens in het kader van de uitzondering op het verbod om bijzondere categorieën persoonsgegeven te verwerken. Het gaat dan om bijzonder gevoelige gegevens met betrekking tot ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid (artikel 9, eerste lid, AVG). De voorwaarden die worden gesteld aan rechtsgeldige toestemming in de zin van de AVG, zijn door de EDPB verder uitgewerkt in Richtsnoeren (05/2020) inzake toestemming overeenkomstig Verordening 2016/679. Kort gezegd, bepalen deze richtsnoeren dat toestemming vrijelijk, specifiek, geïnformeerd, en ondubbelzinnig dient te zijn gegeven. Indien aan deze voorwaarden niet is voldaan, wordt niet voldaan aan de vereisten die gelden voor toestemming. Blijkens deze richtsnoeren verwijst de term uitdrukkelijk naar de manier waarop toestemming door de betrokkene tot uitdrukking wordt gebracht. Een voor de hand liggende manier om ervoor te zorgen dat toestemming uitdrukkelijk is, is

[7] Vgl. de Engelse en Nederlandse vertaling van artikel 9, tweede lid, sub a, AVG op: https://gdpr-text.com/nl/read/article-9/.

het uitdrukkelijk bevestigen van toestemming in een verklaring van de gebruiker.[8]

Vraag 8
Deelt u de analyse dat consumenten te vaak bewust worden misleid door fabrikanten over de mate en wijze van dataverzameling door hun producten, waardoor geen sprake is van expliciete toestemming? Erkent u dat de fabrikanten hier een economisch belang bij hebben?

Antwoord op vraag 8

Het is essentieel voor de bescherming van het grondrecht dat bedrijven, conform de wettelijke vereisten, transparant zijn over welke gegevens ze verzamelen en hoe ze die gebruiken. Dat persoonsgegevens economische waarde kunnen hebben, maakt dit niet anders. Niet voor niets vereist de AVG dat toestemming vrijelijk, specifiek, geïnformeerd, en ondubbelzinnig dient te zijn verleend. De AP ziet daar als toezichthouder op de AVG in Nederland op toe.

[8] Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, hoofdstuk 4.

Vraag 9
Waren u en de relevante toezichthouders op de hoogte van het afluisteren door deze LG smart-tv's in het bijzonder?

Antwoord op vraag 9

De AP heeft desgevraagd aangegeven niet bekend te zijn met een klacht of melding van dergelijke aard. Wel heeft de AP, in EDPB-verband, vorig jaar een onderzoek uitgevoerd naar smart tv's en datastromen. Het rapport '*Verkennend onderzoek smart tv's'* geconcludeerd dat er omvangrijke datastromen plaatsvinden waar consumenten zich vaak niet van bewust zijn.[9] Het betreft een complex ecosysteem met gegevensstromen naar onder meer de fabrikant, het besturingssysteem (bijv. webOS, Google TV), third-party (streaming) apps, advertentienetwerken en partijen die kijkgedrag verzamelen. Voor consumenten zijn deze datastromen, volgens de AP, in hoge mate ondoorzichtig.

Vraag 10
Hoe worden apparaten gecontroleerd op afluistermogelijkheden voordat ze op de Nederlandse en Europese markt komen?

Antwoord op vraag 10

Volgens de AVG en de Telecomwet is de verwerkingsverantwoordelijke verantwoordelijk voor naleving van de vereisten in de AVG en de Telecomwet en dient hij deze ook te kunnen aantonen. Zo dient de verwerkingsverantwoordelijke op grond van artikel 25 van de AVG (privacy door ontwerp en standaard instellingen) voor aanvang van een voorgenomen gegevensverwerking voor de verwerkingsmiddelen als de verwerking passende technische en organisatorische maatregelen te nemen om de privacy van betrokkenen te beschermen. Bij het bepalen van deze maatregelen dient rekening te worden gehouden met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden. De AVG benoemt daarbij nadrukkelijk dat beginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uitgevoerd dienen te worden en de nodige waarborgen in de verwerking ingebouwd ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen. Deze verplichting biedt een belangrijke waarborg om een inbreuk in verband met het grondrecht, zoals bij misbruik of verlies van persoonsgegevens, bijvoorbeeld door afluistermogelijkheden, te voorkomen. De AP ziet, als toezichthouder op de AVG, toe op de naleving van artikel 25 AVG.

In aanvulling daarop, houdt de RDI toezicht op radioapparatuur en of deze onder andere voldoen aan de cybersecurity-eisen van de RED, waaronder of de radioapparatuur beveiligingen bevat om de bescherming van de

[9] https://autoriteitpersoonsgegevens.nl/documenten/rapport-verkennend-onderzoek-smart-tvs

persoonsgegevens en de privacy van de gebruiker en de abonnee te waarborgen. De RDI gaat toezicht houden op digitale producten en of deze voldoen aan de eisen van de CRA, waaronder dataminimalisatie. RDI kan apparaten technisch onderzoeken, bijvoorbeeld in een laboratorium. Toezicht op digitale producten onder de RED en CRA vindt plaats nadat producten op de markt gebracht zijn.

Vraag 11
Welke mechanismen heeft u, al dan niet de Europese Commissie, om producten die consumenten afluisteren van de markt te weren? Bent u bereid te onderzoeken of dat voor de LG smart-tv's een optie is?

Antwoord op vraag 11

Indien de in het antwoord op vraag 4 genoemde eisen van de RED en de CRA niet worden nageleefd kan de RDI maatregelen nemen. Dit kunnen bestraffende maatregelen zijn zoals een boete, maar dit kunnen ook reparerende maatregelen zijn, zoals de verplichting om een terugroepactie uit te voeren of een verkoopverbod. Ook kan de RDI de fabrikant gelasten om het product uit de handel te nemen. Als de betrokken partij niet mee wil werken, dan volgen in bepaalde gevallen maatregelen zoals een last onder dwangsom. Deze maatregelen worden gedeeld met collega-markttoezichthouders binnen de Europese Unie, waardoor de werking van de maatregel voor geheel de Unie kan gelden.

Vraag 12
Wat is het standpunt van het kabinet over de groeiende datahonger van bedrijven die producten maken die steeds meer met elkaar communiceren, gesprekken afluisteren, en privé-informatie doorverkopen aan derden?

Antwoord op vraag 12

De AVG staat de verwerking van persoonsgegevens toe als wordt voldaan aan de daarvoor geldende wettelijke vereisten. Elke verwerking moet rechtmatig, behoorlijk en transparant zijn. Het beginsel van dataminimalisatie betekent bijvoorbeeld dat alleen persoonsgegevens mogen worden verwerkt die strikt noodzakelijk zijn voor een vooraf bepaald doel. Een passende beveiliging betekent dat de verwerking dient te worden beveiligd op een wijze die past bij het risico van een verwerking voor het grondrecht. Daarnaast geldt, zoals toegelicht bij het antwoord op vraag 10, het beginsel van gegevensbescherming door ontwerp en standaard instellingen. De verwerkingsverantwoordelijke is verantwoordelijk voor naleving van de AVG en dient die naleving te kunnen aantonen. Of, en zo ja, in hoeverre in specifieke gevallen aan de AVG wordt voldaan bij apparaten die met elkaar communiceren, gesprekken registreren en gegevens doorgeven aan derden, kan per geval verschillen. De AP ziet als onafhankelijke toezichthouder toe op naleving van de AVG.

Vraag 13
Wat bent u bereid te doen om deze trend te keren en de privacy van consumenten beter te beschermen?

Antwoord op vraag 13

Zoals hierboven reeds uiteengezet, biedt het wettelijke kader in de AVG en e-privacyrichtlijn brede bescherming van de gegevensbescherming en privacy-grondrechten van consumenten.[10] Implementatie van de RED en de CRA dragen bij aan een betere bescherming van persoonsgegevens die worden opgeslagen, verzonden of anderszins verwerkt door digitale producten.

Vraag 14
Kunt u deze vragen afzonderlijk en binnen de gestelde termijn beantwoorden?

Antwoord op vraag 14

De vragen zijn afzonderlijk beantwoord. Helaas is het vanwege benodigde afstemming niet mogelijk gebleken om binnen de termijn voor beantwoording te zorgen.

1) 'Smart-tv's van LG bespioneren gebruikers via microfoon' RTL Z, 9 september 2026.

[10] EUR-Lex - 52024DC0357 - EN - EUR-Lex