Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

> Retouradres Postbus 1671 3800BR Amersfoort

AANTEKENEN met ontvangstbevestiging
KPN BV
T.a.v. 5.1.2.e
Postbus 25110
3001 HC ROTTERDAM

Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (033) 460 08 00
F (033) 460 08 50
www.agentschaptelecom.nl

Contactpersoon
5.1.2.e
T (050) 587 7444

Ons kenmerk
AT-EZK/5.1.2.e

Uw kenmerk
-

Bijlagen
Inspectierapport

Datum 24 november 2022
Betreft Inspectie privacy

Geachte 5.1.2.e,

Agentschap Telecom, als onderdeel van het Ministerie van Economische Zaken en Klimaat, is toezichthouder op de Telecommunicatiewet (Tw) waaronder het toezicht op het verwerken van verkeers- en locatiegegevens door aanbieders van openbare elektronische communicatienetwerken en -diensten zoals bedoeld in Hoofdstuk 11 (Privacy) van de Tw.

In dit kader heeft Agentschap Telecom een inspectie uitgevoerd naar de verwerking van verkeersgegevens, waaronder locatiegegevens, door KPN B.V. (hierna KPN). Aanleiding voor deze inspectie waren diverse signalen waarbij melding werd gemaakt van het verwerken van verkeersgegevens door aanbieders van mobiele elektronische communicatienetwerken ten behoeve van mobiliteitsinformatie. Doel van de inspectie was om te onderzoeken in hoeverre KPN verkeersgegevens verwerkt of heeft verwerkt ten behoeve van mobiliteitsinformatie.

De inspectie bestond uit een deskresearch en een locatiebezoek op 17 oktober 2022. De resultaten van de inspectie vindt u in het inspectierapport dat als bijlage bij deze brief is toegevoegd.

De conclusie is dat op basis van de geleverde informatie door KPN en het nadere onderzoek er geen aanwijzingen zijn gevonden dat KPN verkeersgegevens verwerkt of heeft verwerkt ten behoeve van mobiliteitsinformatie.

Hoogachtend,
De Minister van Economische Zaken en Klimaat,
namens deze,

5.1.2.e

Hoofd Veiligheid afdeling Toezicht
Agentschap Telecom

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

INSPECTIE KPN

Hoofdafdeling Toezicht

Piet Mondriaanlaan 54
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44

Behandeld door
5.1.2.e

rapport

ID-nummer : 5.1.2.e
Rapporteur : 5.1.2.e
Rapport bestemd voor : KPN / Intern AT

Algemene gegevens betrokkene

Naam aanbieder : KPN B.V.
Straatnaam en nummer : Wilhelminakade 123
Postcode : 3072AP
Vestigingsplaats : Rotterdam

KvK : 27124701

Relatienummer AT : 5.1.2.e

1 Inleiding

Agentschap Telecom (hierna: AT) houdt toezicht op de naleving van het bepaalde bij of krachtens de Telecommunicatiewet (hierna: Tw). Dat toezicht ziet onder meer op de naleving van bepalingen die betrekking hebben op de bescherming van persoonsgegevens en de persoonlijke levenssfeer. In het bijzonder richt dit toezicht zich op het verwerken van verkeers- en locatiegegevens[1].

De e-Privacyrichtlijn, geïmplementeerd in de Tw, strekt tot eerbiediging van de grondrechten en beginselen die tot uitdrukking zijn gebracht in met name het Handvest van de grondrechten van de Europese Unie zoals het recht op eerbiediging van zijn privéleven, gezinsleven, woning en zijn communicatie. Verkeers- en locatiegegevens kunnen diepgaand inzicht bieden in het privéleven, gezinsleven, woning en communicatie van een persoon. Gebruikers van mobiele openbare elektronische communicatienetwerken en diensten veronderstellen daarom waarborgen van het vertrouwelijk karakter van de communicatie en de daarmee verband houdende verkeers- en locatiegegevens.

[1] Artikel 11.5 jo. artikel 15.1, lid 1, onder i., van de Tw

Het verwerken van verkeers- en locatiegegevens door aanbieders van openbare elektronische communicatienetwerken en -diensten is om deze reden wettelijk beperkt tot een aantal doelen: het overbrengen van de communicatie, de facturatie en een aantal toegestane eigen bedrijfsdoeleinden. Verwerking van verkeers- en locatiegegevens voor andere doelen dan voorgeschreven in de wet[2] is niet toegestaan om het vertrouwelijke karakter te kunnen waarborgen.

1.1 Aanleiding

AT heeft op 17 oktober 2022 een inspectie uitgevoerd bij KPN B.V. (hierna: KPN), aanbieder van openbare elektronische communicatienetwerken en -diensten (hierna: aanbieder) onder de Tw. Aanleiding voor deze inspectie waren diverse signalen waarbij melding werd gemaakt van het verwerken van verkeersgegevens door aanbieders van mobiele elektronische communicatienetwerken ten behoeve van mobiliteitsinformatie.

Deze inspectie had uitsluitend tot doel inzicht te krijgen of KPN verkeers- en locatiegegevens verwerkt ten behoeve van mobiliteitsinformatie en, indien dit het geval is, deze te toetsen aan de toegestane verwerkingen op basis van artikel 11.5 van de Tw. Locatiegegevens, niet zijnde verkeersgegevens, zoals bedoeld in artikel 11.5a vallen niet onder deze inspectie.

2 Toetsingskader

2.1 Waarborg vertrouwelijk karakter bij verwerking verkeers- en locatiegegevens

Het nationale wettelijk kader voor verwerken van verkeersgegevens is gebaseerd op het Europese kader van de e-Privacyrichtlijn[3]. Deze richtlijn strekt tot eerbiediging van de grondrechten en beginselen die tot uitdrukking zijn gebracht in met name het Handvest van de grondrechten van de Europese Unie zoals het recht op eerbiediging van zijn privéleven, gezinsleven, woning en zijn communicatie. Verkeers- en locatiegegevens kunnen diepgaand inzicht bieden in het privéleven, gezinsleven, woning en communicatie van een persoon. Het verwerken van verkeers- en locatiegegevens is om deze reden wettelijk beperkt tot een aantal doelen die nodig zijn door aanbieders voor het overbrengen van de communicatie, de facturering en een aantal bedrijfsdoeleinden.

Deze regels zijn vastgelegd in artikel 11.5 van de Tw[4]. Dit artikel luidt als volgt:

> 1. *De aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst verwijderen dan*

[2] Verwerking is eveneens toegestaan op basis artikel 11.2a en 11.13 Tw
[3] Richtlijn 2002/58/EG
[4] Dit artikel implementeert artikel 6 van de e-Privacyrichtlijn.

wel anonimiseren de door hen verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees of gebruikers, zodra deze verkeersgegevens niet langer nodig zijn ten behoeve van de overbrenging van communicatie, onverminderd het tweede, derde en vijfde lid.

2. *De aanbieder mag verkeersgegevens verwerken die noodzakelijk zijn voor facturering, waaronder het opstellen van een factuur voor een abonnee of voor degene die zich tegenover de aanbieder rechtens verbonden heeft die factuur te voldoen, dan wel ten behoeve van een betaling van verleende toegang. De verkeersgegevens mogen worden verwerkt tot het einde van de wettelijke termijn waarbinnen de factuur in rechte kan worden betwist of de betaling in rechte kan worden afgedwongen.*
3. *De aanbieder van elektronische communicatiediensten mag voorts de in het eerste lid bedoelde verkeersgegevens verwerken, voor zover en voor zolang dat noodzakelijk is voor:*
    a. *marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten, of*
    b. *de levering van diensten met toegevoegde waarde, mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor voorafgaand aan de verwerking zijn toestemming heeft gegeven. De abonnee of gebruiker kan de gegeven toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.*
4. *De aanbieder stelt de abonnee of gebruiker in kennis van de soorten verkeersgegevens die worden verwerkt voor de in het tweede en derde lid bedoelde doeleinden alsmede omtrent de duur van de verwerking. Voor zover het de verwerking van verkeersgegevens ten behoeve van de doeleinden, bedoeld in het derde lid betreft, wordt de desbetreffende informatie verstrekt voorafgaand aan het verkrijgen van de in dat lid bedoelde toestemming van de abonnee of gebruiker.*
5. *De verwerking van verkeersgegevens in overeenstemming met het eerste tot en met vierde lid mag alleen geschieden door personen die werkzaam zijn onder het gezag van de aanbieder voor facturering, verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude alsmede marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten of de levering van diensten met toegevoegde waarde en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren.*
6. *De aanbieder mag de verkeersgegevens verstrekken aan personen en instanties die zijn belast met de berechting van enig geschil dan wel de beslissing van een geschil als bedoeld in de artikelen 12.1, 12.2 voor zover van toepassing, of 12.9.*

2.2 Toezicht en handhaving

Artikel 15.1 eerste lid, onder g, van de Tw luidt:

> *1. Met het toezicht op de naleving van het bepaalde bij of krachtens deze wet en de eidas-verordening zijn belast de bij besluit van Onze Minister aangewezen ambtenaren, voor zover het betreft de bepalingen die betrekking hebben op:*
> *(…)*
> *g. het gebruik van verkeersgegevens en locatiegegevens als geregeld in artikel 11.5, artikel 11.5a onderscheidenlijk artikel 11.13;*

Artikel 2, eerste lid van het Besluit aanwijzing toezichthouders Telecommunicatiewet luidt:

> *Met het toezicht op de naleving van de bepalingen, bedoeld in artikel 15.1, eerste lid, van de wet, zijn, voor zover het de bevoegdheden betreft van de Minister van Economische Zaken, belast de ambtenaren met de functiebenamingen inspecteur, senior inspecteur, coördinerend/specialistisch inspecteur en inspecteur/medewerker toezicht van de afdeling Toezicht van Agentschap Telecom van het ministerie van Economische Zaken.*

Artikel 15.4, eerste lid, van de Tw luidt:

> *"Onze Minister kan ingeval van overtreding van een wettelijk voorschrift met het toezicht op de naleving waarvan hij ingevolge artikel 15.1 eerste lid, is belast of ingeval van overtreding van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht een bestuurlijke boete opleggen van ten hoogste € 900.000."*

Uit deze bepalingen volgt de toezichthoudende taak van de toezichthouders, alsmede de bevoegdheid om in geval van overtreding van artikel 11.5 van de Tw handhavend op te treden door oplegging van een bestuurlijke boete.

2.3 Begripsbepalingen

2.3.1 Verkeers- en locatiegegevens

In artikel 11.1, aanhef en onder b. van de Tw, worden verkeersgegevens als volgt gedefinieerd:

> *"verkeersgegevens: gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan;"*

Verkeersgegevens zijn de gegevens die worden verwerkt voor het overbrengen van communicatie over een telecommunicatienetwerk of voor de facturering ervan. Deze definitie is een rechtstreekse omzetting van art. 2 onderdeel b van de e-Privacyrichtlijn. Waar het gaat om spraaktelefonie heeft het begrip onder

andere betrekking op het oproepende en opgeroepen nummer, begin en einde van de oproep, duur van de oproep en (waar het mobiele telefonie betreft) ook op locatiegegevens. Waar het gaat om internetverkeer heeft het begrip betrekking op gegevens als de identiteit van de aansluiting, gebruikersnaam ('user id'), IP-adressen, e-mailadres, het gebruikte protocol, begin- en eindtijd sessie, type dienst, volume (kilobytes)[5].

Artikel 11.1, aanhef en onder d. van de Tw, definieert het begrip locatiegegevens:

> *Locatiegegevens: gegevens die in een elektronische communicatienetwerk of door een elektronische communicatiedienst worden verwerkt, waarmee de geografische positie van de eindapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven*

Bij locatiegegevens kan worden gedacht aan gegevens betreffende de breedte-, hoogte- en lengtegraad waarmee de locatie van het mobiele toestel wordt weergegeven, gegevens betreffende de reisrichting, de nauwkeurigheidsgraad van de locatiegegevens, de identificatie van de netwerkcel (Cell ID) waarbinnen het mobiel eindapparaat[6] zich op een bepaald tijdstip bevindt en het tijdstip waarop de locatiegegevens zijn opgeslagen[7]. In dit onderzoek wordt met mobiel eindapparaat bedoeld een eindapparaat dat geschikt is om gebruik te maken van het telecommunicatienetwerk en voorzien is van een SIM-kaart[8].

Locatiegegevens kunnen verkeersgegevens zijn als deze gegevens ook vallen onder de definitie van verkeersgegevens van art. 11.1 onderdeel b, van de Tw. Een voorbeeld van locatiegegevens, die tevens als verkeersgegevens worden aangemerkt, zijn gegevens die in het kader van mobiele telefonie worden verwerkt betreffende de basisstations waar het mobiele toestel van de gebruiker contact mee heeft (Cell ID's) en welke noodzakelijk zijn voor het overbrengen van communicatie tussen de oproepende en opgeroepen gebruiker[9].

2.3.2 Abonnees of gebruikers

In artikel 1.1 van de Tw wordt een abonnee gedefinieerd als:

> *"natuurlijke persoon of rechtspersoon die partij is bij een overeenkomst met een aanbieder van openbare elektronische communicatiediensten voor de levering van dergelijke diensten;"*

In artikel 11.1, aanhef en onder a van de Tw, wordt het begrip 'gebruiker' gedefinieerd als:

> *"een natuurlijke persoon die gebruik maakt van een openbare elektronische communicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd;"*

---

[5] Kamerstukken II 2002/03, 28851, 3, p. 151
[6] Besluit eindapparaten, artikel 1, onder a.i.
[7] Vergelijk overweging 14 van de e-Privacyrichtlijn
[8] Met uitzondering van machine to machine (M2M)
[9] Kamerstukken II 2003/03, 28851, 3, p. 47 en 152

Anders dan de abonnee staat de gebruiker dus niet noodzakelijk in een contractuele verhouding tot de aanbieder van de dienst. De definitie van 'gebruiker' is een rechtstreekse omzetting van art. 2, onderdeel a, e-Privacyrichtlijn.

Uit het feit dat in artikel 11.5 van de Tw wordt gesproken over 'gebruikers of abonnees', volgt dat de verwerking van verkeersgegevens ook strekt tot bescherming van rechtspersonen als abonnee. Zie in dit verband ook overweging 12 uit de e-Privacyrichtlijn:

> *(12) De abonnees van een openbare elektronische-communicatiedienst kunnen zowel natuurlijke als rechtspersonen zijn. Deze richtlijn, die een aanvulling vormt op Richtlijn 95/46/EG, beoogt de fundamentele rechten van natuurlijke personen, en in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, en de rechtmatige belangen van rechtspersonen te beschermen.*

2.3.3 Verwerking van verkeersgegevens

In artikel 11.1, aanhef en onder c. van de Tw, wordt het begrip 'verwerking van verkeersgegevens' gedefinieerd:

> *"verwerking van verkeersgegevens: verwerking als bedoeld in artikel 4, onderdeel 2, van de Algemene verordening gegevensbescherming, met dien verstande dat de desbetreffende handelingen mede betrekking hebben op verkeersgegevens van abonnees die geen natuurlijke personen zijn".*

Artikel 4, onderdeel 2 van de Algemene Verordening Gegevensbescherming (AVG) definieert het begrip 'verwerking':

> *"een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens."*

Een handeling met persoonsgegevens kwalificeert al snel als verwerking. Immers enkel het 'raadplegen' of 'ter beschikking stellen' van verkeersgegevens vormt al een verwerking. Voorts blijkt uit de definitie dat verwerking van verkeersgegevens niet alleen ziet op natuurlijke personen, maar ook op rechtspersonen.

Voor de goede orde wordt nog opgemerkt dat de AVG sinds 25 mei 2018 van toepassing is. De AVG is de opvolger van de Wet bescherming persoonsgegevens (Wbp). De Wbp strekte ter implementatie van de 'Privacyrichtlijn'[10]. Met inwerkingtreding van de AVG is de Privacyrichtlijn ingetrokken en de Wbp vervallen. Artikel 1, aanhef en onder b van de Wbp luidde:

[10] Richtlijn 95/46 EG

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

b. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

Onder de Wbp werd gesproken over 'bewerken' van persoonsgegevens. Onder de AVG is dat vervangen door 'verwerken' van persoonsgegevens. Materieel is er geen verschil.

2.3.4 Anonimiseren

Voor het voldoen aan artikel 11.5, eerste lid van de Tw, is het begrip 'anonimiseren' van belang. In de memorie van toelichting[11] wordt dit begrip als volgt toegelicht:

> *"Onder anonimiseren wordt hier verstaan, dat de betreffende gegevens volledig en op onomkeerbare wijze worden ontdaan van hun persoonsidentificerende kenmerken."*

De hoofdregel uit het eerste lid van artikel 11.5 van de Tw is kort gezegd dat verkeersgegevens die niet langer nodig zijn voor het doel van de transmissie van communicatie moeten worden verwijderd of geanonimiseerd. Zie ook de memorie van toelichting:

> *In artikel 11.5, eerste lid, wordt in navolging van artikel 6, eerste lid, van richtlijn nr. 2002/58/EG als hoofdregel bepaald dat de aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst de door hen verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees en gebruikers verwijderen dan wel anonimiseren zodra deze gegevens niet langer nodig zijn ten behoeve van de overbrenging van communicatie onverminderd hetgeen in het tweede, derde en vijfde lid is bepaald. Het niet geanonimiseerd gebruiken van die verkeersgegevens is – naast het gebruik ten behoeve van de levering van de elektronische communicatiedienst – toegestaan voor factureringsdoeleinden (nader uitgewerkt in artikel 11.5, tweede lid) en onder nadere voorwaarden voor marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten of de levering van diensten met toegevoegde waarde (artikel 11.5, derde lid).*

Deze hoofdregel gold reeds vóór implementatie van de e-Privacyrichtlijn. Zie in dit verband eveneens de memorie van toelichting:

> *"8.2 de verwerking van verkeersgegevens*
> *In richtlijn nr. 97/66/EG is als hoofdregel neergelegd dat de aanbieder van een openbaar telecommunicatienetwerk en de aanbieder van een openbare telecommunicatiedienst na beëindiging van iedere oproep de verwerkte*

[11] Kamerstukken II 2002/03, 28851, nr. 3, p. 154

> *verkeersgegevens met betrekking tot de abonnee of gebruiker dienen te verwijderen dan wel te anonimiseren. Verwerking van deze gegevens in niet geanonimiseerde vorm is – buiten de situatie van levering van de communicatiedienst – slechts toegestaan voor factureringsdoeleinden of, zij het met instemming van de abonnee, voor de marketing van eigen telecommunicatiediensten. Richtlijn nr. 2002/58/EG handhaaft de aangegeven hoofdregel van verwijderen of anonimiseren, maar breidt deze zodanig uit, dat ook de verwerking van gegevens in het kader van internet onder de beschermingsomvang van deze regeling is gebracht."*

In de memorie van toelichting bij het 'oude' artikel 11.5 van de Tw stond[12]:

> *"Anonimisering betekent een zodanige bewerking van de gegevens dat deze redelijkerwijs niet meer herleidbaar zijn tot individuele personen. Afhankelijk van de omstandigheden kan dit meebrengen dat niet kan worden volstaan met het eenvoudigweg verwijderen van de naamgegevens, maar dat bovendien maatregelen getroffen zullen moeten worden om daadwerkelijke herleiding van gegevens tot individuele personen te voorkomen."*

De toelichtingen zijn in lijn met overweging 26 van de AVG waarin het begrip 'anonieme gegevens' wordt ingevuld.

> *"gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is."*

De AVG definieert persoonsgegevens als volgt in artikel 4, eerste lid:

> *1) „persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;*

Zodra verkeersgegevens niet meer nodig zijn heeft de aanbieder de keus om de gegevens te verwijderen, dan wel te anonimiseren. Anonimiseren betekent in dit verband dat datasets op onomkeerbare wijze worden ontdaan van direct of indirect persoonsidentificerende kenmerken. Nadat een proces van anonimiseren is doorlopen, ontstaat een nieuwe dataset waarin de gegevens niet als persoonsgegevens zijn aan te merken.

2.3.5 Pseudonimiseren

In artikel 11.5 van de Tw komt het begrip pseudonimiseren niet voor. In het onderzoek is het echter wel van belang, omdat er een wezenlijk verschil bestaat tussen anonimiseren en pseudonimiseren.

[12] Kamerstukken II 1996-1997, 25533 nr. 3, p.120

Artikel 4, onderdeel 5 van de AVG definieert het begrip 'pseudonimisering':

> *"pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;"*

Het vervangen van alle directe identificatoren door een enkel- of meervoudige (salted) hash (versleuteling) daarvan is een bekende pseudonimiseringstechniek. Of alleen het vervangen van de directe indentificatoren leidt tot een gepseudonimiseerde dataset hangt ook af van de andere attributen in de dataset; deze mogen los of in combinatie niet direct identificerend zijn. Omdat het hier een zeer technische dataset betreft wordt (zonder specifiek onderzoek) aangenomen dat het hashen van de identificerende gegevens[13] volstaat om te pseudonimiseren.

Opgemerkt wordt hierbij dat ook zonder een directe identificator, zoals de IMSI (International Mobile subscriber identification), deze dataset bestaat uit persoonsgegevens. Zie in dit verband ook overweging 26 van de AVG:

> *"Gepseudonimiseerde persoonsgegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, moeten als gegevens over een identificeerbare natuurlijke persoon worden beschouwd".*

Dit is van toepassing op locatiegegevens, want daarvan is bekend dat deze zeer individueel onderscheidend zijn, waarmee identificatie dus ook eenvoudig is. Naast wetenschappelijke literatuur[14], [15] is er ook guidance van de EDPB in dit verband[16].

Geanonimiseerde gegevens vallen niet onder reikwijdte van de AVG. Gepseudonimiseerde gegevens wel want dit zijn nog steeds persoonsgegevens, met als gevolg dat zij alleen mogen worden verwerkt als dat rechtmatig, behoorlijk en transparant gebeurt en daarvoor een grondslag bestaat[17].

2.4 De e-Privacyrichtlijn en de verwerking van verkeersgegevens

Hiervoor onder 2.4 zijn enkele begrippen nader toegelicht. In deze paragraaf zal nader worden toegelicht welke voorwaarden vanuit Europees perspectief zijn gesteld aan het verwerken van verkeersgegevens.

[13] Identificerende gegevens: CTN, IMSI, MSISDN
[14] Zang and Bolot, "Anonimization of location data does not work: a large scale measurement study", https://doi.org/10.1145/2030613.2030630
[15] de Montjoye, YA., Hidalgo, C., Verleysen, M. *et al.*, "Unique in the Crowd: The privacy bounds of human mobility", https://doi.org/10.1038/srep01376
[16] Guidelines 04/2020 evenals 01/2020
[17] Zie artikel 5 en 6 AVG

2.4.1 Doel e-Privacyrichtlijn

De reeds hiervoor aangehaalde e-Privacyrichtlijn strekt tot eerbiediging van de grondrechten en beginselen die tot uitdrukking zijn gebracht in met name het Handvest van de grondrechten van de Europese Unie. In het bijzonder strekt deze richtlijn tot volledige eerbiediging van de in de artikelen 7 en 8 bedoelde rechten van het Handvest van de grondrechten van de Europese Unie[18]. Artikel 7 van het Handvest luidt:

> "*Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie*".

Artikel 8 van het Handvest bepaalt:

> 1. *Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.*
> 2. *Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.*
> 3. *Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.*

De e-Privacyrichtlijn strekt daarmee ten algemene tot bescherming van belangrijke grondrechten, met name dus de bescherming van persoonsgegevens en communicatie.

2.4.2 Plicht tot het waarborgen van het vertrouwelijke karakter van de communicatie

Artikel 5, eerste lid van de e-Privacyrichtlijn luidt als volgt:

> *Vertrouwelijk karakter van de communicatie*
> 1. *De lidstaten garanderen via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische communicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1. Dit lid laat de technische opslag die nodig is voor het overbrengen van informatie onverlet, onverminderd het vertrouwelijkheidsbeginsel.*

Het Hof van Justitie in de Promusicae-zaak[19] legde het uitgangspunt van artikel 5, eerste lid, e-Privacyrichtlijn als volgt uit:

> *Artikel 5, lid 1, van richtlijn 2002/58 bepaalt dat de lidstaten het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens*

[18] Zie overweging 2 van de e-Privacyrichtlijn
[19] Zaak C-275/06 r.o. 47 (ECLI:EU:C:2008:54)

via openbare communicatienetwerken en via openbare elektronische communicatiediensten moeten garanderen en met name in beginsel het opslaan van deze gegevens door anderen dan de gebruikers moeten verbieden, indien de betrokken gebruikers daarin niet hebben toegestemd. Deze bepaling maakt slechts een uitzondering voor personen die overeenkomstig artikel 15, lid 1, de wettelijke toelating hebben gekregen, en de technische opslag die nodig is voor het overbrengen van informatie.

Artikel 6 e-Privacyrichtlijn werkt dit voor verkeersgegevens nader uit:

Verkeersgegevens

1. *Verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronische-communicatienetwerk of -dienst, moeten, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, worden gewist of anoniem gemaakt, onverminderd de leden 2, 3 en 5, alsmede artikel 15, lid 1.*
2. *Verkeersgegevens die noodzakelijk zijn ten behoeve van de facturering van abonnees en interconnectiebetalingen mogen worden verwerkt. Die verwerking is slechts toegestaan tot aan het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen.*
3. *De aanbieder van een openbare elektronische-communicatiedienst mag ten behoeve van de marketing van elektronische-communicatiediensten of voor de levering van diensten met toegevoegde waarde de in lid 1 bedoelde gegevens verwerken voorzover en voor zolang dat nodig is voor dergelijke diensten of marketing, indien de abonnee of de gebruiker waarop de gegevens betrekking hebben daartoe zijn toestemming heeft gegeven. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.*
4. *De dienstenaanbieder moet de abonnee of gebruiker in kennis stellen van de soorten verkeersgegevens die worden verwerkt en van de duur van de verwerking voor de in lid 2 genoemde doeleinden en, voorafgaand aan het verkrijgen van diens toestemming, voor de in lid 3 genoemde doeleinden.*
5. *De verwerking van verkeersgegevens overeenkomstig de leden 1 tot en met 4 mag alleen worden uitgevoerd door personen die werkzaam zijn onder het gezag van de aanbieders van de openbare communicatienetwerken of -diensten voor facturering of verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude en marketing van elektronische-communicatiediensten van de aanbieder of de levering van diensten met toegevoegde waarde, en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren.*
6. *De leden 1, 2, 3 en 5 zijn van toepassing onverminderd de mogelijkheid voor de bevoegde organen om overeenkomstig de toepasselijke wetgeving in kennis te worden gesteld van verkeersgegevens met het oog op het beslechten van geschillen, in het bijzonder met betrekking tot interconnectie en facturering.* [onderstrepingen AT]

Artikel 6 van de e-Privacyrichtlijn geeft aan voor welke specifieke doelen het vertrouwelijke karakter van de communicatie en daarmee verband houdende verkeersgegevens doorbroken mag worden.

2.4.3 Jurisprudentie

In zijn arrest La Quadrature du Net van 6 oktober 2020[20] heeft het Hof van de EU de materiele strekking van de e-privacyrichtlijn als volgt omschreven:

> *"108 Wat in het bijzonder de verwerking en de opslag van verkeersgegevens door aanbieders van elektronische communicatiediensten betreft, blijkt uit artikel 6 en de overwegingen 22 en 26 van richtlijn 2002/58 dat een dergelijke verwerking slechts is toegestaan voor zover en zolang dat nodig is voor de marketing en de facturering van de diensten en voor de levering van diensten met toegevoegde waarde. Zodra die periode is verstreken, moeten de verwerkte en opgeslagen gegevens worden gewist of geanonimiseerd. […]*
>
> *109 Met de vaststelling van richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronische communicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd."*

Duidelijk is derhalve dat artikel 6 van de e-Privacyrichtlijn een limitatieve opsomming van verwerkingsdoelen kent, die slechts bij wet kan worden aangevuld.

2.4.4 Verhouding e-Privacyrichtlijn en AVG

Uit het voorgaande volgt dat de verwerking van verkeersgegevens niet is toegestaan voor andere doeleinden dan die limitatief zijn opgesomd in artikel 6 van de e-Privacyrichtlijn / artikel 11.5 van de Tw. De e-Privacyrichtlijn specificeert daarmee de bepalingen uit de AVG met betrekking tot de verwerking van persoonsgegevens in de sector elektronische communicatie. Zie in dit verband ook de European Data Protection Board (EDPB)[21]:

> *38. Een aantal bepalingen van de e-privacyrichtlijn "specificeren" de bepalingen van de AVG met betrekking tot de verwerking van persoonsgegevens in de sector elektronische communicatie. In overeenstemming met het beginsel lex specialis derogate legi generali, hebben bijzondere bepalingen voorrang boven de algemene regels in de situaties die zij specifiek beogen te regelen. In situaties waarin de e-privacyrichtlijn de regels van de AVG "specificeert" (d.w.z. meer specifiek maakt) krijgen de (specifieke) bepalingen van de e-privacyrichtlijn als "lex specialis" voorrang boven de (meer algemene) bepalingen van de AVG. Elke verwerking van persoonsgegevens waarop de e-privacyrichtlijn niet specifiek van toepassing is (of waarvoor de e-privacyrichtlijn geen "bijzondere regel" bevat), blijft echter onderworpen aan de bepalingen van de AVG.*

[20] ECLI:EU:C:2020:791
[21] 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, https://edpb.europa.eu/our-work-tools/our-documents/styrelsens-yttrande-art-64/opinion-52019-interplay-between-eprivacy_n

> *39. Een voorbeeld van het "specificeren" door de e-privacyrichtlijn van de bepalingen van de AVG wordt gevormd door artikel 6 van de e-privacyrichtlijn, dat betrekking heeft op de verwerking van zogenoemde "verkeersgegevens". In de regel kan de verwerking van persoonsgegevens worden gerechtvaardigd op basis van elk van de in artikel 6 van de AVG genoemde rechtmatigheidsgronden. Het volledige scala van de door artikel 6 AVG geboden mogelijke rechtmatigheidsgronden kan door de aanbieder van een elektronische-communicatiedienst echter niet worden toegepast op de verwerking van verkeersgegevens, omdat artikel 6 van de e-privacyrichtlijn de voorwaarden waaronder verkeersgegevens, met inbegrip van persoonsgegevens, kunnen worden verwerkt, expliciet beperkt. In dat geval moeten de meer specifieke bepalingen van de e-privacyrichtlijn voorrang hebben boven de meer algemene bepalingen van de AVG. Artikel 6 van de e-privacyrichtlijn beperkt echter de toepassingen van andere bepalingen van de AVG, zoals inzake de rechten van de betrokkene, niet. Evenmin doet het afbreuk aan de eis dat de verwerking van persoonsgegevens rechtmatig en behoorlijk moet zijn (artikel 5, lid 1, onder a), AVG).”*

Artikel 6 van e-Privacyrichtlijn regelt daarmee zowel de grondslagen als doelen van verwerking van verkeersgegevens uitputtend, zelfs als dit persoonsgegevens in de zin van de AVG betreffen.

2.5 Verwerking van verkeersgegevens in de Tw

Zoals hiervoor reeds opgemerkt is artikel 6 van de e-Privacyrichtlijn omgezet in artikel 11.5 van de Tw. In navolging van artikel 6 van de e-Privacyrichtlijn regelt artikel 11.5 van de Tw ook uitputtend waarvoor verkeersgegevens mogen worden verwerkt. Zie in dit verband ook de memorie van toelichting:

> *“Deze richtlijn en de uitwerking daarvan in hoofdstuk 11 hebben ten opzichte van de algemene privacyrichtlijn en de uitwerking daarvan in de Wbp een aanvullende werking, waarbij op onderdelen sprake is van een nadere uitwerking van de meer algemene normen uit de algemene privacyrichtlijn onderscheidenlijk de Wbp. Voor specifieke – in de sfeer van elektronische communicatie – voorkomende verwerkingen van persoonsgegevens worden namelijk daarop toegesneden (en in voorkomend geval uitputtende) normen gesteld. Voorts strekt de reikwijdte van de bepalingen van de privacyrichtlijn telecommunicatie zich in beginsel ook uit tot rechtspersonen. De Wbp heeft daarentegen alleen betrekking op de verwerking van gegevens betreffende natuurlijke personen.”*[22]

Ter illustratie dat verkeersgegevens, zelfs in de context van een pandemie, niet voor andere doeleinden mogen worden verwerkt – en de toegestane verwerkingen in artikel 11.5 Tw limitatief zijn – wordt nog verwezen naar de memorie van toelichting bij de Tijdelijke wet informatieverstrekking RIVM i.v.m. Covid-19[23]:

> *“Om de in artikel 14.7, tweede lid, bedoelde informatie te kunnen verstrekken, moeten de aanbieders verkeers- en locatiegegevens bewerken. De op dit moment geldende grondslag voor het verwerken van verkeers- en locatiegegevens is te vinden in de artikelen 11.5 en 11.5a van de Telecommunicatiewet die daarbij*

[22] Kamerstukken II, 28851, nr. 3, p. 45
[23] Tweede Kamer, vergaderjaar 2019–2020, 35 479, nr. 3

uitvoering geven aan richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) hierna: richtlijn 2002/58/EG. Deze artikelen bieden geen grondslag voor de verwerking ten behoeve van het verstrekken van informatie aan het RIVM."

2.6 Tussenconclusie toetsingskader

Artikel 5 van de e-Privacyrichtlijn bepaalt het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens. Artikel 6 van de e-Privacyrichtlijn maakt het doorbreken van dit vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeers- en locatiegegevens mogelijk voor een beperkt aantal doeleinden. Dit vindt zijn weerslag in artikel 11.5 en 11.13 van de Tw. Ná het verwerken ten behoeve van deze limitatief omschreven doeleinden, moeten de resterende gegevens worden verwijderd of worden geanonimiseerd. Het wijzigen van identificerende gegevens in een gehashte versie resulteert niet in geanonimiseerde verkeersgegevens. Verkeersgegevens met gehashte of origineel identificerende gegevens worden tevens gekwalificeerd als persoonsgegevens.

3 Bevindingen

Hierna volgen de bevindingen op basis van de inspectie bij KPN en eigen onderzoek. Allereerst zal kort ingegaan worden op de kwalificatie van KPN, hierna het verloop van de inspectie en tot slot de resultaten van de deskresearch.

3.1 Kwalificatie KPN

Voor het verwerken van verkeersgegevens is met name artikel 11.2a, 11.5 en 11.13 van de Tw van toepassing. Onder de definitie verkeersgegevens kunnen tevens locatiegegevens[24] vallen. Normadressanten voor de voorgaande artikelen zijn aanbieders van openbare elektronische communicatienetwerken of -diensten. KPN is een dergelijke aanbieder en staat als zodanig geregistreerd in het register van de Autoriteit Consument en Markt (ACM). Voor de verwerking van verkeersgegevens moet KPN, binnen de scope van deze inspectie, voldoen aan de eisen zoals gesteld in artikel 11.5 van de Tw.

3.2 Verloop inspectie

Op 17 oktober 2022 heeft ondergetekende 5.1.2.e , 5.1.2.e , en 5.1.2.e , 5.1.2.e , namens AT een bezoek gebracht aan KPN te Zoetermeer. Hier is gesproken met 5.1.2.e , 5.1.2.e en 5.1.2.e , 5.1.2.e , beiden werkzaam bij KPN.

Na de introductie is ingegaan op het privacy statement van KPN, versie september 2022, met name hoofdstuk 10 "*Delen van jouw gegevens met derden*" en specifiek artikel 10.1. "*wat doen wij niet*". In dit artikel staat vermeld: "*KPN verkoopt je gegevens niet aan derden voor marketing of soortgelijke bedrijfsmatige activiteiten. Als wij wel gegevens delen voor activiteiten van derden dan gebeurt dit alleen in geanonimiseerde en geaggregeerde vorm. Dat betekent dat de gegevens op geen enkele manier meer te herleiden zijn tot een individu*".

Het privacy statement maakt onderscheid in contact-/gebruiksgegevens (hoeveel heb je gebeld) en verbruiksgegevens (met wie heb je gebeld, waar en wanneer). Aangezien in artikel enkel wordt gesproken over gegevens geldt dit voor zowel contact-/gebruiksgegevens als verbruiksgegevens. Verbruiksgegevens zijn verkeersgegevens zoals bedoeld in artikel 11.5 van de Tw.

KPN heeft aangegeven verkeersgegevens, waaronder locatiegegevens, uitsluitend te verwerken voor toegestane doeleinden. Verkeersgegevens worden alleen verwerkt voor doelen zoals toegestaan in de Tw. In het privacy statement staat beschreven dat KPN-verbruiksgegevens[25] twee weken en bel/internet gegevens voor de facturering zes maanden bewaart.

[24] Tweede Kamer, 28851, nr. 3, pagina 47
[25] Hiermee worden vluchtige verkeersgegevens dan wel signaleringsgegevens bedoeld.

KPN geeft aan dat, indien er verkeersgegevens aan derde worden verstrekt, dit gebeurt in een geanonimiseerde vorm en pas nadat de termijn van verwerking (zes maanden) is verstreken. Op dit moment worden geen (geanonimiseerde) verkeersgegevens aan derde verstrekt tenzij anderszins door de Tw is bepaald[26].

Met betrekking tot anonimisering is KPN zeer strikt.
Daarbij laat KPN zich leiden door de navolgende uitleg:

- "*Daarbij wordt onder anonimiseren verstaan dat de betreffende gegevens volledig en op onomkeerbare wijze worden ontdaan van hun persoonsidentificerende kenmerken*"
- "*when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data."*[27]

KPN geeft als voorbeeld een voorbeeld uit een rapport van de WP29
"*For example: if an organization collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties. But if the data controller would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as 'on Mondays on trajectory X there are 160% more passengers than on Tuesdays', that would qualify as anonymous data."*

KPN is afgelopen jaren diverse malen benaderd door Mezuro[28] voor het leveren van verkeersgegevens ten behoeve van mobiliteitsinformatie. KPN geeft aan hier geen gehoor aan te hebben gegeven waarbij KPN als reden heeft aangegeven dat de huidige wetgeving dit niet toestaat.

3.3 Deskresearch

Bij het ronde tafelgesprek "Tijdelijke wet informatieverstrekking RIVM i.v.m. Covid-19" van 15 oktober 2020 heeft KPN een "position paper"[29] ingediend. Hierin geeft KPN onder andere aan:
" *Ook is er in de huidige Tw geen grondslag om locatiegegevens te verwerken tot een afgeleide herkomst van een telefoon. Mochten telecomlocatiegegevens nodig worden geacht in het tegengaan van de verspreiding van het COVID-virus, dan moet daarvoor dus een nieuwe wettelijke basis worden gecreëerd – hetgeen met het huidige wetsvoorstel gebeurt*."

Bij AT is bekend dat KPN in 2018 is benaderd door het Centraal Bureau Statistiek om verkeersgegevens te leveren voor het maken van mobiliteitsstatistieken. KPN heeft aangeven hierop niet te zijn ingegaan.

[26] Artikel 11.5, lid 6 en artikel 11.13 Tw
[27] WP29 opinion 05/2014 on anonymisation techniques
[28] Mezuro is een leverancier van mobiliteitsinformatie
[29] Bijlage 2

Een onderzoek op internet heeft vooralsnog geen indicatie opgeleverd dat KPN op enigerlei wijze verkeersgegevens verwerkt of heeft verwerkt voor gebruik bij mobiliteitsinformatie.

4 Conclusie

Op basis van de geleverde informatie door KPN en nader onderzoek kan geconcludeerd worden dat KPN geen verkeersgegevens verwerkt of heeft verwerkt ten behoeve van mobiliteitsinformatie.

Sluiting
Ik heb dit inspectierapport naar waarheid opgemaakt te Amersfoort op 1 november 2022

De toezichthouder,

5.1.2.e
Hoofdafdeling Toezicht
Afdeling Veiligheid

5 Bijlagen

1. Power point presentatie inspectie 17 oktober 2022
2. Position paper ronde tafelgesprek "tijdelijke wet informatieverstrekking RIVM i.v.m. Covid-19, 15 oktober 2020
3. Privacy statement artikel 10.1

Omgang met verkeersgegevens en anonimisatie

5.1.2.e

12 oktober 2022

kpn. Het netwerk van Nederland

definitie Verkeersgegevens 11.1

gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan. Onder verkeersgegevens moeten onder meer de volgende soorten gegevens worden verstaan. Waar het gaat om spraaktelefonie kan men onder meer de volgende verkeersgegevens onderscheiden: oproepende en opgeroepen nummer, begin en einde van de oproep (tijdstip), duur van de oproep en ± waar het mobiele telefonie betreft ± ook de locatiegegevens (gegevens betreffende de basisstations). In de sfeer van internet moet onder meer worden gedacht aan: identiteit aansluiting, gebruikersnaam (user id), IP-adressen, e-mailadres, het gebruikte protocol, begin- en eindtijd sessie, type dienst, volume (aantal kilobytes).

Juridisch kader artikel 11.5

Verkeersgegevens mogen gebruikt worden voor:
- overbrengen communicatie
- facturatie (en als afgeleide daarvan verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude)

Tevens kunnen na toestemming verkeersgegevens worden gebruikt voor andere doeleinden (commercieel, toegevoegde waarde diensten etc.)

Juridisch kader 11.5a Verwerking locatiegegevens niet zijnde verkeersgegevens

MEMORIE VAN TOELICHTING 2003, pagina 157

Voor de verwerking van dergelijke gegevens zullen in het netwerk specifieke technische voorzieningen getroffen moeten worden, waarmee het mogelijk is om nauwkeurige locatiegegevens te genereren. De verwerking van dergelijke gegevens zal (veelal) uitsluitend plaatsvinden met het oog op de levering van diensten met toegevoegde waarde

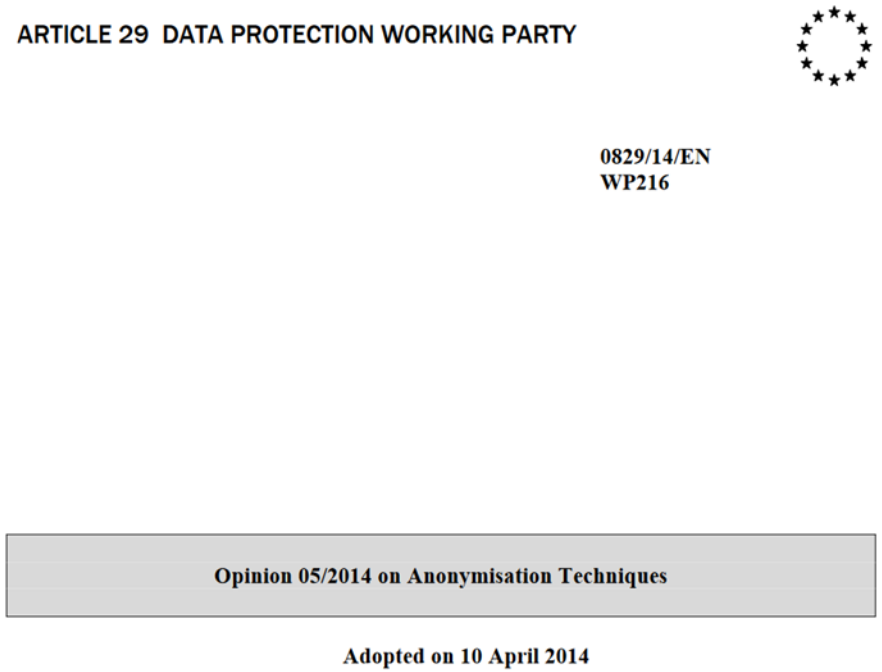
Deze gegevens mogen gebruikt worden na anonimisatie of na toestemming

Anonimiseren

Als hoofdregel geldt dat alle door aanbieders van openbare elektronische communicatienetwerken en -diensten verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees en gebruikers worden verwijderd dan wel geanonimiseerd, zodra deze gegevens niet langer nodig zijn ten behoeve van (het doel van) de overbrenging van communicatie. Daarbij wordt onder anonimiseren verstaan dat de betreffende gegevens volledig en op onomkeerbare wijze worden ontdaan van hun persoonsidentificerende kenmerken

wp29 opinion 05/2014 on anonymisation techniques

pagina 9



ARTICLE 29 DATA PROTECTION WORKING PARTY

0829/14/EN
WP216

Opinion 05/2014 on Anonymisation Techniques

Adopted on 10 April 2014

Secondly, “the means likely reasonably to be used to determine whether a person is identifiable” are those to be used “by the controller or by any other person”. Thus, it is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data.

Voorbeeld uit rapport WP29

For example: if an organization collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties. But if the data controller would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as ‘on Mondays on trajectory X there are 160% more passengers than on Tuesdays', that would qualify as anonymous data

Standpunten CBS
Artikel 9 lid 3 Wbp <vervallen>

3. Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden, wordt niet als onverenigbaar beschouwd, indien de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden

Advies Zwenne op verzoek CBS

PELS RIJCKEN

Advies

voor Centraal Bureau voor de Statistiek
van Gerrit-Jan Zwenne & Lars Groeneveld
datum 31 januari 2020
inzake Advies Telecommunicatiewet
zaaknr 11012720

---

1 Inleiding

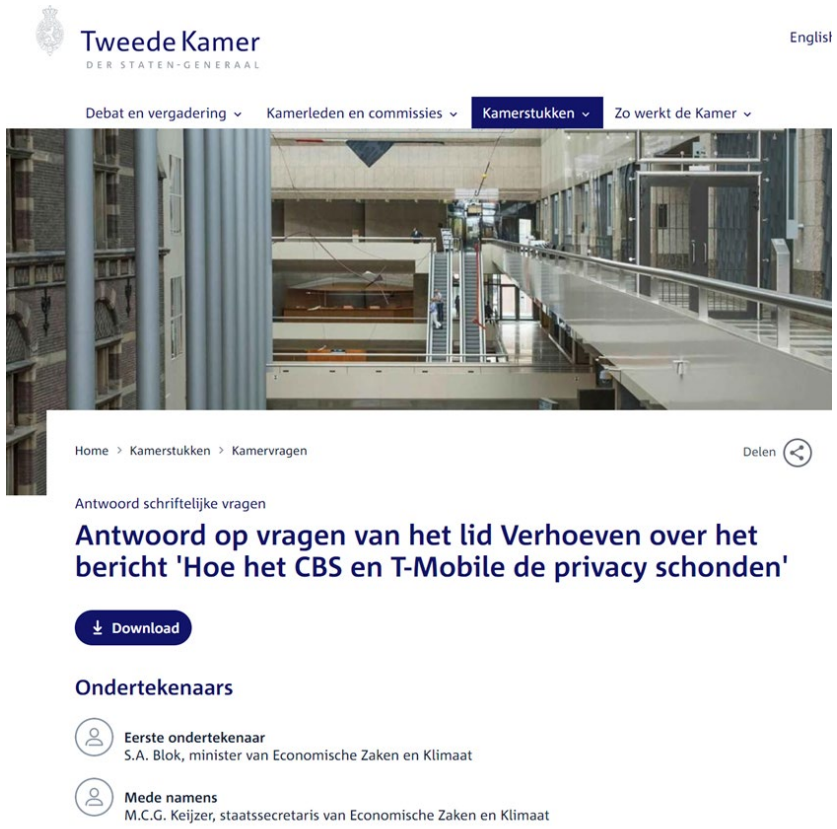
1.1 Het Centraal Bureau voor de Statistiek (hierna: CBS) onderzoekt de mogelijkheid om verkeersgegevens van telecomaanbieder(s) (hierna: Telco(s)), te gebruiken voor statistisch onderzoek. Daarbij zijn enkele vragen gerezen ten aanzien van de rechtmatigheid van dat onderzoek onder de Telecommunicatiewet (of Tw). De vragen van CBS luiden (geparafraseerd) als volgt:

2.3 Voor zover wij uit openbare en niet-openbare bronnen hebben kunnen nagaan, is het gemeenschappelijk uitgangspunt van de ontwikkelde onderzoeksmethoden dat gegevens in geanonimiseerde vorm worden aangeleverd door de betreffende Telco. Uit de verschillende onderzoekmethoden die wij hebben bestudeerd, wordt niet duidelijk hoe de anonimisering van de aangeleverde gegevens is vormgegeven. Ook is niet duidelijk of de gegevens geanonimiseerd zijn volgens de eisen die de AVG daaraan stelt (zie verder randr. 3.17).

4 Conclusie

4.1 Gelet op het bovenstaande voldoet de door CBS beoogde onderzoeksmethode aan de eisen die artikel 11.5 Tw daaraan stelt.

Vragen tweede kamer leden



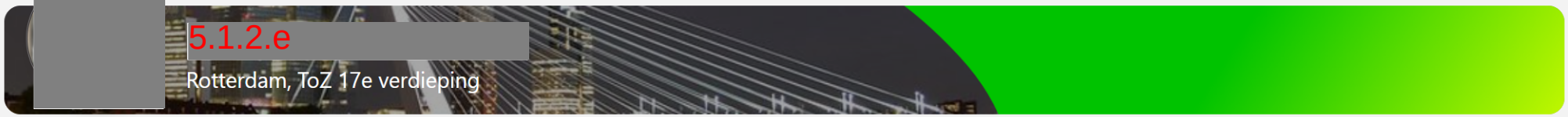
Vraag 4
Wist u dat het CBS op grote schaal werkte met direct en indirect herleidbare locatiegegevens van miljoenen burgers? Wat heeft u gedaan met signalen en zorgen dat het verzamelen van data via T-Mobile strijdig was met privacywetgeving? Wanneer zijn de eerste stappen ondernomen?

Antwoord 4
Het CBS heeft naar eigen zeggen geen toegang gehad tot individuele klantgegevens van personen. De onderzoeksgegevens zouden, aldus het CBS, niet direct of indirect herleidbaar zijn naar personen en het betroffen evenmin direct of indirect herleidbare locatiegegevens van personen. In het artikel van NRC wordt gesteld dat de CBS-medewerkers mogelijk toegang hebben gehad tot verkeersgegevens van klanten van T-Mobile. Het Agentschap Telecom heeft besloten naar aanleiding hiervan een onderzoek in te stellen, bijgestaan door de Autoriteit Persoonsgegevens. Over het onderzoek kunnen op dit moment geen uitlatingen worden gedaan. Het is aan het oordeel van de toezichthouders het Agentschap Telecom en de Autoriteit Persoonsgegevens of deze pilot voldeed aan de wettelijke privacy-eisen.

Vraag 5
Wat vindt u van de opportunistische handelwijze van T-Mobile, inclusief het verzwijgen van activiteiten en het openlijk bepleiten van terughoudendheid met commercieel datagebruik?

Antwoord 5
Met deze vraag doelt de heer Verhoeven vermoedelijk op de door hem vermeende tegenstelling in de houding van T-Mobile over de CBS-pilot en de kritische houding van T-Mobile over de Tijdelijke wet informatieverstrekking RIVM. Ik vind het echter niet aan mij om hier namens de regering een uitspraak over te doen.

5.1.2.e 5.1.2.e



← Terug naar blog overzicht van 5.1.2.e

Reactie op de publicatie van NRC “Hoe het CBS en T-Mobile de privacy schonden”.

11 maart 2021 · 704x gelezen · 5.1.2.e

De NRC heeft vandaag een artikel gepubliceerd en een podcast geplaatst over dataleveringen van T-Mobile aan het CBS.

Uit de podcast blijkt dat T-Mobile jaren lang CBS medewerkers toegang gaf tot gepseudonimiseerde telecomdata, alleen het imsi-nummer was vervangen door een ander nummer. De toezichthouders AT en AP gaan nu een onderzoek starten naar deze leveringen door T-Mobile. Hieronder de link naar de (zeer beluisterwaardige) podcast, mocht je geen 20 minuten willen luisteren, ga dan direct naar minuut 16.30 waar het CBS geconfronteerd wordt met het standpunt van KPN.
http://www.nrc.nl/nieuws/2021/03/11/hoe-het-cbs-en-t-mobile-de-privacy-van-miljoenen-nederlanders-schonden-a4035124

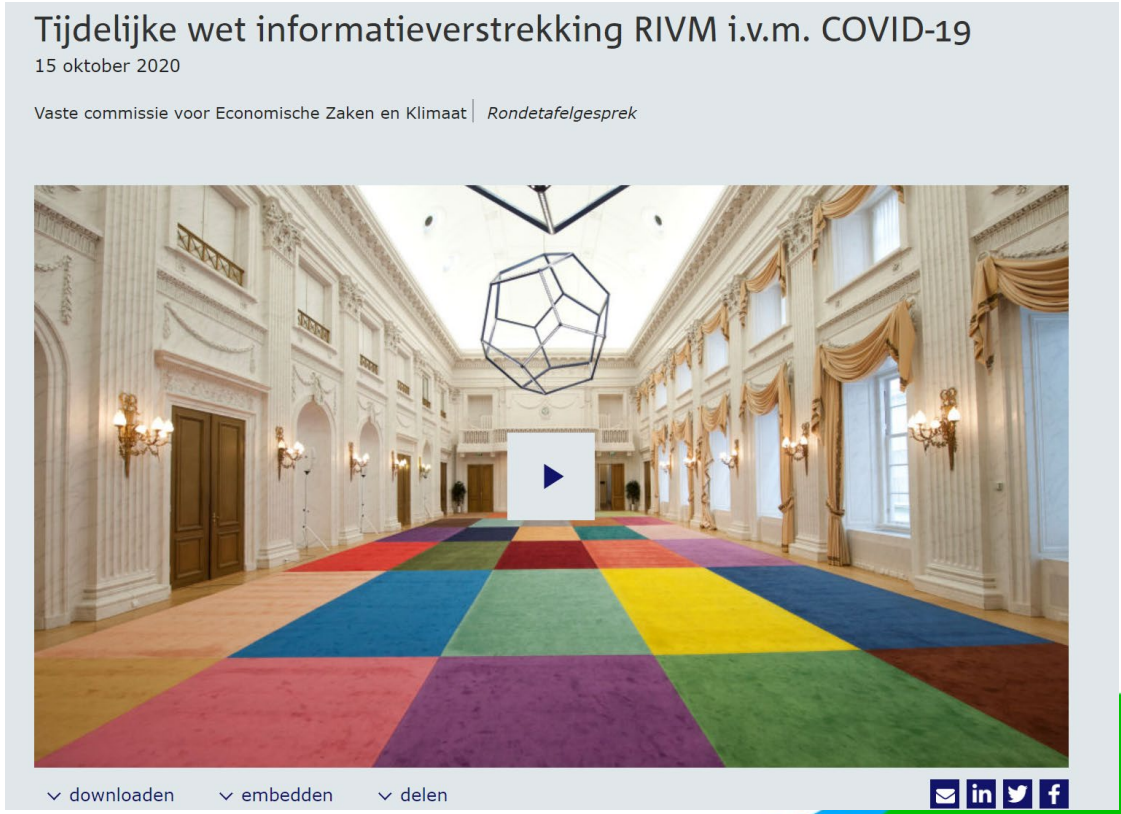
Bewerk

Verwijder

Laatste blogs

Security and costs can't go together! Or can they?

[Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19 | Debat Gemist (tweedekamer.nl)]



kpn. Het netwerk van Nederland

Datum	8 oktober 2020
Auteur	[redacted]
Versie	1.0

KPN inbreng hoorzitting Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19

Als het RIVM, het kabinet en het parlement tot de conclusie komen dat telecomlocatiegegevens nodig zijn voor een effectieve bestrijding van het COVID-19 virus dan heeft KPN de volgende aandachtspunten:

- De bescherming van de privacy van onze klanten is voor KPN van zeer groot belang. De gevraagde berekening zal KPN dan ook alleen maken om te voldoen aan deze wet. De betreffende gegevens zullen voor geen enkel ander doeleinde gebruikt worden of anderszins beschikbaar worden gemaakt.
- De voorgestelde wettekst en de tweede nota van wijziging bevestigen dat de in artikel 14.7 lid 2 gevraagde 'afgeleide herkomst' berekening door telecomproviders moeten worden gemaakt. Er worden dus geen bronbestanden gedeeld met het CBS. Alleen zo kan KPN waarborgen dat privacygevoelige informatie niet onnodig wordt verstrekt of gedeeld.
- In de tweede nota van wijziging wordt verduidelijkt dat voor de gevraagde berekening alleen gebruikt gemaakt mag worden van gegevens als een telefoon actief verbinding maakt met het netwerk. In de begeleidende brief wordt terecht aangegeven dat het dus uitsluitend gaat om gegevens die providers nu ook bewaren voor doeleinden genoemd in artikel 11.5 van de telecommunicatiewet (facturering). Door deze dataminimalisatie komt privacy van klanten zo min mogelijk in het geding en is het voor klanten duidelijk welke data als bron worden gebruikt voor de berekening die geleverd zal moeten worden aan het CBS.

Inleiding

Voor KPN is de privacy van onze klanten van het grootste belang. Het vertrouwen dat onze klanten hebben in onze dienst, het veilig en vertrouwelijk overbrengen van communicatie, staat aan de basis van ons bestaansrecht. KPN heeft sinds het uitbreken van het COVID-virus aangegeven graag te helpen bij de bestrijding hiervan. Dit hebben we onder meer gedaan door onze klanten te voorzien van extra connectiviteit waar dat nodig was toen heel Nederland thuis kwam te werken. Ook hebben we leerlingen die thuis geen internet hadden voorzien van connectiviteit zodat ze online lessen kunnen volgen. Binnen de kaders van de Algemene Verordening Gegevensbescherming (hierna: AVG) en de sectorspecifieke regels in de Telecommunicatiewet (hierna: Tw) zijn we ook bereid locatiedata te delen mocht dit noodzakelijk worden geacht voor de bestrijding van het COVID-virus. Daarbij moet de privacy van onze klanten uiteraard worden gewaarborgd.

De centrale vraag die moet worden beantwoord is of de inzet van telecomlocatiegegevens voldoende bijdraagt aan de bestrijding van het COVID-virus om de voorgestelde wetswijziging door te voeren en de extra bewerking die wordt gevraagd te maken. Dat oordeel is aan uw Kamer.
De Autoriteit Persoonsgegevens (hierna: AP) heeft aangegeven dat telecomlocatiegegevens die voor de bestrijding worden gevraagd niet als anoniem kunnen worden gezien en daarom binnen de huidige kaders van de wet niet mogen worden gedeeld.[1] Als het RIVM, het kabinet en het parlement tot de conclusie komen dat telecomlocatiegegevens nodig zijn voor een effectieve bestrijding van dit virus dan biedt het wetsvoorstel dat nu voorlicht, inclusief de tweede nota van wijziging, voldoende waarborgen om de inbreuk op de privacy van onze klanten tot een minimum te beperken.

Praktijk en privacy

Zowel voor de bescherming van de privacy als voor de praktische uitwerking van de voorgestelde wet is het belangrijk dat de gevraagde locatiegegevens aansluiten bij data die telecomproviders ook nu al bewaren in het kader van hun dienstverlening. Er hoeven dan immers geen nieuwe gegevens te worden verzameld. In het kader van de normale bedrijfsvoering creëert KPN gegevens om geleverde diensten te kunnen factureren, ook wel aangeduid als de factureringsdatabase.[2] KPN slaat deze gegevens een aantal maanden op om te kunnen factureren en voor de afhandeling van facturatieklachten. Deze verwerking is ook beschreven in ons privacy statement, en onze klanten weten daarvan.

---

[1] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-beoordeelt-tijdelijke-wet-telecomdata-op-waarborgen-privacy
[2] De technische term voor deze gegevens is Call Detail Records (CDRs). In de Telecommunicatiewet wordt gesproken over 'verkeersgegevens'. Deze CDRs worden alleen gecreëerd bij bellen, sms of bij gebruik van data als een bepaalde hoeveelheid data wordt bereikt. Het verversen van appjes op de achtergrond, als het eindapparaat niet actief wordt gebruikt, wordt hier niet in opgeslagen.

In de eerste nota van wijziging (25 juni 2020) staat terecht dat wanneer een telefoon in een bepaald uur niet actief contact heeft gemaakt met het netwerk er voor dat uur geen factureringsgegevens worden geregistreerd. Op grond van het huidige voorstel zullen wij die gegevens dus ook niet alsnog gaan verzamelen.

Het wetsvoorstel verlangt dat KPN vervolgens uit de factureringsgegevens een 'afgeleide herkomst' berekent.[3] Dat doen we nu uiteraard niet - dit wordt na inwerkingtreding van de wet een nieuwe bewerking. De basis waarop deze nieuwe bewerking plaatsvindt, gegevens uit de factureringsdatabase, is echter niet nieuw. De tweede nota van wijziging (2 oktober 2020) geeft in het nieuwe lid 7 (artikel 14.7 lid 7) aan dat de aanbieder de berekening van de afgeleide herkomst direct na het delen van deze berekening met het CBS moet verwijderen. Dat draagt naar onze mening bij aan de bescherming van de privacy van onze klanten. Het lijkt ons onwaarschijnlijk dat gegevens die aan het CBS zijn verstrekt nog kunnen worden herleid tot individuele gebruikers. Overigens geeft KPN in haar privacy statement ook al aan gegevens van onze klanten niet te verkopen.[4]

Wettelijk kader

Telecomproviders vallen naast de AVG ook onder de striktere e-Privacyrichtlijn die is geïmplementeerd in de Tw. Toepassingen als Google Maps of Facebook movements trends vallen alleen onder de AVG en locatiegegevens van die diensten hebben daarom louter een verwerkingsgrondslag nodig onder de AVG, zoals bijvoorbeeld een gerechtvaardigd belang. Hierdoor is de verwerking van dergelijke gegevens juridisch sneller toegestaan dan het gebruik van telecomlocatiegegevens, die extra zijn gereguleerd onder de Tw. Voor telecomdata is in artikel 11.5 Tw als hoofdregel neergelegd dat alleen anonieme gegevens zonder nadere grondslag mogen worden verwerkt en gedeeld met derden. De AP oordeelt op basis van *Opinion 05/2014 on Anonymisation Techniques*[5] dat telecomdata niet anoniem zijn zolang er een bronbestand is, waardoor er altijd de mogelijkheid van (indirecte) herleidbaarheid bestaat. Telecomlocatiedata kunnen door de specificatie in de Tw en de uitleg van de AP dus alleen anoniem worden gedeeld als bronbestanden worden verwijderd. Aangezien bij KPN het bronbestand enige maanden bewaard moet blijven voor facturering en navraag c.q. klachten daarover mogen de daarvan afgeleide gegevens op grond van de thans geldende wetgeving gedurende die tijd dus niet worden gedeeld. Ook is er in de huidige Tw geen grondslag om locatiegegevens te verwerken tot een afgeleide herkomst van een telefoon.[6] Mochten telecomlocatiegegevens nodig worden geacht in het tegengaan van de verspreiding van het COVID-virus, dan moet daarvoor dus een nieuwe wettelijke basis worden gecreëerd – hetgeen met het huidige wetsvoorstel gebeurd.
KPN is ermee bekend dat toezichthouders in andere Europese landen geen bezwaar hebben gemaakt tegen het delen van geaggregeerde gegevens en dat meerdere providers in het buitenland gegevens met de Europese Commissie delen. KPN kan echter niet anders dan de interpretatie van de Nederlandse toezichthouder volgen.

Conclusie

Indien uw Kamer concludeert dat telecomlocatiegegevens nodig zijn in de bestrijding van het COVID-virus dan zal KPN daar op grond van het nu voorliggende voorstel voor wet (inclusief de tweede nota van wijziging) aan mee kunnen werken. Deze nieuwe wettelijke basis is daarvoor echter ook echt nodig – de huidige wettelijke regeling is – indachtig de interpretatie van het AP – ontoereikend. In de tweede nota van wijziging is verduidelijkt dat louter gebruik wordt gemaakt van gegevens uit de factureringsdatabase. Hierdoor wordt de impact op de privacy van onze klanten tot een minimum beperkt.

[3] Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19, Artikel 14.7 lid 2.
[4] www.kpn.com/privacy
[5] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216.
[6] In de voorliggende wettekst wordt dit aangemerkt met de term 'mobiel eindapparaat'.

10. Delen van jouw gegevens met derden

10.1 Wat doen wij niet

KPN verkoopt je gegevens niet aan derden voor marketing of soortgelijke bedrijfsmatige activiteiten. Als wij wel gegevens delen voor activiteiten van derden dan gebeurt dit alleen in geanonimiseerde en geaggregeerde vorm. Dat betekent dat de gegevens op geen enkele manier meer te herleiden zijn tot een individu.