Van: [redacted]@autoriteitpersoonsgegevens.nl>
Verzonden: woensdag 14 juni 2017 13:27
Aan: [redacted](STV)
CC: [redacted] drs. [redacted]
Onderwerp: inlichtingen over WifFi-Tracking

Geachte heer [redacted]

Naar aanleiding van ons telefoongesprek ontvangen wij graag verdere informatie over de WiFi- en Bluetooth-tracking zoals die door de NS op haar stations wordt toegepast.
Wij ontvangen graag het technische stroomschema, de wijze waarop de salt wordt gegenereerd, uw artikel over de werkwijze en de contactgegevens van de privacyofficer van de NS.

Met vriendelijke groet,
Mede namens mijn collega [redacted] (in CC)

[redacted]
Senior Inspecteur

AUTORITEIT
PERSOONSGEGEVENS

[redacted]@autoriteitpersoonsgegevens.nl
T 070 8888 500 - F 070 8888 549
Bezuidenhoutseweg 30, 2594 AV Den Haag
Postbus 93374, 2509 AJ Den Haag
autoriteitpersoonsgegevens.nl

Van: [redacted] (STV)
Verzonden: woensdag 14 juni 2017 13:42
Aan: [redacted] drs. [redacted]
CC: [redacted] (NSG)
Onderwerp: Re: inlichtingen over WifFi-Tracking

Geachte heer [redacted], mevrouw [redacted]

Hartelijk dank voor het toesturen van uw contactgegevens. Dit naar aanleiding van ons telefoongesprek van zojuist. In de cc vindt u het mailadres van de NS Privacy Officer [redacted]. U kunt hem telefonisch bereiken op [redacted].

Bijgevoegd is het stroomschema waar ik tijdens ons gesprek naar heb verwezen. Dit stroomschema is onderdeel van het Informatiebeleid SMART Station. Daarnaast is bijgevoegd een artikel uit 2013 waarin we voor vakgenoten hebben beschreven wat we doen en waarom.

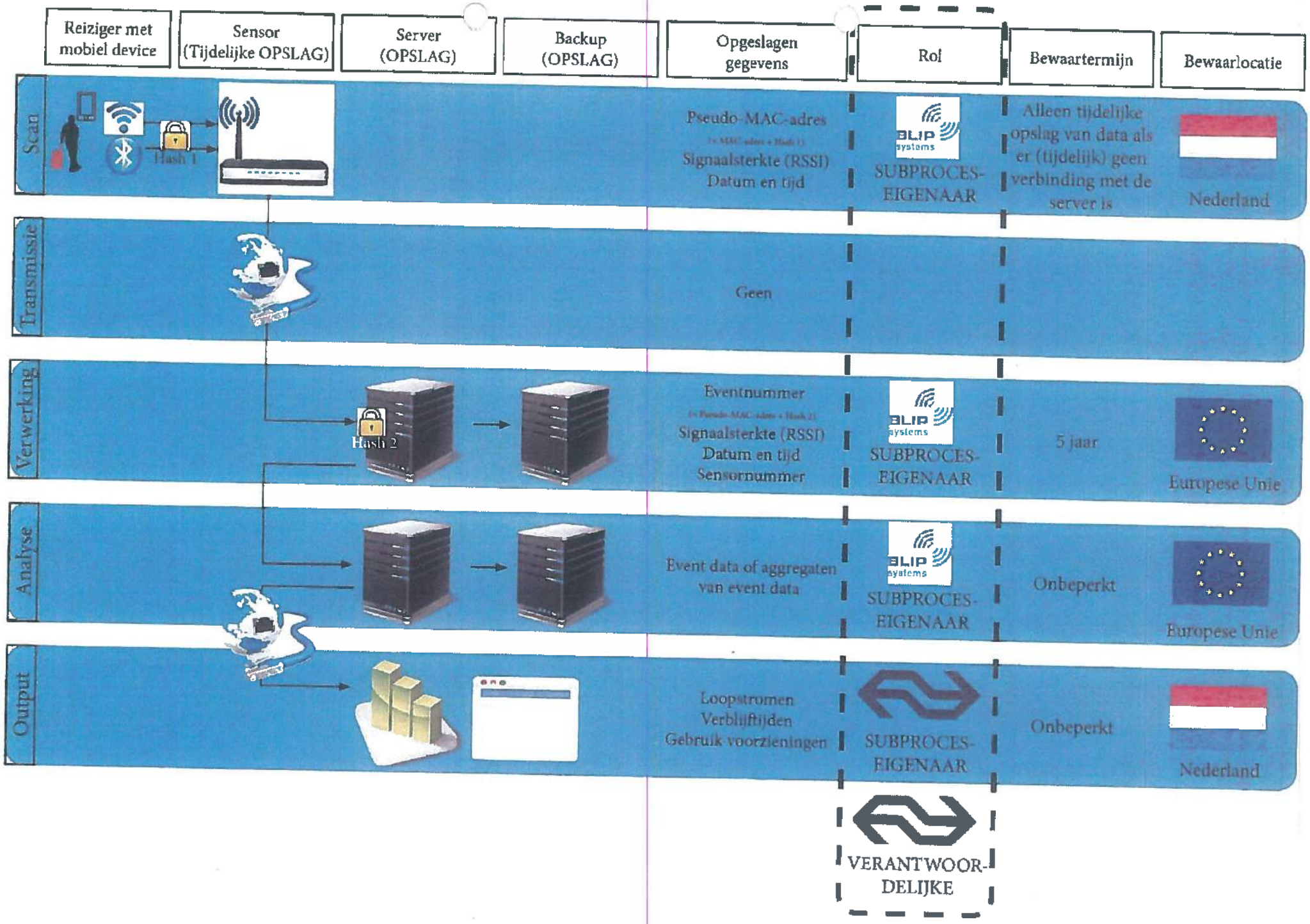
Een technische beschrijving van de hashing (salt) heb ik opgevraagd bij onze leverancier BLIP Systems. Zodra ik deze beschikbaar heb, ontvangt u een afschrift.

Als u in de tussentijd vragen of opmerkingen heeft, kunt u vanzelfsprekend contact met [redacted] of mij opnemen. Tenslotte wijs ik u graag op een interview met mij van vanmorgen dat vanmiddag om 16.00 uur op BNR Nieuwsradio wordt uitgezonden. In dit interview komen de onderwerpen doelmatigheid en privacy uitvoerig aan de orde.

Met vriendelijke groet,

[redacted]

Stationsontwikkelaar
NS Stations


Reiziger met mobiel device
Sensor (Tijdelijke OPSLAG)
Server (OPSLAG)
Backup (OPSLAG)
Opgeslagen gegevens
Rol
Bewaartermijn
Bewaarlocatie
Scan
Hash 1
Pseudo-MAC-adres
Signaalsterkte (RSSI)
Datum en tijd
SUBPROCES-EIGENAAR
Alleen tijdelijke opslag van data als er (tijdelijk) geen verbinding met de server is
Nederland
Transmissie
Geen
Verwerking
Hash 2
Eventnummer
Signaalsterkte (RSSI)
Datum en tijd
Sensornummer
SUBPROCES-EIGENAAR
5 jaar
Europese Unie
Analyse
Event data of aggregaten van event data
SUBPROCES-EIGENAAR
Onbeperkt
Europese Unie
Output
Loopstromen
Verblijftijden
Gebruik voorzieningen
SUBPROCES-EIGENAAR
Onbeperkt
Nederland
VERANTWOOR-DELIJKE

PRIVACY & COMPLIANCE

TIJDSCHRIFT VOOR DE PRAKTIJK

03/2013

Baltzer Science Publishers

ISSN 2211-3754

COLOFON

Privacy & Compliance
Baltzer Science Publishers
Tel +31 6 53 88 1502
info@baltzersciencepublishers.com
www.baltzersciencepublishers.com

Abonnementsprijs
2013, Jaargang 2, 1-6, € 175,00 excl. BTW, incl. verzendkosten (in Nederland). De prijs is exclusief online toegang, voor online toegang en meerdere gebruikers is een prijsmodel te raadplegen op de website: http://www.baltzersciencepublishers.com/nl/general/bestelformulier

Nieuwe abonnementen
Abonnementen kunnen worden gestart per 1 januari van een kalenderjaar. Valt de aanvraag van een abonnement niet samen met het begin van een kalenderjaar, dan worden de reeds verschenen nummers van dat kalenderjaar alsnog verzonden en wordt de prijs van een volledige jaargang in rekening gebracht. Nieuwe abonnementen kunnen schriftelijk, per fax, per telefoon of per email worden opgegeven.

Adreswijziging
Bij adreswijziging wordt u verzocht deze zo spoedig mogelijk en bij voorkeur schriftelijk door te geven aan de uitgeverij onder vermelding van: adreswijziging Privacy & Compliance.

Beëindiging abonnement
Abonnementen kunnen alleen schriftelijk, tot 1 december van het lopende abonnementsjaar, worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch voor een kalenderjaar verlengd.

ISSN: 2211-3754 · E-ISSN: 2211-3762

Baltzer
Science
Publishers

INHOUDSOPGAVE

PRIVACY BY DESIGN BIJ REIZIGERSMETINGEN OP STATIONS

*Jeroen van den Heuvel, Eelco Thiellier, Niels van Gerwen**

In maart van dit jaar ontstond discussie over het tracken en tracen van reizigers op het station van Groningen met behulp van het volgsysteem SMART Station. De projectvoerders geven uitleg over de intrinsieke privacybescherming van het systeem. SMART Station wordt binnenkort ingezet op Utrecht CS en krijgt daarna ook bredere toepassing.

Het belang van reizigersmetingen op stations

Aantrekkelijk openbaar vervoer is belangrijk voor de kwaliteit van wonen, werken, ondernemen en recreëren in Nederland. Vervoer per trein neemt hierbij een belangrijke positie in omdat de trein een aantrekkelijk en duurzaam alternatief is voor de auto, en – op Europese schaal – ook voor het vliegtuig. Het voordeel van reizen per openbaar vervoer is de mogelijkheid om de tijd onderweg te gebruiken voor andere activiteiten, zoals werken, lezen of slapen.
De achilleshiel van reizen per openbaar vervoer is de keten van verschillende vervoerwijzen waarmee de reiziger van deur tot deur reist. De reiziger moet altijd een rit maken naar een halte of station, om vervolgens met bus, tram, metro of trein het grootste deel van de totale reisafstand te overbruggen. Op de bestemming aangekomen, is meestal nog een rit naar de eindbestemming nodig. Tussen deze verschillende schakels in de keten moet van de ene vervoerwijze op de andere worden overgestapt. In veel gevallen gebeurt deze 'transfer' op en rond treinstations. Wetenschappelijk onderzoek toont aan dat de transfer op knooppunten door de reiziger verreweg als zwakste schakel in de reisketen van deur tot deur wordt ervaren.[1] Hoewel er de laatste jaren op stations al veel vooruitgang is geboekt, ligt hier dus nog steeds de kans om het reizen per openbaar vervoer naar een structureel hoger niveau te tillen.

Meten is weten

Het begrijpen van het functioneren van het station, het stationsgebied en het gedrag van reizigers hierbinnen, is cruciaal voor het verbeteren van die noodzakelijke schakel in de reisketen. Met inzicht in de werking van stations kunnen deze beter ontworpen worden, en kan de dienstverlening op het station beter worden afgestemd op de behoefte van reizigers. Op deze manier kunnen reizigers ook bij grote drukte – het gaat al snel om duizenden mensen tegelijk – comfortabeler en veiliger van stations gebruik maken.
Inzicht in aantallen, looptijden en wachttijden is belangrijk voor de inrichting van transfervoorzieningen zoals roltrappen, trappen, deuren, perrons en passages. Inzicht in aantallen is niet alleen belangrijk voor reguliere situaties – bijvoorbeeld een ochtendspits op een drukke maandag – maar is ook belangrijk voor bijzondere situaties zoals bij verstoring van de dienstregeling of evenementen waarbij honderdduizenden reizigers in korte tijd naar of van een stad willen reizen. Bijvoorbeeld tijdens Koningsdag of de Nijmeegse Vierdaagse. Inzicht in looproutes van passanten is essentieel voor een goed aanbod van diensten in en rond het station, zoals ticketing, reisinformatie en retail. Kortom: meten is weten.

Onze uitdaging

Tot voor kort bestonden passantenmetingen op stations in Nederland alleen uit handmatige tellingen en enquêtes, die meestal werden uitgevoerd door studenten. Een dergelijke aanpak heeft twee grote nadelen. Ten eerste is het een zeer kostbare aangelegenheid omdat een groot aantal mensen nodig

* **Jeroen van den Heuvel** is stationsontwikkelaar bij NS Stations en doet promotieonderzoek aan de Technische Universiteit Delft. **Eelco Thiellier** en **Niels van Gerwen** zijn consultants bij NPC, onderdeel van Royal HaskoningDHV. NPC is het projectmanagement- en adviesbureau voor NS, ProRail en regionale vervoerders voor (her)ontwikkeling van stationsgebieden.

1 Zie bijvoorbeeld *Waiting Experience At Train Stations*, door Mark van Hagen (ISBN: 9789059725065)

SMART Station concept

is om de telling uit te voeren. Voor een middelgroot station zijn tientallen medewerkers tegelijk nodig om een goed beeld te krijgen van alle loopbewegingen. Voor een groot station loopt dit al snel op tot vijftig of meer.
Ten tweede is de waarde van ingewonnen informatie beperkt, omdat vanwege de hoge kosten de duur van de tellingen wordt beperkt tot één of enkele dagen. Hierdoor is de statistische betrouwbaarheid van de gegevens beperkt, omdat een specifieke dag flink kan afwijken van het gemiddeld patroon of de situatie bij bijvoorbeeld verstoringen of evenementen.

Wij stonden voor de uitdaging was om een methode te bedenken waarmee op geautomatiseerde wijze passantenstromen op stations over een langere periode inzichtelijk kunnen worden gemaakt.

Bluetooth-tellingen

In het wetenschappelijk en praktisch onderzoek naar voetgangers zijn de laatste jaren diverse ontwikkelingen gaande, die in principe ook voor stations bruikbare instrumenten opleveren. Zo is het geautomatiseerd meten van verkeerstromen in andere vervoersectoren al veel langer gemeengoed, waarbij het opvangen van Bluetoothsignalen uit smartphones en tablets een belangrijke rol speelt om dubbeltellingen te voorkomen.

- Op veel wegen wordt het aantal auto's en hun snelheid gemeten door middel van detectielussen in het wegdek en/of videocamera's langs of boven de weg. Met behulp van Bluetoothmetingen worden routetijden bepaald, die vervolgens voor verkeerskundig onderzoek worden gebruikt of op de grote informatiepanelen langs of boven de weg wordt getoond.[2]

- Op luchthavens worden met behulp van Bluetooth wachtrijen en wachttijden bij de douane gemeten, en worden de looproutes en verblijftijd van passanten gemeten om het winkelaanbod hierop af te stemmen.[3]

- In binnensteden is inzicht in bewegingspatronen belangrijk om problemen op het gebied van infrastructuur en voorzieningen op te lossen of te voorkomen. Ook hiervoor worden sinds kort Bluetoothmetingen ingezet.[4]

Hoewel de technologie voorhanden is om passantenstromen nauwkeurig te meten, bleek deze niet zonder meer geschikt voor stations. Ten eerste omdat passantenstromen op stations kortstondig zó intensief kunnen zijn – meer dan tienduizend passanten per uur via één passage – dat de bestaande technologie te kort schiet om bruikbare meetresultaten leveren. Sommige bestaande systemen kunnen de reizigers letterlijk niet meer bijhouden zodra de spits begint. En juist op de drukke momenten zijn de meest nauwkeurige gegevens nodig om een station goed te kunnen ontwerpen en laten functioneren.
Ten tweede omdat een station als een groot plein functioneert, waarbij veel verschillende stromen passanten samenkomen en kriskras door elkaar bewegen. Auto's op een weg blijven binnen de witte lijnen, fietsers blijven (meestal) op het fietspad of de weg, en passanten in een binnenstad zijn altijd wel toe te wijzen aan een specifieke straat. Op stations zijn voetgangers veel vrijer, waardoor het bijzonder lastig is om achterhalen welke passant welke route precies heeft gelopen.

Na een flinke zoektocht hebben we vastgesteld dat er voor stationsmetingen niet meteen panklare oplossingen bestonden.

2 Zie bijv. http://www.verkeerskunde.nl/bluetooth
3 Zie bijv. http://www.futuretravelexperience.com/2012/11/houston-airports-adopt-bluetooth-based-queue-measurement/
4 Zie bijv. http://www.bk.tudelft.nl/over-faculteit/afdelingen/urbanism/onderzoek/urbanism-on-track/sensing-the-city/project/

Onze oplossing: SMART Station

Om een geschikte oplossing te ontwikkelen hebben NS Stations en NPC – dochter van RoyalHaskoningDHV – de handen ineen geslagen en in één jaar tijd een volledig nieuwe oplossing ontwikkeld: SMART Station. Bij SMART Station worden meerdere meetsystemen tegelijkertijd ingezet. Deze tellen en registreren reizigersbewegingen, en verwerken dit automatisch tot een totaalbeeld van een actuele situatie op en/of rond het station. Op die manier wordt de informatie verkregen die nodig is voor het ontwerp, evaluatie of management van stations.

SMART Station bestaat uit meerdere modules:

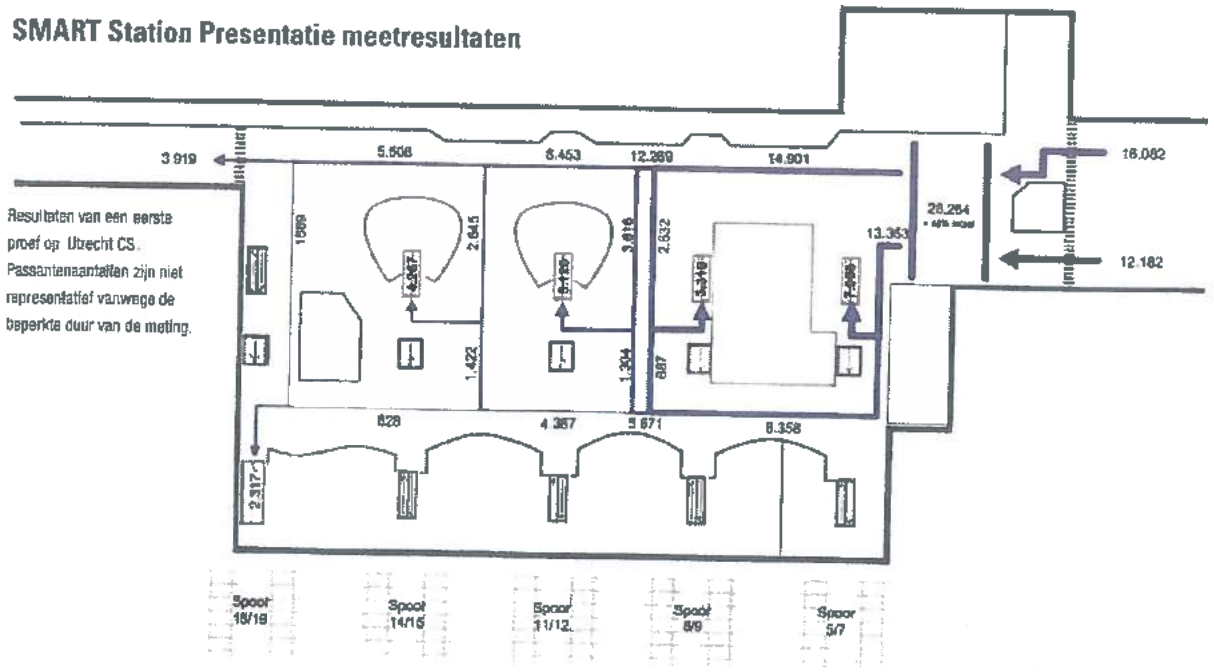
- tel- en volgmodules;
- een analysemodule;
- en een presentatiemodule.

Tellen gebeurt met behulp van infraroodtechnologie. Volgen gebeurt door op verschillende plaatsen in een station, de MAC-adressen (unieke hardwarenummers) van Bluetooth- en WIFI-devices op te vangen. Door de sensoren strategisch te plaatsen, kan aan de hand van de MAC-adressen, detectietijdstippen en de plaats van sensoren een reconstructie worden gemaakt van de looproute van een passant, en hoe lang deze passant over deze route heeft gedaan.
Omdat niet iedereen een Bluetooth/WIFI-device op zak heeft, zijn telefoon uit heeft staan of Bluetooth en/of WIFI niet heeft ingeschakeld om de batterij te sparen, worden de gegevens van de volgsensoren door de analysemodule gecombineerd met de gegevens uit de telsensoren. Op die manier kan met behulp van de presentatiemodule op ieder willekeurig moment een totaalbeeld van de reizigersstroom op een station worden verkregen (zie afbeelding).

Privacyoverwegingen

Omdat SMART Station *mensen*stromen in kaart brengt, is bij de ontwikkeling van het systeem steeds rekening gehouden met de privacybescherming van passanten. Om deze reden zijn we vroeg in het ontwikkelproces van SMART Station samen met gespecialiseerde adviseurs en juristen dieper in de materie gedoken om SMART Station privacyproof te ontwerpen.
Om privacyredenen worden MAC-adressen niet geregistreerd in combinatie met gegevens over de eigenaar/gebruiker van apparatuur. Het SMART Station-systeem 'ziet' alleen nummers om passanten op een anonieme manier te kunnen onderscheiden. Meer informatie heeft SMART Station niet nodig. Gebruikers van SMART Station kunnen die nummers niet gebruiken voor identificatie. Zuiver wettelijk werkt het systeem dan ook niet met 'persoonsgegevens' in de zin van de Wet Bescherming Persoonsgegevens.
We vonden en vinden echter dat onze verantwoordelijkheid verder gaat dan de wet. Stations staan vaak midden in de stad en worden door miljoenen mensen bezocht. Gebruikers van

SMART Station Presentatie meetresultaten



SMART Station zijn daarmee kwetsbaar voor negatieve maatschappelijke perceptie en hebben ook rekening te houden met de mogelijkheid van juridische discussie over 'persoonsgegevens' en wetgevingsontwikkelingen.

Privacy by Design

Om de oplossing nog breder toepasbaar te maken – ook internationaal – hebben we besloten om het privacy aspect zo diep en goed mogelijk binnen SMART Station te verankeren. We hebben hierbij gebruik gemaakt van drie bronnen van inspiratie: de Wet Bescherming Persoonsgegevens, de Privacybeleidskaders van NS met de privacy officer van NS als hoeder hiervan, en ons eigen gezond verstand. Dit heeft geresulteerd in een concept 'informatiebeleidsplan' voor SMART Station, waarmee we het ontwerptraject zijn ingegaan. Het informatiebeleidsplan beschrijft op welke wijze privacy gewaarborgd wordt in de technologie, processen en organisatie van SMART Station, dus op drie niveaus tegelijkertijd.
We hebben dit getoetst op een vroeg prototype van SMART Station middels een privacy audit door externe privacy specialisten. De aanbevelingen van deze audit hebben we doorgenomen met de privacy officer van NS, en vervolgens doorgevoerd in zowel het informatiebeleidsplan als het vervolg van het ontwerptraject.

De door ons gekozen weg komt overeen met het principe van *Privacy by Design*. De basisgedachte daarbij is implementatie van privacy beschermende maatregelen vanaf de start van de ontwikkeling van een technologie tot en met het beëindigen van het gebruik van de technologie. Hierdoor wordt het privacy-aspect een integraal onderdeel van de technologie en de gebruiksprocessen, waardoor de gebruikers van de oplossing maximaal worden gedwongen dan wel gestimuleerd om privacybewuste keuzes te maken.

Drie niveau's

Zoals gezegd is de privacywaarborg op drie niveaus in SMART Station geïntegreerd:

1. **Op technisch niveau,** door gebruik van *Privacy Enhancing Technologies* (PET). Meest belangrijk is de onomkeerbare versleuteling van de door de telmodule ingewonnen MAC-adres gegevens ('one way-hashing'). Deze versleuteling vindt direct bij de sensor plaats op basis van 256 bit-encryptie. Door die conversie worden de originele gegevens meteen bij de bron alweer vernietigd. De versleuteling vindt bovendien plaats met gebruikmaking van datum-informatie. Hierdoor levert de conversie van hetzelfde MAC-adres, ieder dag weer een andere telcode op. Het is op die manier onmogelijk om aan de hand van meerdaagse metingen individuele profielen op te bouwen van terugkerende reizigers.

2. **Op proces-niveau.** De opslag van gegevens is in de tijd gelimiteerd. De telgegevens worden na analyse automatisch weggegooid. Ook is SMART Station met verschillende autorisatieniveaus uitgerust, waardoor alleen de mensen die met bepaalde gegevens mogen werken, daar ook bij kunnen. Privacy is daarnaast nog een selectiecriterium in het inkoopproces: leveranciers moeten door middel van referenties én een kleinschalige praktijktest aantonen dat ze volledig volgens het informatiebeleidsplan SMART Station werken.

3. **Op organisatie-niveau.** Hoewel we met de technologie en de processen alle voorzienbare issues hebben ondervangen, vonden we het belangrijk om ook aandacht te schenken aan de cultuur van de organisatie rond SMART Station. Medewerkers worden geïnformeerd over het informatiebeleidsplan. Hierdoor wordt de kans op problemen tot een minimum teruggebracht. Op bedrijfsniveau is afgesproken om iedere twee jaar een audit uit te voeren om te toetsen of alles conform het informatiebeleidsplan SMART Station verloopt, en zo niet, op welke wijze moet worden bijgestuurd. Bij gerede twijfel over zorgvuldig handelen door NS, NPC en/of de leveranciers kan de privacy officer van NS het systeem in het uiterste geval uit laten schakelen totdat knelpunten zijn opgelost.

Het resultaat van het ontwikkelproces is een meetconcept dat aantoonbaar zorgvuldig omgaat met gegevens over de reizigers in stations.

Resultaten tot nu toe en vervolgstappen

In het voorjaar van 2013 heeft NPC de definitieve versie van SMART Station in opdracht van ProRail voor het eerst toegepast. Aanleiding is het voornemen om station en stationsgebied van Groningen te verbeteren, waarvoor ProRail als spoorbeheerder de initiatiefnemer is. De resultaten van de metingen en de bruikbaarheid in de herontwikkeling van het station zien er veelbelovend uit.[5] Zo is uit de metingen duidelijk zichtbaar geworden welke voorkeuren reizigers hebben voor looproutes. De inzet van SMART Station trok veel media-aandacht, waardoor het concept ook wat het privacybelang van passanten betreft, de vuurdoop heeft doorstaan. De media-aandacht geeft maar aan dat we steeds alert moeten blijven op privacy.
Op dit moment is de toepassingen van SMART Station op station Utrecht Centraal in voorbereiding. Dit met het oog op de verbouwing, die in het najaar een fase ingaat waarbij de transferruimte tijdelijk kleiner moet worden gemaakt om ruimte te maken voor de bouwwerkzaamheden. SMART Station helpt ons aan de inzichten die nodig zijn om dat zo klantvriendelijk mogelijk te doen. Naast de toepassingen in operatie en projecten levert SMART Station veel gegevens voor wetenschappelijk onderzoek. Een van de auteurs promoveert aan de Technische Universiteit Delft op het ontwerp en management van de transferfunctie van stations.
Ook vanuit de markt worden de ontwikkelingen gevolgd. Vanwege de kwaliteit van de oplossing, de relatief lage kosten en toepassing van *Privacy by Design*, is er veel interesse vanuit diverse sectoren uit binnen- en buitenland. Voor NS en NPC is het de uitdaging om SMART Station tijdens de toepassing op stations en daarbuiten te blijven verbeteren. De ontwikkelingen in techniek gaan immers razendsnel. Dit biedt kansen om reizigersmetingen steeds sneller, slimmer en goedkoper uit te voeren. Privacy helpt niet alleen om alert te blijven op risico's en knelpunten, maar blijkt ook een *driver* voor innovatie.

Conclusie

Geconcludeerd kan worden dat inzicht in het functioneren stations cruciaal is voor het verbeteren van de totale reisbeleving van reizigers die van deur tot deur reizen en op de stations overstappen. Het meten van looproutes, looptijden, wachtplaatsen en reizigersaantallen vormt hiervoor de basis. Geautomatiseerde reizigersmetingen bieden vanwege de relatief lage kosten en de mogelijkheid voor continu meten, een zeer aantrekkelijk alternatief voor eenmalige tellingen door mensen. Hoewel geautomatiseerde tellingen in andere (vervoer)sectoren al veel langer gemeengoed is, bestond er vanwege de zeer grote aantallen voetgangersbewegingen in een grote vrije ruimte geen geschikte oplossing voor stations.
Daarom hebben wij SMART Station ontwikkeld.

Omdat het zeer belangrijk is dat zorgvuldig met de privacy aspecten van alle gebruikers van een station wordt omgegaan, is bij de ontwikkeling van dit meetconcept de *Privacy by Design* aanpak gehanteerd. Onderdeel hiervan is niet alleen de technologie, maar ook de processen en de organisatie. De resultaten van de eerste metingen zijn positief. De eerste maatschappelijke reactie op het privacybelang was kritisch maar positief. Ook in de toekomst zullen NS en NPC alert blijven en privacy een leidende factor laten zijn in de doorontwikkeling van SMART Station.

5 Zie: http://www.prorail.nl/Pers/Persberichten/Actueel/Regionaal/Pages/ProRailmeetreizigersstromenviamobieltje.aspx

AANKONDIGINGEN

Koen Versmissen

35th International Conference of Data Protection and Privacy Commissioners.
The Polish Inspector General for Personal Data Protection. Ma. 23 t/m do. 26 september 2013, Warschau.
http://www.giodo.gov.pl/259/id_art/762/j/en

Praktijkcursus Wet Bescherming Persoonsgegevens.
Euroforum. Di. 3, 10 en (optioneel) 24 september 2013, Utrecht. € 1799; leden NVvIR en VPR € 1.499 (excl. btw).
Trainers: Gerrit-Jan Zwenne, Bart Schermer, Jeroen Terstegge, Jeroen Koëter.
http://www.euroforum.nl/juridisch/cursus-wet-bescherming-persoonsgegevens/

The 4th Annual European Data Protection and Privacy Conference.
Forum Europe. Di. 17 september 2013, Brussel. €150.
Sprekers o.a. Viviane Reding, Jan-Philipp Albrecht, Christopher Graham.
http://www.eu-ems.com/summary.asp?event_id=147

Masterclass Europese Privacy Verordening.
Studiecentrum voor Bedrijf en Overheid. Di. 24 september, Utrecht. € 699 (excl. btw).
Docenten: Gerrit-Jan Zwenne, Jeroen Terstegge, Quinten Kroes.
http://www.sbo.nl/overheid/cursus-wet-bescherming-persoonsgegevens-andere-privacywetgeving-/#masterclass

---

Training Privacy Impact Assessment voor beleidsambtenaren.
De Privacypraktijk & Martijn van der Veen Consultancy. Vr. 27 september 2013, Utrecht of Den Haag.
€ 695 (excl. btw). Docenten: Koen Versmissen & Martijn van der Veen.
http://www.deprivacypraktijk.nl/training-pia-voor-beleidsambtenaren

---

Postdoctorale Specialisatiecursus Privacy en Persoonsgegevens.
Tilburg Institute for Law, Technology, and Society / De Brauw Blackstone Westbroek / Nederland ICT.
Vr. 27 september, 4 oktober, 1 en 15 november 2013, Tilburg. € 2750.
Docenten: Corien Prins, Lokke Moerel, Peter van Schelven.
http://www.nederlandict.nl/Files/TER/Programme_%20cursus_Privacy_en_Persoonsgegevens_2013.pdf

---

Training Privacy en Wet Bescherming Persoonsgegevens.
NIBE-SVV / De Privacypraktijk. Wo. 2 oktober 2013, Amsterdam. € 706 (vrij van btw). Trainer: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20en%20Wet%20Bescherming%20Persoonsgegevens

---

Training Privacy van Werknemers.
NIBE-SVV / De Privacypraktijk. Wo. 9 oktober 2013, Amsterdam. € 706 (vrij van btw). Trainer: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20van%20werknemers

Training Privacy en Internet.
NIBE-SVV / De Privacypraktijk. Ma. 28 oktober 2013, Amsterdam. € 808 (vrij van btw).
Trainer: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20en%20internet

Training Privacy in de Praktijk.
NIBE-SVV / De Privacypraktijk. Ma. 4 november 2013, Amsterdam. € 503 (vrij van btw).
Trainer: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20in%20de%20praktijk

Training Wet Bescherming Persoonsgegevens.
PBLQ ROI. Do. 7 november 2013, Den Haag. € 790 (vrij van btw).
http://www.pblq.nl/roi/opleidingen/2013/beleids-en-bestuurskunde/bestuursrecht/wet-bescherming-persoonsgegevens

Cursus Privacy Compliance Actualia.
NIBE-SVV / De Privacypraktijk. Ma. 11 november 2013, Amsterdam. € 706 (vrij van btw).
Docent: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20Compliance%20Actualia

Privacy Compliance Masterclass.
NIBE-SVV / De Privacypraktijk. Ma. 11, 18 en 25 november 2013, Amsterdam. € 1925 (vrij van btw).
Docent: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20Compliance%20Masterclass

Basiscursus Wet Bescherming Persoonsgegevens.
Universiteit Leiden, Juridisch Post Academisch Onderwijs. Do. 21 en 28 november 2013, Leiden.
€ 1495 (vrij van btw). Docenten: Peter Blok, Jeroen Koëter, Gerrit-Jan Zwenne.
http://www.paoleiden.nl/cms2/index.php?option=com_content&view=article&id=565

Privacy Compliance Professional Sessiedagen.
NIBE-SVV / De Privacypraktijk. Najaar 2013. € 1995 (indicatief; vrij van btw).
Docenten: Koen Versmissen + gastdocenten. Programma wordt samengesteld in overleg met de deelnemers.
http://www.nibesvv.nl/Opleidingen/Privacy%20Compliance%20Professional%20%20sessiedagen

Het National Privacycongres.
Kluwer Opleidingen. Vr. 22 november 2013, Amsterdam.
Sprekers o.a. Lokke Moerel, Hester de Vries, Gerrit Jan Zwenne. € 795.
http://www.kluwershop.nl/opleidingen/details.asp?pr=16058

IAPP Europe Data Protection Congress 2013.
International Association of Privacy Professionals. Di. 10 t/m do. 12 december 2013, Brussel.
https://www.privacyassociation.org/events_and_programs/iapp_europe_data_protection_congress_2013

www.nibesvv.nl

TE MAKEN MET PRIVACYEISEN?

VOORBEREIDEN OP DE PRIVACYVERORDENING VAN DE EU?

NIBE-SVV biedt u dit najaar weer verschillende privacytrainingen: Privacy compliance masterclass, Privacy compliance professional sessiedagen, Privacy compliance actualia, Privacy in de praktijk, Privacy en internet, Privacy en Wet bescherming persoonsgegevens en Privacy van werknemers.

NIBE SVV
HET KENNISINSTITUUT VAN DE FINANCIËLE WERELD

De trainingen reiken u handvatten aan om te kunnen voldoen aan de huidige privacywetgeving en om u voor te bereiden op de nieuwe privacyverordening van de EU. NIBE-SVV biedt de trainingen aan in samenwerking met het gerenommeerde advies- en trainingsbureau De Privacypraktijk.

SUCCES DOEN WE SAMEN

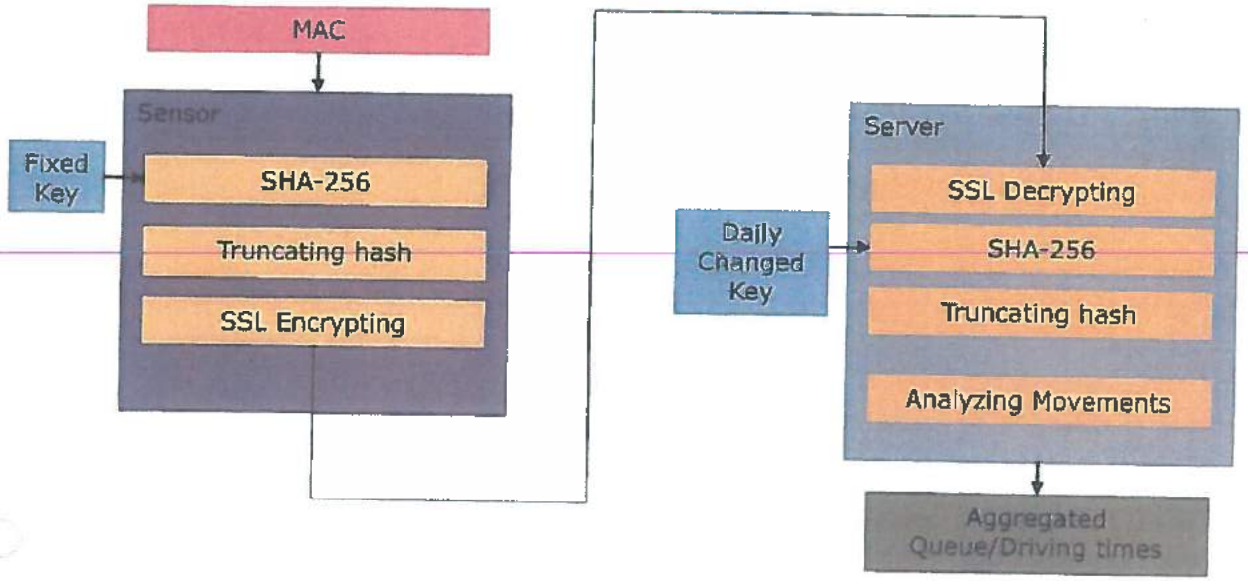
Van: [redacted](STV) [mailto[redacted]@nsstations.nl]
Verzonden: woensdag 14 juni 2017 14:19
Aan: [redacted] drs. [redacted]
CC: [redacted](NSG)
Onderwerp: Re: Inlichtingen over WifFi-Tracking

Geachte heer [redacted], mevrouw [redacted]

In aanvulling op het onderstaande bericht vindt u in de bijlage de door BLIP Systems geleverde informatie over de methode van (dubbele) hashing. Ik hoor het graag als u vragen heeft.

Hartelijke groeten,
[redacted]

Privacy



BLIP systems

BlipTrack uses a SHA-256 algorithm in the BlipNode (Bluetooth/Wi-Fi sensor) to generate a one way hash code of the tracked device's MAC address. Only truncated hash-codes are transmitted to the central server. There is no way to revert the truncated hash codes back to real MAC addresses.

The rehashing in the BlipTrack server is made at the time data is received from the BlipNode, so the truncated hash-code from the sensor is not stored.

The rehashing works by encrypting the truncated hash-code from the sensor using SHA-256 with a SALT which is changed on a daily basis at a predefined time of day e.g. at 04:00. The rehashing is implemented to prevent identification of returning passengers by combining tracking data with other sources of data such as CCTV.

The now twice hashed and truncated code is stored in the database.

This code is impossible to track over multiple days, as well as being impossible to relate to a real MAC-address.

Van: [redacted] drs. [redacted]@autoriteitpersoonsgegevens.nl>
Verzonden: woensdag 14 juni 2017 14:27
Aan: [redacted](STV);[redacted]
CC: [redacted](NSG)
Onderwerp: RE: inlichtingen over WifFi-Tracking

Geachte heer[redacted]

Dank u voor deze twee slides van Bliptrack. De relevante zinsnede: "*The rehashing works by encrypting the truncated hash-code from the sensor using SHA-256 with a SALT which is changed on a daily basis at a predefined time of day e.g. at 04:00*" geeft echter nog geen antwoord op de vraag:

Hoe wordt de salt samengesteld? U gaf telefonisch aan dat hiervoor de datum wordt gebruikt?

Wij horen graag van u.

Hoogachtend,
Autoriteit Persoonsgegevens,

Namens deze,
[redacted]en[redacted]

[redacted]
Senior Supervision Officer

AUTORITEIT
PERSOONSGEGEVENS

[redacted]@autoriteitpersoonsgegevens.nl
T 070 8888 500 - F 070 8888 501
M 06 25 69 19 88
Bezuidenhoutseweg 30, 2595 AJ The Hague, The Netherlands
P.O.Box 93374, 2509 AJ The Hague, The Netherlands
autoriteitpersoonsgegevens.nl

Van: [redacted](STV) <[redacted]@nsstations.nl>
Verzonden: woensdag 14 juni 2017 15:15
Aan: [redacted], drs[redacted]
CC: [redacted](NSG)
Onderwerp: Re: inlichtingen over WifFi-Tracking

Geachte heer[redacted], mevrouw[redacted]

Zojuist heb ik aan BLIP gevraagd om een technische beschrijving te leveren van de wijze waarop de hash 2 (cf. het schema) wordt toepast; met in het bijzonder de wijze waarop wordt gezorgd dat deze hash iedere dag anders is (verwijzend naar mijn uitspraak "daghash" of "datumhash").

Wordt zo snel mogelijk vervolgd. Hartelijk dank voor uw geduld.

Met vriendelijke groet,

[redacted]

[redacted] drs. [redacted]

Van: [redacted] (STV) [redacted]@nsstations.nl>
Verzonden: woensdag 14 juni 2017 16:01
Aan: [redacted] drs. [redacted]
CC: [redacted]
Onderwerp: Re: inlichtingen over WifFi-Tracking

Geachte heer [redacted] mevrouw [redacted]

Omdat het antwoord zeer technisch is en ik (als niet encryptie-specialist) geen ruis wil veroorzaken, begin ik met een letterlijke weergave van de reactie van BLIP Systems (cursief).

We use the SHA-256 algorithm to do the actual encryption:
http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

It is implemented using:
* `java.util.Random`
* `java.security.MessageDigest`

The daily new salt is generated like this:

```
private byte[] currentSalt = new byte[8];
new Random().nextBytes(currentSalt);
```

And for each `truncatedHashFromBlipNode` *received from the BlipNodes we do like this:*

```
MessageDigest md = MessageDigest.getInstance("SHA-256");
md.update(currentSalt);
md.update(truncatedHashFromBlipNode);

byte[] digest = md.digest();
System.arraycopy(digest, digest.length - 8, truncatedDigest, 0,
truncatedDigest.length);
```

—

We end up storing the `truncatedDigest`
(which is a hash and truncate of the original MAC address, and then a hash and truncate again).
—

In mijn, iets meer beleidsmatige woorden gebeurt het volgende:
1. Een MAC adres wordt in het werkgeheugen van de sensor gehashed door middel van een SHA-256 encryptie, waarbij na hashing 8 bits van het (gepseudonimiseerde) nummer worden verwijderd ("truncated");
2. De uitkomst wordt via een SSL-verbinding naar de server gestuurd;
3. Bij binnenkomst wordt de uitkomst van 1. in het werkgeheugen van de server nogmaals gehashed met een SHA-256 encryptie. Dit keer is de hash gebaseerd op een getal dat iedere dag random wordt getrokken. Na deze hash worden wederom 8 bits van het (geanonimiseerde) nummer verwijderd ("truncated");
4. De uitkomst van 3. is het eventnummer waarnaar in het door mij aangeleverde stroomschema onder "Processing" wordt verwezen. Dit eventnummer wordt in de server opgeslagen bij de bijbehorende sensor-ID (plek), datum/tijd en signaalsterkte (RSSI);
5. Op de server wordt het random getal iedere dag om 4.00 uur door een nieuw, random getrokken getal vervangen. Deze getallen worden nergens opgeslagen of gelogd. Hierdoor kan zelfs met een bekend MAC-adres na een dag al niet meer worden bepaald of het betreffende device op het station is geweest.

Hopelijk vult dit antwoord uw informatiebehoefte inzake de wijze van hashing in.

Met vriendelijke groet,

AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
NS
T.a.v. de FG, de heer [redacted]
Postbus 2572
3500 GN Utrecht

Datum
7 juli 2017

Ons kenmerk
z2017-05365

Contactpersoon
Mw. drs. [redacted]
070 8888 500

Onderwerp
Wifi en bluetooth tracking NS stations

Geachte heer [redacted]

De Autoriteit Persoonsgegevens (AP) heeft persvragen ontvangen over bluetooth- en wifi-tracking op NS-stations. Naar aanleiding van die vragen heeft de AP op woensdag 14 juni 2017 telefonisch contact opgenomen - via uw afdeling woordvoering - met de NS projectmanager wifi-tracking, de heer [redacted] Heuvel. De heer [redacted] heeft op 14 juni met meerdere e-mails een nadere toelichting gegeven op de technische werking van het systeem. De AP heeft in het gesprek aangegeven schriftelijk te zullen reageren. Met deze brief stelt de AP u nadere vragen.

Verklaringen NS

De heer [redacted] heeft tijdens het gesprek, en via de e-mails, de volgende informatie verstrekt.

- De NS doet bluetooth- en wifi-tracking op stations sinds 2012.
- De NS maakt gebruik van de diensten van het Deense bedrijf Bliptrack.[1] De NS heeft een bewerkersovereenkomst gesloten met Bliptrack waarin gebruik door Bliptrack van de verzamelde gegevens voor eigen doeleinden is uitgesloten.
- Het doel is anonieme passagiersstromen in kaart te brengen. Dit gebeurt soms als experiment bij de inrichting van nieuwe stations of de verbouwing van bestaande stations om te kijken hoe je bijvoorbeeld de roltrap het beste kunt plaatsen of waar je de winkels het beste kunt plaatsen. Meestal wordt de tracking ingezet om te tellen hoeveel mensen er in en uit een station gaan (loopstroomtelling), op een perron staan, of zich op andere plekken/doorgangen in het station bevinden (crowd management). De NS gebruikt de tracking ook om te meten hoeveel mensen van

[1] Dit Deense bedrijf is onlangs overgenomen door het bedrijf Gentrack. Zie het persbericht van Bliptrack van 3 mei 2017, URL: http://blipsystems.com/blip-systems-becomes-part-of-gentrack-to-boost-software-range/.

station A naar station B reizen. Ten slotte gebruikt de NS de tracking om op grond van tellingen op specifieke perrons van station Schiphol te voorspellen hoeveel mensen er in Amsterdam Centraal Station worden verwacht.

- De NS gebruikt de OV-chipkaartgegevens om statistisch te tellen hoeveel mensen er in en uit de stations gaan. Daarnaast gebruikt de NS twee stereocamera's op de perrons 1 en 2 van station Schiphol voor anonieme tellingen van het aantal personen op deze perrons.
- De NS informeert over de tracking via een bordje/sticker bij de ingang van stations, op de plek waar ook over cameratoezicht wordt geïnformeerd, en waar de huisregels van het station hangen. De NS heeft in haar privacyverklaring een alinea opgenomen over wifi- en bluetooth-tracking.[2] Daarnaast heeft de NS onlangs actief de pers geïnformeerd over de aanwezigheid van tracking.
- De NS biedt geen opt-outmogelijkheid voor tracking. Personen die niet getrackt willen worden, kunnen de wifi- en bluetoothfunctionaliteit van hun telefoon uitschakelen. De NS wil niet via een opt-out alsnog persoonsgegevens verzamelen.
- De NS past (via technologie van, en op servers van, het bedrijf Bliptrack) een *hashing methode* toe op de verzamelde MAC-adressen. Een MAC-adres (Media Access Control adres) is een vrijwel unieke reeks (meestal in hexadecimale vorm) die, toegekend aan een apparaat (een smartphone, tablet of computer), dat apparaat identificeert en het mogelijk maakt dat apparaten in een ethernetnetwerk met elkaar kunnen communiceren. De *hash* wordt op alle stations in Nederland (waar deze tracking plaatsvindt) op dezelfde manier berekend.
- De MAC-adressen worden op de sensoren *gehasht*, waarbij de laatste 8 bits van de *hash* van het MAC-adres worden verwijderd (*truncated*) en dan naar de server gestuurd. Daar worden ze voor de tweede keer *gehasht*, met een *salt*. Een *salt* is een nummer dat aan de *hash* wordt toegevoegd, om de uitkomsten van de *hash* onvergelijkbaar te maken met eerdere *hashes* van hetzelfde MAC-adres waarbij een andere *salt* is gebruikt. De NS genereert de *salt* door een standaard *java random number generator*, met een *seed* die gebaseerd is op de datum/tijd. Na deze tweede *hash* worden opnieuw de laatste 8 bits van de *hash* verwijderd.
- De *salt* wordt niet gelogd, en na 24 uur verwijderd.
- De NS noemt de *gehashte* MAC-adressen op de server 'eventnummers'. Deze nummers worden opgeslagen met de bijbehorende sensor-ID (plek), datum/tijd en signaalsterkte (RSSI).
- De NS bewaart de gegevens gedurende 5 jaar, om de drukte op stations, de loopstromen en reispatronen door de tijd heen te kunnen vergelijken.

Vragen AP

De AP maakt uit deze informatie op dat u geen toestemming vraagt van betrokkenen voor de verwerking van persoonsgegevens. Aangezien de overige grondslagen niet van toepassing lijken te zijn, neemt de AP aan dat u een beroep doet op de grondslag van artikel 8, onder f, van de Wbp. Om te kunnen beoordelen of de NS de gegevens voor gerechtvaardigde doeleinden verzamelt, of de gegevensverwerking voldoet aan de noodzakelijkheidsvereisten en of het gerechtvaardigd belang van de NS opweegt tegen het recht van betrokkenen op bescherming van hun persoonlijke levenssfeer, verzoekt de AP u om nadere informatie en bescheiden.

[2] NS privacyverklaring, URL: http://www.ns.nl/privacy.html.

1. Verstrek een afschrift van de (gedateerde en gesigneerde) overeenkomst met Bliptrack. U mag hierin desgewenst de financiële gegevens zwart maken.
2. Verstrek een afschrift van interne besluitvorming over het gebruik van wifi- en bluetooth tracking door de NS, bijvoorbeeld e-mailcorrespondentie met goedkeuring van het plan door de directie, waaruit blijkt dat de NS sinds 2012 bluetooth en wifi tracking toepast. Indien u bij aanvang van deze metingen gebruik hebt gemaakt van de diensten van een andere partij, verstrek een afschrift van de (gedateerde en gesigneerde) overeenkomst met deze partij. Indien de genoemde bescheiden niet beschikbaar zijn, verstrek andere schriftelijke bescheiden waaruit blijkt dat de NS hiertoe in 2012 heeft besloten.
3. U schrijft op de website http://www.stations.nl/beleid/privacy "*ProRail en NS Stations verbeteren de dienstverlening op en rond het station continu.*" Verkrijgt ProRail toegang tot de tracking-gegevens? Zo ja, is ProRail samen met de NS verantwoordelijk voor de gegevensverwerking? Ontvangt ProRail gegevens die gegenereerd worden door de tracking? Zo ja, in welke vorm (ruwe data of geaggregeerde gegevens?)
4. De AP maakt uit de website http://www.stations.nl/beleid/privacy op dat er op dit moment sprake is van tracking op zes stations, namelijk: Amsterdam Centraal, Leiden Centraal, Amsterdam Zuid, Utrecht Centraal, Schiphol Airport en 's Hertogenbosch. Uit de mondelinge toelichting bleek dat er ook tijdelijke tracking is toegepast op sommige locaties. Verstrek een overzicht van alle locaties waar de NS wifi en/of bluetooth tracking toepast (of heeft toegepast) sinds 2012, inclusief alle stations waar deze tracking alleen tijdelijk heeft plaatsgevonden. Indien u concrete plannen hebt om het aantal permanente locaties uit te breiden in het komende jaar, verstrek ook een overzicht van deze planning.
5. Sinds wanneer informeert u de bezoekers van stations over de wifi-tracking? Verstrek een overzicht per station van de manier waarop u informeert, en sinds wanneer u deze informatie verstrekt.
6. Verstrek een limitatief overzicht van de doeleinden waarvoor de NS (1) de ruwe en (2) de gehashte tracking-gegevens (heeft) verwerkt.
7. De NS biedt op sommige stations (in ieder geval in de *International Lounges* en op de flex werkplekken[3]) en in sommige treinen publieke gratis wifi-toegang aan.[4] Worden, bij het gebruik hiervan, de MAC-adressen van apparaten van de gebruikers vastgelegd? Zo nee, geef een limitatieve opsomming welke gegevens eventueel wel worden vastgelegd. Zo ja, welke organisatie heeft/organisaties hebben/ deze gegevens in beheer, en wat is de bewaartermijn van deze gegevens? Indien de NS een overeenkomst hiervoor heeft met één of meer derde partijen, verstrek een afschrift van deze (gedateerde en gesigneerde) overeenkomst(en). U mag hierin desgewenst de financiële gegevens zwart maken.
8. In sommige winkel en horecalocaties op stations wordt eveneens gratis wifi-toegang aangeboden. Worden hierbij de MAC-adressen van van (apparaten van de) gebruikers vastgelegd?
9. De NS maakt gebruik van camera-toezicht op stations. Hoe lang worden de vastgelegde camerabeelden bewaard? Staan de camera's dag en nacht aan?

[3] http://www.ns.nl/reisinformatie/voorzieningen/voorzieningen-op-het-station.html
[4] http://www.ns.nl/reisinformatie/voorzieningen/voorzieningen-in-de-trein.html.

10. Beschrijf de technische toegang van de NS tot de in- en uitcheckgegevens van OV-chipkaarthouders op de stations. Betreft dit realtime toegang, of verkrijgt u *batches* over een bepaalde periode? Verkrijgt de NS individuele reisgegevens, of toegang tot geaggregeerde of statistische gegevens over het in- en uitchecken per station of per tijdseenheid?
11. Geef een nadere toelichting op de noodzaak van deze wijze van tracken. Licht toe welke andere methoden u heeft overwogen, en als niet toereikend hebt beoordeeld. Ga in ieder geval op het alternatief om de MAC-adressen onmiddellijk, op de sensor, te anonimiseren en op de mogelijkheid om steekproeven te nemen (geautomatiseerde of handmatige tijdelijke of in tijd beperkte metingen). Ga daarnaast in op elk van de andere methoden die u al toepast, zoals het tellen van het aantal reizigers via OV-chipkaartgegevens (zowel op grond van in- en uitcheck handelingen in de stations, als met betrekking tot verplaatsingen tussen stations), het tellen van reizigers via stereocamera's, het bewaren van statistieken over aantallen in- en uitcheck handelingen per station voor elk van de doeleinden die u in antwoord op vraag 5 heeft genoemd.
12. Geef een nadere toelichting op de wijze waarop u mensen die stations betreden informeert. Heeft u onderzocht of deze wijze van informeren de doelgroep effectief bereikt? Zo ja, verstrek een afschrift van dit onderzoek. Zo nee, onderbouw met bijvoorbeeld een vergelijking tussen het aantal bezoekers aan het aantal stations waarop de tracking plaatsvindt, en bezoek aan de webpagina http://www.stations.nl/beleid/privacy waar bezoekers informatie kunnen lezen over de doeleinden van deze gegevensverwerking.
13. Heeft u vragen of klachten van betrokkenen ontvangen over deze wijze van tracking? Zo ja, verstrek een overzicht van de ontvangen vragen en klachten.
14. Geef een nadere toelichting op de technische en organisatorische waarborgen die u heeft getroffen, zoals de opt-outmogelijkheid door het uitschakelen van de wifi en bluetooth-functionaliteit. Ga hierbij in op de afweging die u heeft gemaakt tussen de privacyrechten van reizigers en stationsbezoekers en uw gerechtvaardigd belang om de metingen op deze wijze te verrichten.
15. Verstrek een gedetailleerde beschrijving van de exacte technische werkwijze, en onderbouw met afschriften van de technische specificaties en screenshots van de van instellingen van de gebruikte sensoren en achterliggende systemen (bij BlipTrack). Verstrek een databasemodel waaruit blijkt hoe de metingen (welke exacte gegevens) worden vastgelegd. Verstrek een uittreksel uit het script of de code waarin de frequentie van metingen door sensoren is bepaald (hoe vaak per tijdseenheid er gescand wordt, en gedurende welk tijdvak (24/7 of beperkter). Beschrijf per station (waar op dit moment de tracking wordt toegepast) van hoeveel sensoren u gebruik maakt. Beschrijf hoe de plaats is bepaald van de sensor(en) in de stations, en het bereik van de sensoren. Beschrijf de eventuele maatregelen die u hebt getroffen om te voorkomen dat de MAC-adressen van passanten, die het station niet betreden, geregistreerd worden. Licht ook toe hoe het systeem dubbeltellingen vermijdt (van bijvoorbeeld de wifi en bluetooth MAC adressen behorend bij één apparaat), en of, en zo ja, welke maatregelen er zijn getroffen om gerandomiseerde MAC-adressen te herkennen.
16. Verstrek een screenshot van de database waarin de tien oudst aanwezige records met ruwe data bovenaan staat. Voeg de gebruikte query bij. Verstrek een uitdraai van het script waarmee eventnummers ouder dan 5 jaar worden gewist.

AUTORITEIT
PERSOONSGEGEVENS

Datum
7 juli 2017

Ons kenmerk
z2017-05365

17. Heeft de NS ooit gegevens die gegenereerd zijn door de bluetooth en wifi-tracking aan opsporingsautoriteiten verstrekt? Zo ja, verstrek een overzicht van de data waarop informatie is gevraagd, ten behoeve van welke opsporingsdienst, en beschrijving van de verstrekte gegevens, inclusief eventuele opvragingen die de NS eventueel heeft geweigerd.

Reactietermijn
De AP verwacht dat u de gevraagde informatie en bescheiden binnen drie weken toestuurt, uiterlijk **vrijdag 28 juli 2017.**

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Autoriteit Persoonsgegevens,
Namens deze,

[redacted]

Mw. drs. [redacted]
Senior inspecteur

aangetekend

NS

NS Legal

Laan van Puntenburg 100
Postbus 2812
3500 GV Utrecht
Nederland
www.ns.nl

Postbus 2812, 3500 GV Utrecht
Autoriteit Persoonsgegevens
t.a.v. mw. drs. [redacted]
Postbus 93374
2509 AJ Den Haag

Datum 14 juli 2017
Ons kenmerk NSL/2017/12298-1
Onderwerp Wifi tracking op stations

Telefoon [redacted]
E-mail [redacted]@ns.nl

Geachte mevrouw [redacted]

Naar aanleiding van uw schrijven gedateerd 7 juli 2017, kenmerk z2017-05365, hetwelk ik op maandag 10 juli jl. ontving, bericht ik u het volgende.

U heeft het schrijven gericht aan de FG. NS heeft echter sinds de inwerkingtreding van de Wet bescherming persoonsgegevens (Wbp) geen Functionaris Gegevensbescherming in de zin van artikel 62 van deze wet benoemd, noch aangemeld bij de Autoriteit Persoonsgegevens.
Bij NS Groep N.V. vervul ik de functie van privacy coördinator. Sinds NS onder het toezicht van de Autoriteit Persoonsgegevens (voorheen CBP) valt, is correspondentie in verband met toezicht en handhaving steeds gericht geweest aan de directie van NS Groep N.V.
Aangezien ik overigens niet bevoegd ben om de vennootschap in rechte te vertegenwoordigen, verzoek ik u uw vragen te richten aan directie NS Groep N.V. aan de Laan van Puntenburg 100, 3511 ER te Utrecht. Niettemin heb ik uw schrijven inmiddels doorgeleid naar de directie van NS Groep N.V. en zal ik intern de nodige voorbereidingen treffen voor een zorgvuldige behandeling van uw brief.

Verder heeft uw brief heeft bij mij de vraag opgeroepen of hier sprake is van een onderzoek op grond van artikel 60 Wbp. Voor de goede orde ontvangt NS graag een nadere duiding van de vragen die voortvloeien uit het gesprek van AP met de projectleider voor wifi tracking.

Tot slot verzoek ik u om de termijn waarbinnen u de gevraagde informatie en bescheiden van NS verwacht, te verruimen tot en met 14 augustus 2017. Gelet op het feit dat uw brief mij eerst op 10 juli heeft bereikt is deze termijn, gezien de omvang en complexiteit van uw vragen, betrekkelijk kort. Daar komt de omstandigheid bij, dat uw verzoek om inlichtingen midden in de periode van zomervakanties valt. Een ruimere termijn stelt ons in staat om de gewenste kwaliteit van antwoorden waar te maken.

Graag verneem ik van u,

Hoogachtend,

[redacted]

dhr. drs. [redacted]
privacy coördinator NS groep N.V.

N.B. deze brief wordt u ook per faxbericht toegezonden

AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
NS Groep N.V.
T.a.v. de directie
Laan van Puntenburg
3511 ER UTRECHT

Datum
18 juli 2017

Ons kenmerk
z2017-05365

Contactpersoon
Mw. drs. [redacted]
070 8888 500

Onderwerp
Wifi en bluetooth tracking NS stations

Geachte directie,

De Autoriteit Persoonsgegevens (AP) heeft op 14 juli 2017 de schriftelijke reactie ontvangen van uw privacy coördinator, de heer [redacted], op de brief met vragen van de AP van 7 juli 2017. De heer [redacted] geeft aan dat hij de brief intern heeft doorgeleid, maar verzoekt om correspondentie in het vervolg tot de directie te wenden. De AP geeft hierbij gehoor aan dit verzoek.

De heer [redacted] vraagt om twee weken uitstel voor de beantwoording van de gestelde vragen, tot maandag 14 augustus 2017, in plaats van uiterlijk vrijdag 28 juli 2017. In verband met de zomervakantie honoreert de AP dit verzoek. De AP merkt op dat dit geen uitstel betekent van uw verantwoordelijkheid voor de gegevensverwerking. U dient als verantwoordelijke voor de gegevensverwerking via bluetooth- en wifi-tracking goed te kunnen onderbouwen dat de gegevensverwerking noodzakelijk is ter behartiging van uw gerechtvaardigd belang. Indien u bij de beantwoording van de vragen zelf tot de conclusie zou komen dat sprake is van een verwerking van persoonsgegevens (bijvoorbeeld gedurende de 24 uur dat u de gehashte mac-adressen bewaart in combinatie met de salt), adviseert de AP u tussentijdse maatregelen te treffen en deze te documenteren bij uw beantwoording van de vragen van de AP. Dat geldt ook indien u er niet zeker van bent of uw werkwijze, mede gelet op het feit dat de metingen in de openbare ruimte worden verricht, voldoet aan de vereisten van proportionaliteit en subsidiariteit, en dat uw belang prevaleert boven het recht van betrokkenen op bescherming van hun persoonlijke levenssfeer.

De heer [redacted] vraagt of sprake is van een ambtshalve onderzoek in de zin van artikel 60 van de Wbp. Dat is op dit moment (nog) niet het geval. De AP heeft de inlichtingen verzocht, zoals toegelicht in de brief van 7 juli 2017, naar aanleiding van persvragen over bluetooth en wifi-tracking op NS-stations. De AP verzoekt

AUTORITEIT
PERSOONSGEGEVENS

Datum
18 juli 2017

Ons kenmerk
z2017-05365

de inlichtingen in het kader van haar algemene bevoegdheden genoemd in de artikelen 5:15 tot en met 5:19 van de Algemene wet bestuursrecht (Awb). Wellicht ten overvloede wijs ik u erop dat u op grond van artikel 5:20 van de Awb verplicht bent aan de uitoefening van deze bevoegdheden mee te werken.

De AP ziet de schriftelijke beantwoording van de vragen graag uiterlijk maandag 14 augustus 2017 tegemoet.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Autoriteit Persoonsgegevens,
Namens deze,

[redacted]

Mw. drs. [redacted]
Senior inspecteur

VERTROUWELIJK

Postbus 2812, 3500 GV Utrecht
Autoriteit Persoonsgegevens
t.a.v. mw. drs. [redacted]
Postbus 93374
2509 AJ Den Haag

College bescherming persoonsgegevens
15 AUG 2017
Ontvangen

NS

NS Legal
Laan van Puntenburg 100
Postbus 2812
3500 GV Utrecht
Nederland
www.ns.nl

Datum 14 augustus 2017
Uw kenmerk z2017-05365
Ons kenmerk NSL/2017/12426-2
Onderwerp verzoek om inlichtingen WiFi/BT tracking

Telefoon [redacted]
E-mail [redacted]@ns.nl

Geachte mevrouw [redacted]

In uw brief van 7 juli 2017 met kenmerk z2017-05365, verzocht u om nadere inlichtingen over het verwerken van WiFi/Bluetooth tracking gegevens. In antwoord hierop deel ik u namens NS Groep N.V. het volgende mee.

Inleiding

NS past op dit moment op een zestal stations WiFi en Bluetooth tracking toe (hierna aangeduid als WiFi/BT tracking).

Naar het oordeel van NS en uitgaande van de daarvoor in recente rechtspraak ontwikkelde criteria[1], is geen sprake van het verwerken van persoonsgegevens in de zin van de Wet bescherming persoonsgegevens. NS beschikt niet over de middelen waarmee houders van apparaten met ingeschakelde WiFi en/of Bluetooth functie op haar stations kunnen worden geïdentificeerd. Uitgesloten is bijvoorbeeld dat NS bij aanbieders van mobiele telefoon- en internetdiensten de extra informatie kan verkrijgen die nodig is om de identiteit van de eindgebruikers of abonnees van zulke apparaten vast te stellen. Het is niet zo dat NS van reizigers of bezoekers van stations de gegevens verzamelt waarmee kan worden vastgesteld welke apparaten met een bepaald MAC-adres bij welk geïdentificeerde natuurlijke persoon horen.
Er is dus geen sprake van het verwerken van persoonsgegevens, waarop de Wet bescherming persoonsgegevens van toepassing is. Niettemin heeft NS ervoor gekozen om bij het inrichten van het proces betreffende het vastleggen en gebruiken van WiFi/BT trackinggegevens steeds te handelen alsof deze gegevens kwalificeren als persoonsgegevens. De wens zo zorgvuldig mogelijk te zijn staat hierbij centraal. Door de beginselen uit de privacywetgeving als uitgangspunt te hanteren is NS in staat om op een transparante en verantwoorde manier te voorzien in informatie die van essentieel belang is voor de

[1] Zie o.a. HvJEU 19 oktober 2016, C-582/14, ECLI:EU:C:2016:779 en recent Rb Midden Nederland 2 augustus 2017, ECLI:NL:RBMNL:2017:4011.

uitoefening van haar bedrijf op de stations, niet alleen voor de commerciële exploitatie, maar vooral ook voor het publieke belang dat samengaat met het beheer van stations. Dit laatste ziet op het waarborgen van de veiligheid, het mogelijk maken van een goede doorstroming en het verbeteren van de dienstverlening aan reizigers (bijvoorbeeld door voorzieningen aan te bieden op die plaatsen waar reizigers daar behoefte aan hebben). In onderhavig document annex bijlagen beantwoordt NS de door u gestelde vragen. In aanvulling daarop, en voor een beter begrip van de gegeven antwoorden, wordt ook verwezen naar de documenten die hierbij als bijlagen gaan. In totaal gaat het om acht documenten die in een apart overzicht zijn vermeld.

Daar waar in de beantwoording van de vragen gesproken wordt over NS, wordt bedoeld NS Groep N.V. en haar dochtervennootschappen. Onder WiFi/BT tracking wordt verstaan het proces waarbij WiFi- en/of Bluetoothsignalen, die worden verzonden door apparaten die reizigers en bezoekers van stations bij zich dragen, worden omgezet tot geaggregeerde anonieme informatie over aantallen en loopstromen.

Alvorens hierna tot een inhoudelijke beantwoording van uw vragen over te gaan, wil ik u graag attenderen op het feit dat de Autoriteit Persoonsgegevens (hierna: AP) op 14 juni jl. rechtstreeks telefonisch informatie over bedrijfsprocessen bij NS heeft ingewonnen bij de desbetreffende projectleider van NS Stations B.V., de heer [redacted]. Tot dusver was gebruikelijk dat de AP het Privacy Office of de privacy-coördinator binnen onze organisatie benaderde.
NS verzoekt de AP vriendelijk om alle communicatie te richten aan het Privacy Office van NS, die de AP zo nodig in contact kan brengen met anderen binnen NS.

De inhoudelijke reactie op de vragen van AP

De inhoudelijke reactie van NS bestaat uit twee delen, te weten: (1) een reactie op de "Verklaring NS" en (2) de inhoudelijke beantwoording van vragen van de AP.

deel I: Reactie op de "Verklaringen NS"

Uw brief van 7 juli 2017 aan NS, kenmerk z2017-05365, bevat onder de kop "Verklaringen van NS" uw weergave van het telefonisch onderhoud met de heer [redacted] projectleider WiFi/BT tracking op stations. De inhoud van het telefoongesprek is in de optiek van NS en van de heer [redacted] in uw brief niet volledig en ook niet geheel juist weergegeven. Wij lopen de diverse aandachtspunten uit de "Verklaringen van NS" na en voorzien die van bijbehorend commentaar in de rechterkolom van onderstaand overzicht.

"Verklaring van NS"	Commentaar NS
De NS past sinds 2012 WiFi/BT tracking op stations toe.	Correcte weergave
De NS maakt gebruik van de diensten van het Deense bedrijf Blip Systems. De NS heeft een bewerkersovereenkomst gesloten met Blip Systems waarin gebruik door Blip Systems van de verzamelde gegevens voor eigen doeleinden is uitgesloten.	Zie de overeenkomst met Blip Systems in bijlage onder nummers 1. en 2.
Het doel is anonieme passagiersstromen in kaart te brengen. Dit gebeurt soms als experiment bij de inrichting van nieuwe stations of de verbouwing van bestaande stations om te kijken hoe je bijvoorbeeld de roltrap het beste kunt plaatsen of waar je de winkels het beste kunt plaatsen. Meestal wordt de tracking ingezet om te tellen hoeveel mensen er in en uit een station gaan (loopstroomtelling), op een perron staan, of zich op andere plekken/doorgangen in het station bevinden (crowd management). De NS gebruikt de tracking ook om te meten hoeveel mensen van station A naar station B reizen. Ten slotte gebruikt de NS de tracking om op grond van tellingen op specifieke perrons van station Schiphol te voorspellen hoeveel mensen er in Amsterdam Centraal Station worden verwacht.	Dit is een gedeeltelijke weergave van hetgeen de heer Van den Heuvel mondeling heeft toegelicht. In het gesprek is aangegeven dat de meetinstallatie per station anders is en dat het ontwerp van de installatie afhankelijk is van de reden waarom NS metingen verricht. Zie verder het antwoord op vraag 6.
De NS gebruikt de OV-chipkaartgegevens om statistisch te tellen hoeveel mensen er in en uit de stations gaan. Daarnaast gebruikt de NS twee stereocamera's op de perrons 1 en 2 van station Schiphol voor anonieme tellingen van het aantal personen op deze perrons.	NS maakt van diverse bronnen gebruik om te tellen hoeveel mensen er een station in of uit gaan. Bij voorkeur maakt NS gebruik van geaggregeerde OV-chipkaart data, dat wil zeggen: data ontdaan van identificerende kenmerken. NS maakt hier gebruik van omdat dit beperkte extra kosten met zich meebrengt. Indien nodig maakt NS ook gebruik van stereoscopische sensoren. Deze sensoren genereren alleen tekstbestanden met aantallen per tijdseenheid.

De NS informeert over de tracking via een bordje/sticker bij de ingang van stations, op de plek waar ook over cameratoezicht wordt geïnformeerd, en waar de huisregels van het station hangen. De NS heeft in haar privacyverklaring een alinea opgenomen over wifi- en bluetooth-tracking. Daarnaast heeft de NS onlangs actief de pers geïnformeerd over de aanwezigheid van tracking.	Volledigheidshalve is daarnaast ook aangegeven dat NS sinds 2013 actief de publiciteit heeft opgezocht uit overwegingen van transparantie en publieksinformatie. Zie verder in de bijlage document nr. 3
De NS biedt geen opt-out mogelijkheid voor tracking. Personen die niet getrackt willen worden, kunnen de wifi- en bluetoothfunctionaliteit van hun telefoon uitschakelen. De NS wil niet via een opt-out registratie alsnog persoonsgegevens verzamelen.	Correcte weergave
De NS past (via technologie van, en op servers van, het bedrijf Bliptrack) een hashing methode toe op de verzamelde MAC- adressen. Een MAC-adres (Media Access Control adres) is een vrijwel unieke reeks (meestal in hexadecimale vorm) die, toegekend aan een apparaat (een smartphone, tablet of computer), dat apparaat identificeert en het mogelijk maakt dat apparaten in een ethernetnetwerk met elkaar kunnen communiceren. De hash wordt op alle stations in Nederland (waar deze tracking plaatsvindt) op dezelfde manier berekend.	Zie hierover § 3.2 van het Informatiebeleidsplan SMART station, zie bijlage document nr. 4
De MAC-adressen worden op de sensoren gehasht, waarbij de laatste 8 bits van de hash van het MAC-adres worden verwijderd (truncated) en dan naar de server gestuurd. Daar worden ze voor de tweede keer gehasht, met een salt. Een salt is een nummer dat aan de hash wordt toegevoegd, om de uitkomsten van de hash onvergelijkbaar te maken met eerdere hashes van hetzelfde MAC-adres waarbij een andere salt is gebruikt. De NS genereert de salt door een standaard java random number generator, met een seed die gebaseerd is op de datum/tijd. Na deze tweede hash worden opnieuw de laatste 8 bits van de hash verwijderd.	Correcte weergave. zie verder bijlage document nr. 4
De salt wordt niet gelogd, en na 24 uur verwijderd.	Correcte weergave. Zie verder bijlage document nr. 4
De NS noemt de gehashte MAC-adressen op de server 'eventnummers'. Deze nummers worden opgeslagen met de bijbehorende sensor-ID (plek), datum/tijd en signaalsterkte (RSSI).	Correcte weergave
De NS bewaart de gegevens gedurende 5 jaar, om de drukte op stations, de loopstromen en reispatronen door de tijd heen te kunnen vergelijken.	De MAC-adressen worden niet bewaard. De "eventnummers" worden maximaal 5 jaren bewaard. De reden hiervoor is om terug te kunnen kijken indien een specifiek patroon moet worden geanalyseerd dat voorheen nog niet was gedefinieerd.

deel II: beantwoording van de door AP gestelde vragen

1. **Overeenkomst met Blip Systems**
   Wij verwijzen u naar de bijlage, documentnummers 1 en 2, te weten: opdrachtbevestiging en IT- inkoopvoorwaarden van NS.

2. **Afschrift van interne besluitvorming over gebruik van WiFi/BT tracking**
   Wij verwijzen u naar bijlage, document nr. 5 waaruit blijkt dat de directie van NS Stations B.V. haar goedkeuring heeft verleend aan het toepassen van WiFi/BT tracking. Verder treft u in de bijlagen documenten aan met de nummers 1 en 2 met betrekking tot de samenwerking met Blip Systems.
   In 2012 heeft NS de levering van WiFi/BT tracking aanbesteed. In het kader hiervan zijn er contacten geweest met de firma [redacted]. Deze leverancier heeft ten tijde van de aanbesteding gebruik gemaakt van een testopstelling die geleverd werd door een toeleverancier, te weten [redacted]. De aanbestedingsprocedure heeft niet geleid tot een opdrachtovereenkomst met deze leverancier. Bij de besluitvorming om niet met deze leverancier verder te gaan is veel betekenis toegekend aan belangen verband houdend met privacy en gegevensbescherming. Uiteraard is de testopstelling direct na beëindiging van de procedure verwijderd.

3. **De samenwerking tussen NS en ProRail B.V.**
   ProRail B.V. heeft geen toegang tot IT-systemen van NS waarin WiFi/BT tracking gegevens van NS worden verwerkt. Overigens verstrekt NS geen "ruwe data" aan ProRail B.V., maar slechts geaggregeerde data. Feitelijk zou dat ook niet kunnen, omdat NS niet over de "ruwe data" beschikt. Het doel van de verstrekking van de geaggregeerde informatie is om ProRail in staat te stellen inzichten te verwerven in de loopstromen van reizigers door de fysieke infrastructuur (stationshal, transfers, perrons) waarvoor zij een beheersconcessie van de Rijksoverheid heeft.
   Een voorbeeld hiervan is de informatie die nodig is voor *crowd control* als middel om de veiligheidsrisico's te beheersen na de formele overbelastverklaring door ProRail van spoor 5 op Utrecht Centraal. Zie ook de beantwoording van vraag 6 voor wat betreft Utrecht Centraal.
   Een 5-tal medewerkers van ProRail heeft door NS geautoriseerde toegang verkregen tot een systeem dat alleen geaggregeerde data bevat.
   Overigens draagt Prorail B.V. geen verantwoordelijkheid voor de verwerking van gegevens.

4. **Locaties van NS waar WiFi/BT tracking wordt toegepast**
   Op dit moment wordt op de volgende locaties Wifi/BT tracking toegepast: Amsterdam Centraal, Leiden Centraal, Amsterdam-Zuid, Utrecht Centraal, Schiphol Airport en 's-Hertogenbosch. Op station Groningen werd alleen in het jaar 2013 gebruik gemaakt van WiFi/BT tracking.
   Sinds 2016 exploiteert NS in samenwerking met andere aanbieders van Openbaar Vervoer de zogenaamde OV Servicewinkel. Het gaat om de stations Arnhem, Den Haag Centraal, Breda, Amsterdam Centraal, Utrecht CS en 's-Hertogenbosch (Tickets & Service winkel). Tijdens het interne onderzoek naar aanleiding van uw verzoek om inlichtingen over WiFi/BT tracking, kwam aan het licht dat in elk van deze OV Servicewinkels aanvankelijk een sensor stond opgesteld, met het doel om de verblijfstijd te meten van klanten in de OV Servicewinkel.
   Er is vastgesteld dat er geen gebruik wordt gemaakt van meetresultaten, derhalve is besloten om de sensoren buiten werking te stellen.
   Overigens heeft geen koppeling bestaan tussen de sensoren in de OV Servicewinkels en WiFi/BT tracking, noch zijn gegevens van de sensoren in verband gebracht met andere

bronnen van gegevens binnen NS.
Inmiddels is, zoals gezegd, het meten van verblijfstijden in de OV Servicewinkels beëindigd en zijn de sensoren uitgeschakeld.

5. Informatie aan bezoekers van de stations

Sinds december 2016 is in het privacy statement op zowel ns.nl/privacy als stations.nl/privacy een bekendmaking opgenomen over WiFi/BT tracking. Verder zijn in de periode 6 t/m 23 maart 2017 op de 6 stations stickers bij in- en uitgangen aangebracht waarmee het publiek over de tracking wordt geïnformeerd. Zoals in het voorgaande uiteengezet is dat niet zozeer gedaan omdat de Wet bescherming persoonsgegevens dat vereist, maar omdat NS heeft gemerkt dat reizigers hier prijs op stellen.

6. Doeleinden voor verwerking van WiFi/BT gegevens

Er worden sinds de ontwikkeling van WiFi/BT tracking op stations geen ruwe tracking gegevens verwerkt. In het ontwerp heeft NS hier bewust voor gekozen. Voor een meer gedetailleerd inzicht in de verwerking verwijzen wij u naar het document "Informatiebeleidsplan en Privacy Impact Assessment SMART Station versie 2016", paragraaf 3.2. (technologie), bijlage nummer 4.
Het doel van de verwerking van de *gehashte* tracking gegevens is per locatie en per tijdsperiode bepaald. NS heeft bewust "*tracking omwille van tracking*" vermeden.
Het doel van tracking is verbonden aan de specifieke informatiebehoefte die samenhangt met de functies van de betreffende stations. Dat zijn de verkeerskundige functie in het spoorwegnetwerk van Nederland en de commerciële exploitatie van voorzieningen op de stations. De informatiebehoefte varieert niet alleen naar plaats, maar ook naar tijd. Zo is bijvoorbeeld op station Groningen alleen in het jaar 2013 WiFi/BT tracking toegepast omdat de informatie over loopstromen in die periode noodzakelijk was voor het opnieuw inrichten van het station. Sinds de afronding van dit traject bestaat voor station Groningen geen behoefte om nog langer WiFi/BT tracking toe te passen. Informatie over het generieke doel van WiFi/BT tracking vindt u op pagina 5 van het Informatiebeleidsplan SMART station dat hier als bijlage gaat.

Hieronder gaat een overzicht van de belangrijkste doelen per tijdsperiode:

station	doel(en) van WiFi/BT-tracking
Amsterdam Centraal	• 2016-heden: meten van effecten op loopstromen in het kader van het voorgenomen besluit rond de sluiting van de OV-Chipkaart poortjes. (zie voorbeeld van resultaten in bijlage, nr 6). • 2017-heden: verkeersonderzoek naar mogelijke knelpunten en oplossingsrichtingen bij invoering PHS (Programma Hoogfrequent Spoor, te beginnen met de verbinding Eindhoven - Amsterdam CS). • juli t/m september 2016: pilot exploitatie van winkelvoorzieningen. Mede aan de hand van loopstromen is gezocht naar de meest optimale positie van de kiosken.
Amsterdam-Zuid	• 2017-heden: onderzoek naar operatie "Vangnet Amsterdam Zuid" (*crowd control*) en studie naar capaciteit van de Minervapassage met het oog op ingebruikname van de Noord-Zuid Lijn in Amsterdam.
Schiphol Airport	• 2013-2014: loopstromen in kaart brengen ten behoeve van invoering OV-chipkaart en de gewenste opstelling van poortjes. • 2014-2015: Meerjaren Infrastructuur, Ruimte en Transport (hierna afgekort als: MIRT)- planstudie voor Openbaar Vervoer

	Schiphol-Amsterdam-Almere-Lelystad; eerste fase planvorming herontwikkeling station Schiphol. • 2016-heden: tweede fase planvorming herontwikkeling station (MIRT Verkenning); operatie Vangnet Schiphol Airport (*crowd control*). (zie voorbeeld van resultaten in bijlage, nr 6). De metingen op Schiphol Airport vinden plaats in samenwerking met de luchthaven.
Leiden Centraal	• 2013-heden: Proefstation voor nieuwe sensoren/technieken voor WiFi/BT tracking. Leiden Centraal is qua aantallen reizigers het 6e station van Nederland en heeft een eenvoudige lay-out (één tunnel met transfers naar de perrons). Dit maakt Leiden Centraal geschikt als proeflocatie alvorens op andere locaties nieuwe meetmodellen (met minder sensoren) toe te passen. Daarmee kan worden voorkomen dat in de toekomst onnodig veel sensoren worden geplaatst. • 2015-heden: monitoring totale passantenstroom in de reizigerstunnel vanwege forse groei van aantallen reizigers. Leiden Centraal heeft de aandacht omdat het kan uitgroeien tot "ernstig transferknelpunt", zoals vastgesteld in de Nationale Markt- en Capaciteitsanalyse van de Rijksoverheid.
Utrecht Centraal	• 2013-2015: ontwikkeling SMART Station concept tijdens de verbouwing van Utrecht Centraal. • 2015-2016: planvorming ontwikkeling ingangen bij Noordertunnel (zie voorbeeld van resultaten in bijlage, nr. 6). • 2017: onderzoek naar operatie "Vangnet Utrecht Centraal" (*crowd control*); studie naar maatregelen vanwege overbelastverklaring door ProRail van perron 5 en transfers tussen de stationshal en perron 5.
's-Hertogenbosch	• 2017: Planvorming voor herontwikkeling van het station in het kader van MIRT-planstudie; monitoring van de totale passantenstroom in de reizigerstunnel vanwege snelle groei van aantallen reizigers. 's Hertogenbosch kan uitgroeien tot transferknelpunt, zoals vastgesteld in de Nationale Markt- en Capaciteitsanalyse van de Rijksoverheid.
Groningen	• In 2013: Loopstromen door het station in kaart brengen ten behoeve van het plan voor de herontwikkeling van het station. Uitvoering/herbouw is inmiddels in voorbereiding (zie voorbeeld van resultaten in bijlage, nr. 6). WiFi/BT tracking vindt sinds eind 2013 hier niet meer plaats.

7. Gratis WiFi diensten, aangeboden door NS

NS biedt op bepaalde stations en in bepaalde treinen gratis WiFi aan haar klanten aan, zonder dat klanten daarbij hun identiteit bekend hoeven te maken. Klanten en bezoekers worden ook niet om hun persoonsgegevens gevraagd.
Op geen enkele wijze is er een verband tussen WiFi/BT tracking op stations onder beheer en supervisie van NS Stations B.V. en de WiFi service die door andere bedrijfsonderdelen van NS Groep N.V. wordt aangeboden.

NS biedt gratis WiFi service aan via een IT- infrastuctuur die los staat van de overige IT-

systemen van NS. Er vindt geen uitwisseling van data plaats, er bestaat geen koppeling van systemen, er zijn geen processen ingericht waarin data wordt vergeleken, er zijn geen afspraken over het met elkaar in verband brengen van data of informatie die kan worden ontleed aan de data. NS heeft geen systeem dat de MAC-adressen koppelt aan de identiteit van personen.

In het Informatiebeleidsplan SMART station (bijlage, nr. 4) is in § 3.4 onder "Governance" de rolverdeling tussen NS Stations als hoofd Proceseigenaar en partners/leveranciers beschreven alsmede de wijze waarop het toezicht is georganiseerd.

Waar biedt NS gratis WiFi service aan?

♦ in de lounges van NS International op Amsterdam CS, Schiphol Airport en Rotterdam CS, uitsluitend voor reizigers met een eerste klas internationaal vervoersbewijs, zonder dat klanten daarbij hun identiteit behoeven bekend te maken. Toegang tot de lounge wordt verkregen op vertoon van een geldig (internationaal) vervoersbewijs. Na afloop van elke sessie of na het verbreken van de WiFi-verbinding, vindt geen opslag voor verdere verwerking van MAC-adressen plaats.
De gratis WiFi service in de lounges van NS International vormt geen onderdeel van WiFi/BT tracking op stations.

♦ in de "Huiskamer" op een aantal stations. De "Huiskamer" is een voorziening voor reizigers en andere bezoekers van stations, die zich kenmerkt door een huiselijke sfeer met een hapje en een drankje en de mogelijkheid om gebruik te maken van WiFi service zonder dat klanten daarbij hun identiteit behoeven bekend te maken. Na afloop van elke sessie of na het verbreken van de WiFi-verbinding, vindt geen opslag voor verdere verwerking van MAC-adressen plaats.
De WiFi service in de "Huiskamer" van NS vormt geen onderdeel van WiFi/BT tracking op stations.

♦ in treinen van NS Reizigers (binnenlands vervoer op het hoofdrailnet). Ook voor deze WiFi-dienstverlening geldt dat reizigers niet hun identiteit hoeven (of kunnen) bekend maken om daarvan gebruik te maken. Na afloop van elke sessie, na het verbreken van de WiFi verbinding of na het verlaten van de trein, vindt geen opslag voor verdere verwerking van MAC-adressen plaats.
De gratis wifi service in treinen van NS Reizigers vormt derhalve geen onderdeel van Wifi/BT tracking op stations.

♦ in de internationale treinen (Thalys, ICE) wordt WiFi service aangeboden door Thalys International, respectievelijk Deutsche Bahn. De verwerking van MAC adressen vindt geheel buiten NS plaats. Op geen enkele wijze vindt uitwisseling van gegevens plaats tussen de buitenlandse vervoerders en NS; daarnaast worden gegevens niet met gegevens van NS vergeleken en worden geen koppelingen met systemen van NS gelegd.
De WiFi service op internationale treinen naar België en Duitsland vormen geen onderdeel van WiFi/BT tracking op stations.

♦ Met betrekking tot de zogeheten "flex werkplekken" die op bepaalde stations of in de directe omgeving van deze stations worden aangeboden, merkt NS op dat de exploitatie en het beheer van deze voorzieningen volstrekt onafhankelijk van NS wordt uitgevoerd door Regus Amsterdam B.V., statutair gevestigd te Amsterdam. Tussen NS en Regus bestaat op enkele locaties slechts de verhouding tussen verhuurder en huurder.
Er vindt op geen enkele wijze uitwisseling van tracking data plaats tussen NS en Regus, noch worden koppelingen tussen systemen gemaakt of wordt data onderling vergeleken.

Het aanbod van WiFi op de "flex werkplekken" van Regus bij stationslocaties van NS vormt geen onderdeel van WiFi/BT tracking op stations.

8. **Aanbod van gratis WiFi in winkel en horeca voorzieningen op stations.**
De exploitatie en de serviceverlening die samenhangt met bepaalde horeca voorzieningen, waaronder gratis WiFi, valt niet onder de verantwoordelijkheid van NS. Exploitanten van deze voorzieningen zijn zelfstandig verantwoordelijk voor hun eventueel aanbod van WiFi en de wijze waarop zij de data verwerken.
Ook hier gaat het om IT-infrastructuur die los van NS functioneert. Er is op geen enkele wijze een verband, technisch noch organisatorisch, tussen de gratis WiFi diensten op stations en WiFi/BT tracking op stations. Er vindt geen uitwisseling van data of informatie plaats, er bestaan geen koppelingen tussen diverse systemen. Voor zover NS bekend kunnen de desbetreffende klanten van deze WiFi-diensten gebruik maken zonder dat hun identiteit bekend moet worden gemaakt.

9. **Cameratoezicht op stations.**
NS zet permanent cameratoezicht in bij bewaking en beheersing van de veiligheidssituatie op haar stations. NS is Wbp-verantwoordelijk voor de verwerking van camerabeelden op stations. De camerabeelden worden uiterlijk 28 dagen na de totstandkoming vernietigd. Het beheer van de verwerking van camerabeelden is de exclusieve verantwoordelijkheid van NS Security.
Er is op geen enkele wijze, technisch noch organisatorisch, een proces waarbij camerabeelden in verband kunnen worden gebracht met WiFi/BT tracking data. Er vindt geen uitwisseling van camerabeelden en WiFi/BT tracking data plaats, er worden geen koppelingen gelegd tussen camerabeelden en WiFi/BT tracking data. De verwerking van camerabeelden op stations maakt geen deel uit van WiFi/BT tracking op stations.

10. **In- en uitcheckgegevens van houders van een OV chipkaart.**
De in- en uitchecktransacties van kaarthouders van NS komen *realtime* in het datacenter van NS. De toegang tot deze data wordt bepaald door het autorisatie- en informatiebeveiligingsbeleid van NS. Op grond hiervan hebben bepaalde daartoe geautoriseerde functionarissen die werkzaam zijn binnen het datacenter, uit hoofde van hun functie toegang tot deze kaarttransacties.
NS Reizigers B.V. verkrijgt check in - check out gegevens voor facturatie, serviceverlening op verzoek van de klant, het nakomen van verplichtingen die voortvloeien uit de vervoersovereenkomst met kaarthouder, waaronder begrepen maar niet beperkt tot het toepassen van de regeling "geld-terug-bij-vertraging" en het nakomen van verplichtingen die voortvloeien uit de Wet bescherming persoonsgegevens, zoals het recht van inzage en correctie.

Functionarissen buiten de datacenters hebben geen toegang tot check in - check uit transacties. Tot deze groep behoren de analisten van SMART station. Zij ontvangen periodiek overzichten van aantallen passages per poort of in/uitcheck paal op stations. Het gaat om aantallen die zijn ontleend aan OV-chipkaarttransacties waarvan alle identificerende kenmerken zijn verwijderd zodat slechts de "kale" aantallen overblijven. De gerapporteerde aantallen zijn per 15 minuten gedurende de spitsuren en per 60 minuten buiten de spitsuren.
Doel van deze informatievoorziening is om het onnodig toepassen van WiFi/BT tracking te vermijden op locaties waar met aantallen passages kan worden volstaan om informatie over loopstromen te genereren.

11. **De noodzaak voor NS om WiFi tracking toe te passen zoals beschreven in het Informatiebeleidsplan SMART Station, zie bijlage document nummer 4.**
Met betrekking tot het Informatiebeleidsplan SMART station verwijzen wij u voor de

beantwoording van uw vragen bij dit punt, in het bijzonder naar § 1.1, § 2.2, § 3.2 en § 3.4 van dit document.
NS heeft in de jaren tot 2012 met enige regelmaat handmatig tellingen laten verrichten. Het resultaat van deze inzet is beschreven in § 1.1, pagina 3 van het Informatiebeleidsplan SMART station.

Over het gerechtvaardigd belang van NS
De gegevensverwerking WiFi/BT tracking baseert NS, zoals u terecht aanneemt in uw brief van 7 juli jl., op de behartiging van een gerechtvaardigd belang, waarbij naar haar oordeel de verwerking voldoet aan de vereisten van proportionaliteit en subsidiariteit en het gerechtvaardigd belang prevaleert boven het recht van de betrokkenen op bescherming van hun persoonlijke levenssfeer. Eén en ander wordt hieronder nader uitgewerkt.

Het gerechtvaardigd belang van NS is, zoals hierboven ook toegelicht, samenvattend gelegen in:

- het kunnen meten van de effecten op loopstromen na het besluit om de OV-chipkaart poortjes te sluiten;
- het kunnen onderzoeken van mogelijke knelpunten en oplossingsrichtingen, zowel vervoerskundige knelpunten als die welke te maken hebben met de inrichting van het station, waaronder de aangeboden voorzieningen;
- noodzaak tot *crowd control*;
- het in kaart brengen van loopstromen vanwege de specifieke doelen per station; wij verwijzen naar de beantwoording van vraag 6;
- herinrichting van diverse stations, zowel vanuit het publiek belang als vanuit commercieel perspectief, te weten de positionering van de voorzieningen op de stations;
- het efficiënt, zowel qua uitvoering als qua kosten, inrichten van een proces om de genoemde doelen te bereiken.

NS draagt er zorg voor dat de gegevens op een zorgvuldige wijze worden verwerkt, met inachtneming van vereisten van proportionaliteit en subsidiariteit. Door de door NS gekozen werkwijze, zoals uiteengezet in de bijlagen bij deze brief ter beantwoording van vraag 15 uit uw brief van 7 juli 2017, blijkt dat NS er zorg voor draagt dat niet meer gegevens worden verzameld en verwerkt dan nodig zijn voor het realiseren van de door NS vastgestelde doelen voor de desbetreffende verwerking.

NS heeft onderzocht over welke mogelijkheden (en dus ook alternatieven) zij beschikt om de door haar nagestreefde doelen te realiseren:

(a) Handmatige tellingen
Zoals volgt uit het Informatiebeleidsplan SMART station (bijlage, document nr. 4, pag. 3), bestond er voorheen voor NS geen effectieve methode om loopstromen te meten en dus om de door haar nagestreefde doelen, die hoofdzakelijk liggen in het publieke belang, te behalen. Tot 2011 werden de loopstromen gemeten door middel van handmatige tellingen. Dit is een zeer kostbare, onpraktische en minder betrouwbare methode. Er dienen namelijk fysiek mensen op de stations bij alle in- en uitgangen aanwezig te zijn. Dit betekent een groot aantal tellers met hoge arbeidskosten. Echter, tegenover deze hoge kosten staat dat het geleverde inzicht bij deze optie zeer beperkt is. Het gaat immers om de telresultaten die betrekking hebben op slechts één of twee dagen.
De vraag is dan ook of deze dagen voldoende representatief zijn. Tot 2011 heeft NS dit alternatief gehanteerd en de conclusie hiervan is dat de verkregen inzichten onnauwkeurig en te generiek waren om de door haar nagestreefde doelen te bereiken.

Aangezien NS door gebruik van deze methode de door haar nagestreefde doelen, die ook zijn gelegen in het publieke belang, niet kon bereiken heeft zij besloten dit alternatief vanaf 2011 niet langer te hanteren.

(b) Aantallen check-in/check-uit per poort/per paal
Een andere methode om de nagestreefde doelen te behalen is om de aantallen check-in/check-uit transacties per toegangspoort/-paal in kaart te brengen. Ook bij deze methode worden geen persoonsgegevens verwerkt, maar slechts met aantallen per tijdsperiode per poort-/paalnummer. Dit alternatief zou vanuit privacy oogpunt dus voldoende rekening houden met de belangen van de reizigers.

NS heeft dit alternatief onderzocht en is tot de conclusie gekomen dat deze methode, om meerdere redenen, voor een aantal stations inderdaad de voorkeur heeft. De eerste reden is dat deze methode door reizigers wordt ervaren als minder ingrijpend. De tweede reden is dat dit alternatief minder kostbaar is dan de andere twee in deze brief beschreven methoden (te weten de inzet van sensoren en het handmatig tellen). Een derde reden is gelegen in het feit dat deze methode, voor de stations met een betrekkelijk eenvoudige infrastructuur en inrichting, voldoende betrouwbare resultaten oplevert.

Voor de meer complexere stations zoals bijvoorbeeld Schiphol (onder andere vanwege de transferfunctie naar de luchthaven) volstaat de methodiek van het aantal poort-/paal passages niet. Per station is gekeken en afgewogen of met deze methode kon worden volstaan. Op basis van deze afweging is vervolgens besloten om deze methode te gebruiken waar dat mogelijk is, dat wil zeggen in de stations die in termen van infrastructuur en inrichting minder complex zijn. In deze stations wordt de benodigde informatie (dus de aantallen), in de spitstijd per kwartier vastgelegd en buiten de spits per uur.
Voor zes stations bleek dat dit, gelet op de complexiteit in termen van infrastructuur en inrichting, niet mogelijk. Voor deze stations is daarom ervoor gekozen om ook gebruik te maken van WiFi/BT tracking (zie het antwoord op vraag 6). In deze stations worden de geaggregeerde aantallen van poort-/paalpassages gebruikt om meetresultaten en conclusies te valideren. Het kan bijvoorbeeld zijn dat de metingen via sensoren een extreem hoge of lage uitschieter laten zien. In zo'n geval kunnen de aantallen poort-/paalpassages worden gebruikt om te zien of de meting via de sensoren correct is.

(c) Sensoren inzetten (WiFi/BT tracking)
Deze derde methode behoeft hier ons inziens geen nadere uitleg qua werking, aangezien elders in deze brief dit punt voldoende duidelijk uiteen wordt gezet. Niettemin verwijzen wij u naar het Informatiebeleidsplan SMART station (bijlage, document nr. 4) , in het bijzonder § 2.1 en § 3.2.
Er zijn stations in Nederland die, gezien hun complexiteit in termen van infrastructuur en inrichting, niet geschikt zijn om via de hierboven tweede genoemde methode de door NS nagestreefde doelen te realiseren. Om die reden is NS op zoek gegaan naar een andere methode en die heeft zij gevonden in het inzetten van sensoren (WiFi/BT tracking). Ook voor deze methode geldt dat NS daarmee de door haar nagestreefde doelen weet te behalen. Echter, het nadeel van deze methode is dat deze betrekkelijk kostbaar is. Ook daarom is er soms voor gekozen om de methode als beschreven onder sub (b) toe te passen.

Zoals in de inleiding van onderhavige brief uiteengezet, worden er door middel van deze methode geen persoonsgegevens verwerkt. NS heeft er voor gekozen om het proces

zodanig in te richten alsof (dus met de fictie dat) hier wel sprake is van de verwerking van persoonsgegevens. NS onderkent daarmee dat er reizigers en bezoekers zijn die WiFi/BT tracking als belastend ervaren en er prijs op stellen dat is gewaarborgd dat van de op deze wijze verkregen gegevens op zorgvuldige en transparante wijze gebruik wordt gemaakt. Om deze reden heeft NS ervoor gekozen om alleen gebruik te maken van WiFi/BT tracking waar er aantoonbaar geen alternatieve methoden kunnen worden ingezet (subsidiariteit), en dat dan alleen op een wijze waarbij de belangen van reizigers en bezoekers aantoonbaar niet meer kunnen worden geraakt dan nodig is in het licht van de doeleinden waarvoor de techniek wordt ingezet (proportionaliteit).
Zie ook het antwoord op vraag 11, sub (b).

NS is van mening dat zij het huidige proces met voldoende technische en organisatorische waarborgen heeft omkleed en dat voldoende rekening is gehouden met de belangen van reizigers en bezoekers, en dat deze dus niet prevaleren. De inrichting van het proces wordt uitvoerig toegelicht in deze brief en de daarbij behorende bijlagen. En daarbij komt, meent NS, vooral betekenis toe aan de getroffen technische maatregelen, zoals de maatregel dat MAC-adressen onmiddellijk worden gehasht binnen de sensoren die het signaal opvangen, dat er daarna nogmaals een hash plaatsvindt op het moment dat het eerder gehashte MAC-adres op de server van Blip Systems binnenkomt en dat deze hash onomkeerbaar is. Het is daarmee duidelijk dat het voor NS uitgesloten is om op een later moment het oorspronkelijke MAC-adres nog terug te halen. Ten overvloede wordt hierbij opgemerkt dat dit MAC-adres, uitgaand van de daarover in de rechtspraak ontwikkelde criteria, voor NS niet als persoonsgegeven kwalificeert.

Alles overziend is NS van mening dat het volledige door haar ingerichte proces, voldoet aan de vereisten van de Wbp, mocht hier al sprake zijn van het verwerken van persoonsgegevens.

12. Informatie aan bezoekers van de stations

Sinds december 2016 informeert NS systematisch haar bezoekers van de betreffende stations door middel van een privacy statement op ns.nl/privacy en via stations.nl/privacy. Daarnaast zijn bij de ingangen van de betreffende stations stickers aangebracht die de toepassing van tracking onder de aandacht brengen.
Zie verder ook het antwoord op vraag 5.

13. Klachten van bezoekers van de stations

In de afgelopen vijf jaren is op zeven stations gebruik gemaakt van WiFi/BT tracking, zijnde Amsterdam Centraal, Amsterdam Zuid, Groningen, 's-Hertogenbosch, Leiden Centraal, Schiphol Airport en Utrecht Centraal, waarbij wordt opgemerkt dat het gebruik in Groningen inmiddels, na afronding van de herinrichting aldaar, is beëindigd.
NS heeft over WiFi/BT tracking op deze stations één klacht ontvangen.

14. Toelichting op waarborgen voor een veilige en integere verwerking

Toegang tot de database is beperkt tot ongeveer 10 personen en beheer en uitgifte van de accounts ligt bij NS zelf. Omdat de informatie in de database waartoe deze gebruikers toegang hebben alleen geaggregeerde gegevens bevat is er geen multifactor authenticatie toegepast.
Het netwerkverkeer is SSL versleuteld voor zowel de verbinding tussen de server en sensor alsook tussen de server en browser van de gebruiker.

Voor het najaar 2017 staat een audit van de beveiligingsmaatregelen door een externe, onafhankelijke partij geplanned. Desgewenst kunnen wij de uitkomsten daarvan met u delen.

15. Toelichting op de technische werkwijze met sensoren en de verdere verwerking door Blip Systems onder verantwoordelijkheid van NS.
Zie § 3.2 technologie in het Informatiebeleidsplan SMART station, bijlage document nummer 4.

♦ Op 11 augustus 2017 waren op de locaties als bedoeld bij het antwoord op vraag 6 de volgende aantallen Wifi/Bluetooth sensoren geïnstalleerd:

- Amsterdam Centraal: 34
- Amsterdam Zuid: 12
- 's-Hertogenbosch: 12
- Leiden Centraal: 5
- Schiphol Airport: 16
- Utrecht Centraal: 34

♦ Op welke wijze wordt voorkomen dat apparatuur van bezoekers buiten het station wordt gedetecteerd:
De fysieke bouwconstructie van stations (grotendeels beton, staal) en de relatief grote afstand tot de externe omgeving van het stationsgebouw, vormen een generieke technische beperking van het detectiebereik. Een verdere beperking wordt gecreëerd door de ingebouwde filters voor de signaalsterkte.

♦ Dubbeltellingen
NS heeft de keuze gemaakt om geen maatregelen te treffen die dubbeltellingen moeten voorkomen. Daar waar een aantal apparaten in samenhang wordt gedetecteerd, bijvoorbeeld een bezoeker die drie apparaten bij zich draagt, wordt dat als drie geteld. Het gaat NS uiteindelijk om statistisch inzicht in loopstromen. Niet gedetecteerde, maar wel aanwezige Wifi/BT signalen en dubbeltellingen doen naar het oordeel van NS geen afbreuk aan de algemene betrouwbaarheid van de verkregen informatie.

16. Oudste aanwezige records ruwe data in de database van Blip Systems zie bijlagen, documentnummers 7 en 8.
In de database van Blip Systems wordt ruwe data per dag in een tabel opgeslagen.
De oudste aanwezige dagtabel dateert van 15 maart 2017 (stand per 9 augustus 2017).
Zie hiervoor de schermafdruk van de database met de aanwezige dagtabellen, gesorteerd van oud naar nieuw (zie bijlage, document nr. 7).
Daarnaast treft u een schermafdruk van de geopende dagtabel van 15 maart 2017, met daarin de 10 oudste records bovenaan deze dagtabel (zie bijlage document nr. 8).

17. Verstrekking van tracking gegevens
NS heeft nimmer verzoeken of wettelijke vorderingen van opsporingsautoriteiten ontvangen om gegevens te verstrekken die zijn gegenereerd door WiFi/BT tracking.
NS heeft dergelijke gegevens ook niet op eigen initiatief verstrekt.

Wij hopen u met het voorgaande naar behoren te hebben geïnformeerd.
Mocht u over WiFi/BT tracking op stations van NS nog vragen hebben dan vernemen wij die graag.

Hoogachtend,

[redacted]

coördinator privacy NS Groep N.V.

Bijlage(n) Bijlagen nrs 1 t/m 8

Bijlagenummer	Naam document
1	De opdrachtbevestiging tussen NS en Blip Systems.
2	Artikel 50 van de IT-inkoopvoorwaarden van NS die van toepassing zijn op de relatie tussen NS en Blip Systems.
3	Publicaties in de media.
4	Informatiebeleidsplan SMART station.
5	Investeringsvoorstel, zijnde het document waaruit blijkt dat de directie van NS Stations B.V. haar goedkeuring heeft verleend aan het toepassen van WiFi/BT tracking.
6	Voorbeelden van resultaten.
7	Printscreen van de database waarop de aanwezige dagtabellen zichtbaar zijn en waaruit volgt dat de oudste aanwezige dagtabel dateert van 15 maart 2017 (stand per 9 augustus 2017).
8	Printscreen van de database waarop de geopende dagtabel van 15 maart 2017 zichtbaar is, met daarin de 10 oudste records bovenaan deze dagtabel.

Bijlagen bij de brief van NS van 14 augustus 2017 aan de Autoriteit Persoonsgegevens, met kenmerk NSL/2017/12426-2 inzake WiFi/BT tracking op stations van NS.

Hieronder treft u een overzicht aan van de bijlagen behorende bij bovengenoemde brief. In de brief wordt naar deze bijlagen verwezen onder vermelding van het hieronder genoemde nummer en op de bijlagen zijn de corresponderende nummers opgenomen.

Bijlagenummer	Naam document
1	De opdrachtbevestiging tussen NS en Blip Systems.
2	Artikel 50 van de IT-inkoopvoorwaarden van NS die van toepassing zijn op de relatie tussen NS en Blip Systems.
3	Publicaties in de media.
4	Informatiebeleidsplan SMART station.
5	Investeringsvoorstel, zijnde het document waaruit blijkt dat de directie van NS Stations B.V. haar goedkeuring heeft verleend aan het toepassen van WiFi/BT tracking.
6	Voorbeelden van resultaten.
7	Printscreen van de database waarop de aanwezige dagtabellen zichtbaar zijn en waaruit volgt dat de oudste aanwezige dagtabel dateert van 15 maart 2017 (stand per 9 augustus 2017).
8	Printscreen van de database waarop de geopende dagtabel van 15 maart 2017 zichtbaar is, met daarin de 10 oudste records bovenaan deze dagtabel.

Bijlage 1 bij de brief van 14-08-2017 met kenmerk NSL/2017/12726.

NS Stations

Exploitatiebedrijf

Stationshal 17
Postbus 2534
3500 GM Utrecht
www.nsstations.nl

Postbus 2534, 3500 GM Utrecht
BLIP Systems A/S
[redacted]
Hækken 2, Vester Hassing
9310 Vodskov, Denmark

Datum 23 juli 2013
Ons kenmerk AD/JvdH/2013/smartstation01
Onderwerp Purchase order SMART Station Utrecht Centraal

Telefoon [redacted]
Telefax -
E-mail [redacted]@nsstations.nl

Dear Mr. [redacted] dear [redacted]

I am happy to inform you that NS Stations has agreed to purchase the products and services as specified in (1) our Request for Proposal of 14 November 2012, including appendices, (2) the Information Notice of 4 December 2012, including appendices, and (3) your final Proposal of 28 January 2013, including appendices. The purchase order includes support and maintenance for two years, starting from the date at which SMART Station is fully operational at Utrecht Central station.

In case of inconsistencies between the documents in which the products and services are specified, the document with a higher rank in the following list prevails over all others:

1. NS Stations' Information Notice of 4 December 2012, including appendices (appendix 1)
2. NS Stations' Request for Proposal of 14 November 2012, including appendices (appendix 2)
3. BLIP Systems' final Proposal of 28 January 2013, including all appendices (appendix 3)

By signing this letter BLIP Systems A/S agrees to deliver all products and services in accordance with the specifications, terms and conditions stated in the listed documents above. BLIP Systems agrees that the scanunits will be installed at the station by a Third Party appointed by NS Stations.

NS Stations aims to purchase an end to end solution. Therefore, we have agreed that BLIP Systems is allowed (and encouraged) to check the installation works by the Third Party. We have agreed that BLIP Systems will approve the installation by the Third Party in accordance with the procedure described in appendix 4, step K.

After approval of the installation of the scanunits at Utrecht Central station BLIP Systems is fully responsible for the performance of its products and services in accordance with the specifications and the intended use. Support and maintenance service levels are specified in the Service Level Agreement (appendix 5). Non-performance of one or more scanunits which reasonably can be attributed to changes in the station environment including power and connectivity, are excluded from this responsibility.

Because this is our first joint project with many learnings, I want to emphasize the importance of compliance of all parties involved with the split between the realization phase (steps F-P in appendix 4) and the operational phase (from step Q onwards). After finalizing the installation and calibration of the scanunits at Utrecht Central station, I suggest that we organize a (second) kickoff at your office in Denmark to start the design of the SMART Station server with all its data filters, information queries and presentation tools.

The total purchase order amounts [redacted] (excluding VAT), referring to the pricing scheme which we have agreed on (see appendix 6). BLIP Systems and NS Stations have agreed on the invoicing schedule which is described in appendix 7. Referring to the purchase order number [redacted], invoices can be sent to:

NS Stations BV
Crediteurenadministratie
Postbus 2534
3500 GM Utrecht
The Netherlands

I kindly ask you to return a signed copy of this letter to confirm the acceptance of this order under all terms and conditions stated. I am counting on a successful en smooth implementation of SMART Station at Utrecht Centraal, which is the showcase for all of us!

Kind regards,

[redacted]

NS Stations

Confirmation of agreement

Blip Systems A/S
[redacted]
Voskov, 23 July 2013

[redacted]

NS Stations B.V.
[redacted]
Utrecht, 23 July 2013

[redacted]

Appendices

Appendix 1: NS Stations' Information Notice of 4 December 2012, including appendices
Appendix 2: NS Stations' Request for Proposal of 14 November 2012, including appendices
Appendix 3: BLIP Systems' final Proposal of 28 January 2013, including all appendices
Appendix 4: Project procedures & processes SMART Station Utrecht Centraal
Appendix 5: Service Level Agreement for SMART Station Utrecht Centraal
Appendix 6: Detailed pricing scheme for SMART Station Utrecht Centraal
Appendix 7: Invoicing schedule

Bijlage 2 bij de brief van 17-08-2017 met kenmerk IISZ/2017/12720-2

doubt, NS shall be entitled to forbid their use and the Other Party shall be obliged to remove the tools or equipment in question and replace them as soon as possible with tools or equipment that do meet these requirements. Any resulting delay in the performance of the Services shall be the responsibility of the Other Party. Inspection of tools and equipment by NS does not relieve the Other Party from any responsibility and/or liability arising from their use.

49. Working conditions, health and safety

The Other Party is responsible for the working conditions, health and safety on the site. The Other Party shall observe all applicable legal requirements, regulations of the Arbeidsinspectie (Labour Inspectorate) and local health and safety regulations.

50. Processing of personal data

50.1 The terms of this Article 0 are applicable where the Services to be provided by the Other Party (partly) involve the processing of personal data on behalf of NS.

50.2 The Other Party shall always process personal data in accordance with the provisions of the Personal Data Protection Act [Wet bescherming persoonsgegevens] and any other applicable regulations, conditions and provisions.

50.3 Subject to any contrary legal obligations, the Other Party and anyone acting on its authority may process personal data only on the instruction of NS. Processing operations expressly described in an Order Form or Agreement are deemed to be carried out on behalf of NS. Other processing operations may only be carried out with the prior written consent of NS.

50.4 Without prejudice to Article 24 , the Other Party shall treat the personal data coming to its attention during execution of the Service as confidential, except insofar as it is legally obliged to disclose such information or the performance of its task necessitates disclosure. The Other Party shall impose the obligation to treat personal data as secret on all persons acting under its authority and having access to the personal data to be processed.

50.5 The Other Party shall take technical and organisational measures to protect the personal data to be processed by it on behalf of NS against loss or any form of unlawful processing. Taking into account the state of the art and the costs of compliance, these measures shall guarantee an appropriate level of protection, bearing in mind the risks entailed by the processing and the nature of the data to be protected, and must also be directed towards avoiding unnecessary collection and further processing of personal data. To allow NS to monitor fulfilment of the said measures, the Other Party shall inform NS of the measures taken before starting any processing of personal data.

50.6 The Other Party shall process personal data on behalf of NS only in the Netherlands.

50.7 The Other Party should safeguard NS from any financials penalties from 'Dutch Data Protection Authority'.

51. Laws and regulations

The Other Party, its personnel and third parties engaged by it are obliged strictly to comply with and observe all regulations, conditions and provisions, insofar as they relate to the Services to be provided by it.

52. Subcontracting; social security and tax obligations

52.1 The terms of this Article are only applicable if the Other Party has, or wishes to have, obligations under the agreement carried out by third parties.

52.2 The Other Party is not entitled to have any part of the Agreement carried out by third parties or to use personnel hired from outside without first having received the written consent of NS. In this context the term third parties excludes businesses forming part of the same Group of companies as that to which the Other Party belongs and for which the Group has given an express guarantee. The Other Party safeguards NS against any claim that a social security administration agency and/or tax department claims to have against NS on the basis of temporary staff hirer's liability and/or sequential liability.

52.3 The Other Party gives an assurance to NS that it will meet, in good time, all its obligations under applicable tax and social security legislation in relation to the staff employed or to be employed by the Other Party or by a third party engaged by the Other Party in the context of the performance of the agreement.

52.4 The Other Party is obliged to supply NS in writing, immediately upon request, before and/or after the commencement of execution of the Agreement, with the name and address of the social security administration agency with which the Other Party is registered, the membership number under which the Other Party is registered with the social security administration agency (as evidenced by a valid certificate of registration) and its salaries tax number.

52.5 The Other Party is obliged to present NS, immediately upon request, with a declaration of the social security administration agency and the tax authority concerning the payment history of the Other Party, which declaration shall not be more than three months old.

52.6 Insofar as activities under the Agreement are carried out on the site of NS, the Other Party shall, immediately upon request, before starting to execute the Agreement and also every week during execution, furnish a written statement

Bijlage 3 bij de brief van 17-08-2017 met kenmerk NL/2017/12426-2

Met wifi-tracking naar een optimaal netwerk

Wie met zijn smartphone op zak in het ov reist, is een waardevolle bron van informatie. De wifi- en bluetooth-signalen die de telefoon verspreidt kunnen vervoerders gebruiken voor crowd control, een betere inrichting van het station en zelfs voor optimalisatie van het netwerk.

AUTEUR VINCENT WEVER FOTO ROSTISLAV GLINSKY / SHUTTERSTOCK

Station Schiphol Airport.

NS meet sinds 2013 op een aantal grote stations via tientallen wifi- en bluethooth-trackers de reizigersstromen. Het project Smart Station begon met een proef in Groningen, die alweer weer is beëindigd. Inmiddels hangen er sensoren in Utrecht Centraal, Leiden Centraal, Amsterdam Centraal, Amsterdam Zuid en 's-Hertogenbosch. De vetste kluif voor data-analisten is misschien wel station Schiphol Airport.
"Toen we in 1995 Schiphol Plaza openden met het station er recht onder, zag het er hier totaal anders uit", zegt Jeroen van den Heuvel, stationsontwikkelaar bij NS. Trots voeren hij en collega-onderzoeker Rik Schakenbos de geuzennaam 'loopstroomnerd'. "Er waren ten eerste veel minder passagiers, zowel per trein als met het vliegtuig. En er stonden veel minder objecten. Als je ziet wat er nu staat aan incheckpalen, kaartautomaten, bewegwijzering..."
Schiphol Plaza heeft nu alle eigenschappen van een echt plein. Mensen lopen kriskras door elkaar. Een duidelijke routing ontbreekt. Daardoor is het ondoenlijk om nog handmatig te tellen, met werkstudenten. Er moest dus iets anders gebeuren. Nu houdt NS tot op de seconde nauwkeurig bij hoeveel mensen zich waar bevinden met behulp van stereocamera's en volgers, sensoren die het wifi- en bluetooth-signaal uitpeilen dat reizigers met hun mobiele telefoon uitzenden. Een miljoeneninvestering, verzekert Van den Heuvel. Op het treinstation Schiphol Airport alleen al hangen 48 apparaten, verspreid over de hal en de perrons.

Privacy

Je gaat ze pas zien als je ze doorhebt. En soms zijn ze helemaal onzichtbaar, verstopt in bijvoorbeeld een kaartautomaat of de balie van de servicedesk. Op bepaalde plekken kan je zomaar worden opgepikt door zes of zeven sensoren, als je in ieder geval je wifi of bluetooth hebt aanstaan. Want alleen dan gaat je telefoon automatisch op zoek naar een netwerk. Van dat 'vragende' signaal maken de sensoren gebruik; ze registreren het en slaan het op.
Daarmee komt ook direct de vraag rond privacy om de hoek kijken. Volgens Schakenbos hoef je je daar geen zorgen om te maken. "Dit systeem is *designed by privacy*. Dat was dus het uitgangspunt." Voor het signaal wordt opgeslagen wordt het MAC-adres, de unieke code van elk mobiel apparaat, twee keer *gehasht* of geanonimiseerd. "Ja, daar zijn de exploitanten van de winkels wel chagrijnig over", lacht Van den Heuvel.
In december 2015 bepaalde het (toenmalige) College Bescherming Persoonsgegevens dat het *tracken* van het wifi-signaal niet zomaar mag. Mensen moeten vooraf worden geïnformeerd. En NS mag de data niet zonder hashen opslaan en verwerken. Naar aanleiding van de uitspraak hield NS de methode nog eens tegen het licht. Smart Station bleek binnen de grenzen van de wet te vallen. Alle gegevens blijven bovendien binnen de EU, en in bezit van NS.
Op het station stellen pictogrammen en een verwijzing naar een website de reiziger ervan op de hoogte dat hun signaal kan worden gevolgd. Van den Heuvel: "In 2012 hebben we dit al geprobeerd, maar toen bleken mensen alleen een pictogram niet te begrijpen. Mensen dachten dat ze er gratis wifi konden krijgen."

Toeristentrap

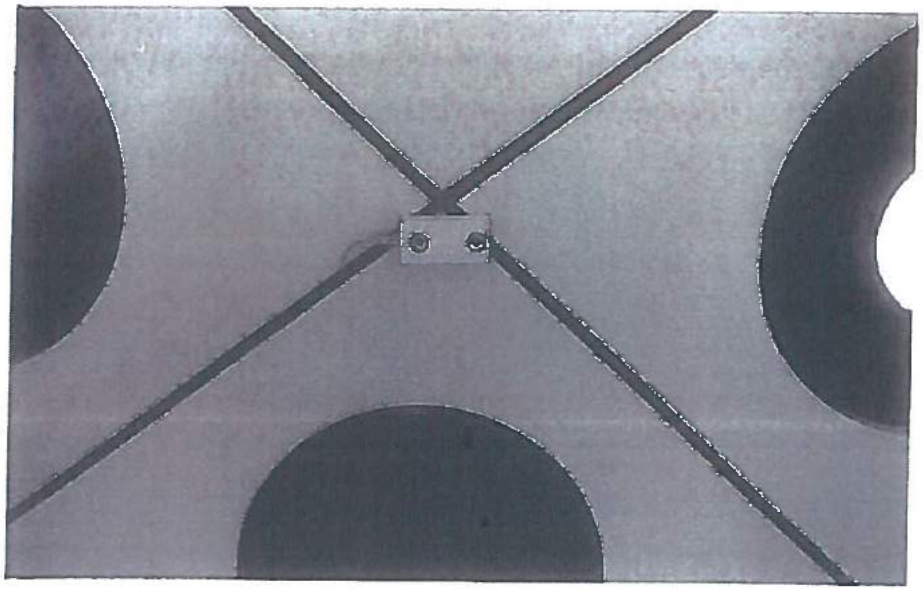
We gaan richting de roltrappen van spoor 1-2, waar de treinen richting Amsterdam vertrekken. In officieus jargon de 'toeristentrap'. "Wist je dat deze ene roltrap dagelijks 20.000 reizigers naar het perron vervoert? Dat zijn meer instappers dan op het hele station Breda", aldus Van den Heuvel. Hij wijst naar boven naar de zwarte luifel boven de roltrap. "Daar hangt zo'n sensor." Het is een klein wit kastje met twee gaatjes. Je loopt er zo aan voorbij. "Dit is een stereoscopische camera."
Op basis van de toenmalige voetgangersmodellen bleek het onmogelijk om de omgeving in te richten. Van den Heuvel: "We zijn de trappen toen heel lomp met bouwhekken gaan afsluiten om te kijken wat er gebeurde. Door de tel- en tracksensordata te analyseren kwamen we tot de inzichten die ProRail en NS nodig hadden om het station te verbeteren. Zo is een hellingbaan aan de Hoofddorpzijde vervangen door een vaste trap, en een vaste trap door een roltrap. Dat bleek veel beter voor de doorstroming. We doen hier dus aan reizigersgedreven stationsontwerp."

Gele hesjes

Op het perron zoeken we een plek op onder een van de informatieschermen, net onder de roltrap. Schakenbos klapt zijn iPad open. "Kijk, hier zie je dit deel van het perron opgedeeld in secties. Dat meten we met stereocamera's. Doe maar eens een stapje opzij en je zal zien dat de teller in het ene vakje omlaag gaat en het andere vakje omhoog." En inderdaad: nauwkeurig meet de applicatie waar het druk is en waar niet. "Als het te druk dreigt te worden, komen de 'gele hesjes' in actie; dat zijn de servicemedewerkers die als het rustig is informatie geven en anders aan *crowd control* doen. Vergis je niet, van een roltrap kunnen zo zeventig tot tachtig mensen per minuut komen. Die moeten allemaal een plekje vinden op het perron. En zoals we allemaal weten, is dat op Schiphol best een

Vreetschuur

Toen NS op Schiphol begon te meten, waren er een paar onverwachte bijeffecten. Zo bleken infraroodsensoren op het station niet nauwkeurig genoeg. "Die zagen een duif soms aan voor een voetganger." Bovendien was het soms veel te druk voor de klassieke infraroodsensoren. Stereocamera's kunnen wel precies reizigers tellen.
Ook bleken er elke nacht van vrijdag op zaterdag een raadselachtig groot aantal overstappers tussen treinen. Vreemd, omdat er op dat tijdstip slechts één trein Schiphol aandoet: de nachtnettrein. De overstappers bleven ook allemaal precies even lang, namelijk 58 minuten. Na ter plekke te hebben gekeken, was het mysterie opgelost. Het ging om stappers die midden in de nacht op Schiphol een Burger King vonden die nog open was en daarna de volgende trein pakten. Van den Heuvel: "Deze Burger King blijkt de nachtelijke vreetschuur van de Randstad."



De stereocamera zie je alleen als je er op let.

uitdaging." Via oortjes krijgen de medewerkers te horen dat ze mensen moeten verspreiden over het perron, of een trap voor korte tijd moeten afsluiten als het perron vol is.

Feyenoord

Ook de RET zet wifi-tracking in als middel voor crowd control. Dat is met name nodig op drukke dagen, zoals tijdens North Sea Jazz of de marathon van Rotterdam, tegt Beatrix Lourens, manager sociale veiligheid van de RET uit. Met name de marathon is een uitdaging voor de vervoerder, omdat een groot deel van het parcours parallel loopt aan het metronet. Mensen pakken de metro van halte naar halte om op verschillende plekken deelnemers aan te moedigen. "Als we zien dat het te druk wordt, sluiten we soms een station voor korte tijd af of leiden we de mensen om", aldus Lourens. Dat gebeurde onlangs ook bij de huldiging van Feyenoord. Bovendien heeft de RET de loopstromendata gebruikt om de plaatsing van verkoopautomaten en bewegwijzering op metrostations aan te passen.

Routeadvies

Londen gaat nog een stapje verder. De techsite Gizmodo vroeg eerder dit jaar gegevens op bij Transport for London (TfL) in het kader van de Britse Wet Openbaarheid Bestuur. TfL blijkt de verzamelde gegevens via wifi- en bluetooth-tracking niet alleen te gebruiken voor de looproute binnen metrostations maar ook om te kijken hoe mensen hun weg vinden in het dichtvertakte metronet van Londen. Want veel stations zijn op verschillende manieren te bereiken. Maar liefst 54 metrostations kregen wifi-trackers, en dit was nog maar een eerste proef.

Ook in Londen moet je in- en uitchecken (met de Oyster-card) maar verder was het voor TfL gissen hoe passagiers hun reis maken. Dat werd voor het eerst inzichtelijk. Zo bleek 44 procent van de reizigers tussen Victoria en Liverpool Street gebruik te maken van de snelste verbinding, al had die een overstap. 26 procent van de reizigers verkoos de directe, maar langzamere verbinding via de Circle Line. "Door wifi-data te gebruiken en te combineren met geaggregeerde data van de Oyster Card en die van contactloos betalen, zouden we een veel rijkere databron hebben om zo op meerdere gebieden optimale planningsbeslissingen te nemen", schrijft TfL.

Ook ziet TfL mogelijkheden om het adverteren te verbeteren, door bijvoorbeeld reclame te laten zien op plekken waar mensen even stilstaan. Op termijn wil de autoriteit, net als in Nederland, automatisch betalen op basis van je locatiegeschiedenis mogelijk maken. In een vergezicht denkt de Londense vervoerautoriteit reizigers een routeadvies te kunnen geven: welke trap is sneller, de vaste of de roltrap? Mocht een fiets sneller zijn dan de bus, die real-time wordt gevolgd via bluetooth, dan krijg je dat advies. Maar voortopig is dat nog toekomstmuziek.

Netwerkanalyse

In Nederland is het ook nog niet zo ver. Maar over netwerkanalyse denkt NS wel na. Van den Heuvel: "We hebben de apparatuur nu op de belangrijkste spoorknooppunten hangen, dus we kunnen de meerwaarde van netwerkanalyse nu verzilveren." Het project staat nog in de kinderschoenen. Van den Heuvel hoopt dat NS hiervoor snel een aantal mensen kan vrijmaken. Zo wil hij graag wifi-tracking op station Schiphol uitbreiden door een koppeling met de luchthaven te maken. "Met het autoverkeer is het verzamelen van netwerkdata via tracking heel normaal, maar in voetgangersland is dit revolutionair. Het zou helemaal mooi zijn als we ook drukte kunnen gaan voorspellen op basis van wifi-tracking. Want drukte bij de bagageband betekent onvermijdelijk een half uur later drukte op het perron."

station	wifi/bluetooth	infrarood-/stereocamera	totaal
Utrecht Centraal	24	31	55
Leiden Centraal	5	2	7
Schiphol Airport	21	27	48
Amsterdam Centraal	30	12	42
Amsterdam Zuid	12	26	38
's-Hertogenbosch	12	4	16
totaal	104	102	206

PRIVACY & COMPLIANCE

TIJDSCHRIFT VOOR DE PRAKTIJK

03/2013

Baltzer *Science* Publishers

ISSN 2211-3754

Bijlage 3 bij de brief dd 17-06-2014 met kenmerk 1201411127.20-2

COLOFON

Privacy & Compliance
Baltzer Science Publishers
Tel +31 6 53 88 1602
info@baltzersciencepublishers.com
www.baltzersciencepublishers.com

Redactie
Mr. drs. J. (Jeroen) Terstegge,
(Hoofdredacteur) PrivaSense
K.J. (Klaas) Bruin, KLM
Mr. H. (Huib) Gardeniers, NetzLegal Consultants
Mr. S.H. (Sergej) Katus, Privacy Management Partners
Dr. J.A.G. (Koen) Versmissen, CIPP/E,
Privacy Management Partners

Vaste medewerkers
Mr. F. (Friederike) van der Jagt, Stibbe
Mr. dr. E.P.M. (Elisabeth) Thole, Van Doorne

Redactiesecretaris
Dr. J.A.G. (Koen) Versmissen, CIPP/E,
Privacy Management Partners
06 81678016
koen.versmissen@pmpartners.nl

Bureauredacteur / vormgeving
Eric G.F. van den Berg
ericgfvandenberg@gmail.com
Omslag en format:
Tom van Staveren
graphicisland@upcmail.nl

Abonnementsprijs
2013, Jaargang 2, 1-6, € 175,00 excl. BTW, incl. verzendkosten (in Nederland). De prijs is exclusief online toegang, voor online toegang en meerdere gebruikers is een prijsmodel te raadplegen op de website: http://www.baltzersciencepublishers.com/nl/general/bestelformulier

Nieuwe abonnementen
Abonnementen kunnen worden gestart per 1 januari van een kalenderjaar. Valt de aanvraag van een abonnement niet samen met het begin van een kalenderjaar, dan worden de reeds verschenen nummers van dat kalenderjaar alsnog verzonden en wordt de prijs van een volledige jaargang in rekening gebracht. Nieuwe abonnementen kunnen schriftelijk, per fax, per telefoon of per email worden opgegeven.

Adreswijziging
Bij adreswijziging wordt u verzocht deze zo spoedig mogelijk en bij voorkeur schriftelijk door te geven aan de uitgeverij onder vermelding van: adreswijziging Privacy & Compliance.

Beëindiging abonnement
Abonnementen kunnen alleen schriftelijk, tot 1 december van het lopende abonnementsjaar, worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch voor een kalenderjaar verlengd.

ISSN: 2211-3754 • E-ISSN: 2211-3762

Baltzer
Science
Publishers

INHOUDSOPGAVE

PRIVACY BY DESIGN BIJ REIZIGERSMETINGEN OP STATIONS

*Jeroen van den Heuvel, Eelco Thiellier, Niels van Gerwen**

In maart van dit jaar ontstond discussie over het tracken en tracen van reizigers op het station van Groningen met behulp van het volgsysteem SMART Station. De projectvoerders geven uitleg over de intrinsieke privacybescherming van het systeem. SMART Station wordt binnenkort ingezet op Utrecht CS en krijgt daarna ook bredere toepassing.

Het belang van reizigersmetingen op stations

Aantrekkelijk openbaar vervoer is belangrijk voor de kwaliteit van wonen, werken, ondernemen en recreëren in Nederland. Vervoer per trein neemt hierbij een belangrijke positie in omdat de trein een aantrekkelijk en duurzaam alternatief is voor de auto, en – op Europese schaal – ook voor het vliegtuig. Het voordeel van reizen per openbaar vervoer is de mogelijkheid om de tijd onderweg te gebruiken voor andere activiteiten, zoals werken, lezen of slapen.
De achilleshiel van reizen per openbaar vervoer is de keten van verschillende vervoerwijzen waarmee de reiziger van deur tot deur reist. De reiziger moet altijd een rit maken naar een halte of station, om vervolgens met bus, tram, metro of trein het grootste deel van de totale reisafstand te overbruggen. Op de bestemming aangekomen, is meestal nog een rit naar de eindbestemming nodig. Tussen deze verschillende schakels in de keten moet van de ene vervoerwijze op de andere worden overgestapt. In veel gevallen gebeurt deze 'transfer' op en rond treinstations. Wetenschappelijk onderzoek toont aan dat de transfer op knooppunten door de reiziger verreweg als zwakste schakel in de reisketen van deur tot deur wordt ervaren.[1] Hoewel er de laatste jaren op stations al veel vooruitgang is geboekt, ligt hier dus nog steeds de kans om het reizen per openbaar vervoer naar een structureel hoger niveau te tillen.

Meten is weten

Het begrijpen van het functioneren van het station, het stationsgebied en het gedrag van reizigers hierbinnen, is cruciaal voor het verbeteren van die noodzakelijke schakel in de reisketen. Met inzicht in de werking van stations kunnen deze beter ontworpen worden, en kan de dienstverlening op het station beter worden afgestemd op de behoefte van reizigers. Op deze manier kunnen reizigers ook bij grote drukte – het gaat al snel om duizenden mensen tegelijk – comfortabeler en veiliger van stations gebruik maken.
Inzicht in aantallen, looptijden en wachttijden is belangrijk voor de inrichting van transfervoorzieningen zoals roltrappen, trappen, deuren, perrons en passages. Inzicht in aantallen is niet alleen belangrijk voor reguliere situaties – bijvoorbeeld een ochtendspits op een drukke maandag – maar is ook belangrijk voor bijzondere situaties zoals bij verstoring van de dienstregeling of evenementen waarbij honderdduizenden reizigers in korte tijd naar of van een stad willen reizen. Bijvoorbeeld tijdens Koningsdag of de Nijmeegse Vierdaagse. Inzicht in looproutes van passanten is essentieel voor een goed aanbod van diensten in en rond het station, zoals ticketing, reisinformatie en retail. Kortom: meten is weten.

Onze uitdaging

Tot voor kort bestonden passantenmetingen op stations in Nederland alleen uit handmatige tellingen en enquêtes, die meestal werden uitgevoerd door studenten. Een dergelijke aanpak heeft twee grote nadelen. Ten eerste is het een zeer kostbare aangelegenheid omdat een groot aantal mensen nodig

* **Jeroen van den Heuvel** is stationsontwikkelaar bij NS Stations en doet promoticonderzoek aan de Technische Universiteit Delft. **Eelco Thiellier** en **Niels van Gerwen** zijn consultants bij NPC, onderdeel van Royal HaskoningDHV. NPC is het projectmanagement- en adviesbureau voor NS, ProRail en regionale vervoerders voor (her)ontwikkeling van stationsgebieden.

1 Zie bijvoorbeeld *Waiting Experience At Train Stations*, door Mark van Hagen (ISBN: 9789059725065)

SMART Station concept

is om de telling uit te voeren. Voor een middelgroot station zijn tientallen medewerkers tegelijk nodig om een goed beeld te krijgen van alle loopbewegingen. Voor een groot station loopt dit al snel op tot vijftig of meer.
Ten tweede is de waarde van ingewonnen informatie beperkt, omdat vanwege de hoge kosten de duur van de tellingen wordt beperkt tot één of enkele dagen. Hierdoor is de statistische betrouwbaarheid van de gegevens beperkt, omdat een specifieke dag flink kan afwijken van het gemiddeld patroon of de situatie bij bijvoorbeeld verstoringen of evenementen.

Wij stonden voor de uitdaging was om een methode te bedenken waarmee op geautomatiseerde wijze passantenstromen op stations over een langere periode inzichtelijk kunnen worden gemaakt.

Bluetooth-tellingen

In het wetenschappelijk en praktisch onderzoek naar voetgangers zijn de laatste jaren diverse ontwikkelingen gaande, die in principe ook voor stations bruikbare instrumenten opleveren. Zo is het geautomatiseerd meten van verkeerstromen in andere vervoersectoren al veel langer gemeengoed, waarbij het opvangen van Bluetoothsignalen uit smartphones en tablets een belangrijke rol speelt om dubbeltellingen te voorkomen.

- Op veel wegen wordt het aantal auto's en hun snelheid gemeten door middel van detectielussen in het wegdek en/of videocamera's langs of boven de weg. Met behulp van Bluetoothmetingen worden routetijden bepaald, die vervolgens voor verkeerskundig onderzoek worden gebruikt of op de grote informatiepanelen langs of boven de weg wordt getoond.[2]

- Op luchthavens worden met behulp van Bluetooth wachtrijen en wachttijden bij de douane gemeten, en worden de looproutes en verblijftijd van passanten gemeten om het winkelaanbod hierop af te stemmen.[3]

- In binnensteden is inzicht in bewegingspatronen belangrijk om problemen op het gebied van infrastructuur en voorzieningen op te lossen of te voorkomen. Ook hiervoor worden sinds kort Bluetoothmetingen ingezet.[4]

Hoewel de technologie voorhanden is om passantenstromen nauwkeurig te meten, bleek deze niet zonder meer geschikt voor stations. Ten eerste omdat passantenstromen op stations kortstondig zó intensief kunnen zijn – meer dan tienduizend passanten per uur via één passage – dat de bestaande technologie te kort schiet om bruikbare meetresultaten leveren. Sommige bestaande systemen kunnen de reizigers letterlijk niet meer bijhouden zodra de spits begint. En juist op de drukke momenten zijn de meest nauwkeurige gegevens nodig om een station goed te kunnen ontwerpen en laten functioneren.
Ten tweede omdat een station als een groot plein functioneert, waarbij veel verschillende stromen passanten samenkomen en kriskras door elkaar bewegen. Auto's op een weg blijven binnen de witte lijnen, fietsers blijven (meestal) op het fietspad of de weg, en passanten in een binnenstad zijn altijd wel toe te wijzen aan een specifieke straat. Op stations zijn voetgangers veel vrijer, waardoor het bijzonder lastig is om achterhalen welke passant welke route precies heeft gelopen.

Na een flinke zoektocht hebben we vastgesteld dat er voor stationsmetingen niet meteen panklare oplossingen bestonden.

2 Zie bijv. http://www.verkeerskunde.nl/bluetooth
3 Zie bijv. http://www.futuretravelexperience.com/2012/11/houston-airports-adopt-bluetooth-based-queue-measurement/
4 Zie bijv. http://www.bk.tudelft.nl/over-faculteit/afdelingen/urbanism/onderzoek/urbanism-on-track/sensing-the-city/project/

Onze oplossing: SMART Station

Om een geschikte oplossing te ontwikkelen hebben NS Stations en NPC – dochter van RoyalHaskoningDHV – de handen ineen geslagen en in één jaar tijd een volledig nieuwe oplossing ontwikkeld: SMART Station. Bij SMART Station worden meerdere meetsystemen tegelijkertijd ingezet. Deze tellen en registreren reizigersbewegingen, en verwerken dit automatisch tot een totaalbeeld van een actuele situatie op en/of rond het station. Op die manier wordt de informatie verkregen die nodig is voor het ontwerp, evaluatie of management van stations.

SMART Station bestaat uit meerdere modules:

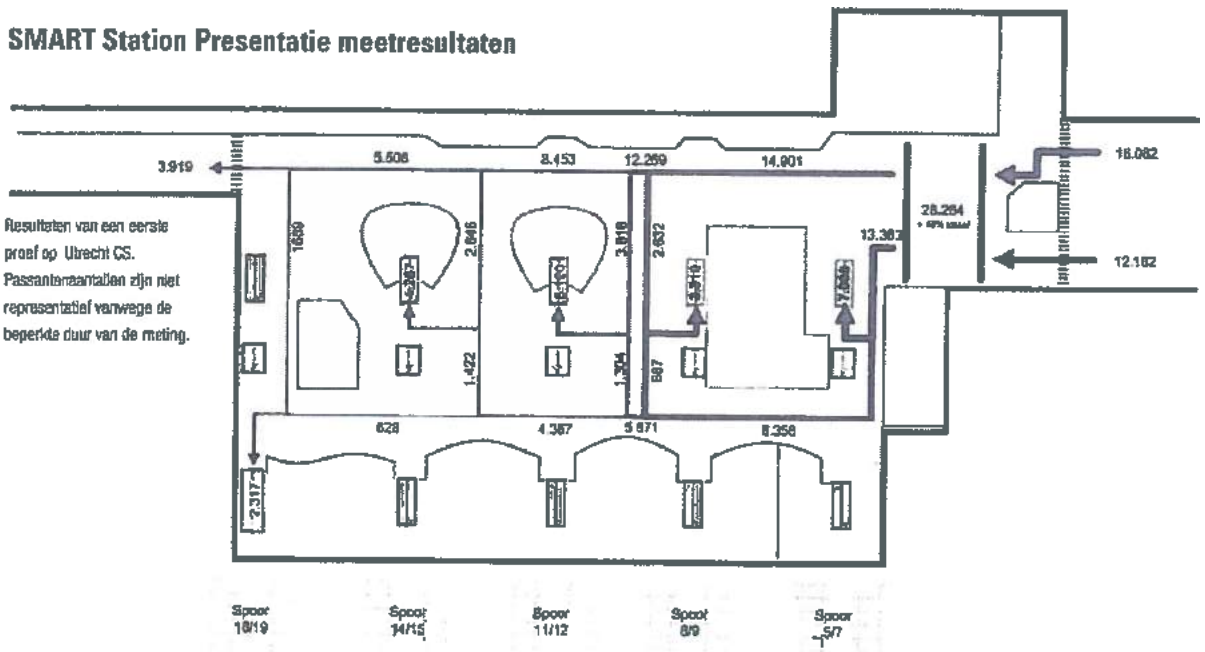
- tel- en volgmodules;
- een analysemodule;
- en een presentatiemodule.

Tellen gebeurt met behulp van infraroodtechnologie. Volgen gebeurt door op verschillende plaatsen in een station, de MAC-adressen (unieke hardwarenummers) van Bluetooth- en WIFI-devices op te vangen. Door de sensoren strategisch te plaatsen, kan aan de hand van de MAC-adressen, detectietijdstippen en de plaats van sensoren een reconstructie worden gemaakt van de looproute van een passant, en hoe lang deze passant over deze route heeft gedaan.
Omdat niet iedereen een Bluetooth/WIFI-device op zak heeft, zijn telefoon uit heeft staan of Bluetooth en/of WIFI niet heeft ingeschakeld om de batterij te sparen, worden de gegevens van de volgsensoren door de analysemodule gecombineerd met de gegevens uit de telsensoren. Op die manier kan met behulp van de presentatiemodule op ieder willekeurig moment een totaalbeeld van de reizigersstroom op een station worden verkregen (zie afbeelding).

Privacyoverwegingen

Omdat SMART Station *mensen*stromen in kaart brengt, is bij de ontwikkeling van het systeem steeds rekening gehouden met de privacybescherming van passanten. Om deze reden zijn we vroeg in het ontwikkelproces van SMART Station samen met gespecialiseerde adviseurs en juristen dieper in de materie gedoken om SMART Station privacyproof te ontwerpen.
Om privacyredenen worden MAC-adressen niet geregistreerd in combinatie met gegevens over de eigenaar/gebruiker van apparatuur. Het SMART Station-systeem 'ziet' alleen nummers om passanten op een anonieme manier te kunnen onderscheiden. Meer informatie heeft SMART Station niet nodig. Gebruikers van SMART Station kunnen die nummers niet gebruiken voor identificatie. Zuiver wettelijk werkt het systeem dan ook niet met 'persoonsgegevens' in de zin van de Wet Bescherming Persoonsgegevens.
We vonden en vinden echter dat onze verantwoordelijkheid verder gaat dan de wet. Stations staan vaak midden in de stad en worden door miljoenen mensen bezocht. Gebruikers van

SMART Station Presentatie meetresultaten



SMART Station zijn daarmee kwetsbaar voor negatieve maatschappelijke perceptie en hebben ook rekening te houden met de mogelijkheid van juridische discussie over 'persoonsgegevens' en wetgevingsontwikkelingen.

Privacy by Design

Om de oplossing nog breder toepasbaar te maken – ook internationaal – hebben we besloten om het privacy aspect zo diep en goed mogelijk binnen SMART Station te verankeren. We hebben hierbij gebruik gemaakt van drie bronnen van inspiratie: de Wet Bescherming Persoonsgegevens, de Privacybeleidskaders van NS met de privacy officer van NS als hoeder hiervan, en ons eigen gezond verstand. Dit heeft geresulteerd in een concept 'informatiebeleidsplan' voor SMART Station, waarmee we het ontwerptraject zijn ingegaan. Het informatiebeleidsplan beschrijft op welke wijze privacy gewaarborgd wordt in de technologie, processen en organisatie van SMART Station, dus op drie niveaus tegelijkertijd.
We hebben dit getoetst op een vroeg prototype van SMART Station middels een privacy audit door externe privacy specialisten. De aanbevelingen van deze audit hebben we doorgenomen met de privacy officer van NS, en vervolgens doorgevoerd in zowel het informatiebeleidsplan als het vervolg van het ontwerptraject.

De door ons gekozen weg komt overeen met het principe van *Privacy by Design*. De basisgedachte daarbij is implementatie van privacy beschermende maatregelen vanaf de start van de ontwikkeling van een technologie tot en met het beëindigen van het gebruik van de technologie. Hierdoor wordt het privacy-aspect een integraal onderdeel van de technologie en de gebruiksprocessen, waardoor de gebruikers van de oplossing maximaal worden gedwongen dan wel gestimuleerd om privacybewuste keuzes te maken.

Drie niveau's

Zoals gezegd is de privacywaarborg op drie niveaus in SMART Station geïntegreerd:

1. **Op technisch niveau,** door gebruik van *Privacy Enhancing Technologies* (PET). Meest belangrijk is de onomkeerbare versleuteling van de door de telmodule ingewonnen MAC-adres gegevens ('one way-hashing'). Deze versleuteling vindt direct bij de sensor plaats op basis van 256 bit-encryptie. Door die conversie worden de originele gegevens meteen bij de bron alweer vernietigd. De versleuteling vindt bovendien plaats met gebruikmaking van datum-informatie. Hierdoor levert de conversie van hetzelfde MAC-adres, ieder dag weer een andere telcode op. Het is op die manier onmogelijk om aan de hand van meerdaagse metingen individuele profielen op te bouwen van terugkerende reizigers.

2. **Op proces-niveau**. De opslag van gegevens is in de tijd gelimiteerd. De telgegevens worden na analyse automatisch weggegooid. Ook is SMART Station met verschillende autorisatieniveaus uitgerust, waardoor alleen de mensen die met bepaalde gegevens mogen werken, daar ook bij kunnen. Privacy is daarnaast nog een selectiecriterium in het inkoopproces: leveranciers moeten door middel van referenties én een kleinschalige praktijktest aantonen dat ze volledig volgens het informatiebeleidsplan SMART Station werken.

3. **Op organisatie-niveau.** Hoewel we met de technologie en de processen alle voorzienbare issues hebben ondervangen, vonden we het belangrijk om ook aandacht te schenken aan de cultuur van de organisatie rond SMART Station. Medewerkers worden geïnformeerd over het informatiebeleidsplan. Hierdoor wordt de kans op problemen tot een minimum teruggebracht. Op bedrijfsniveau is afgesproken om iedere twee jaar een audit uit te voeren om te toetsen of alles conform het informatiebeleidsplan SMART Station verloopt, en zo niet, op welke wijze moet worden bijgestuurd. Bij gerede twijfel over zorgvuldig handelen door NS, NPC en/of de leveranciers kan de privacy officer van NS het systeem in het uiterste geval uit laten schakelen totdat knelpunten zijn opgelost.

Het resultaat van het ontwikkelproces is een meetconcept dat aantoonbaar zorgvuldig omgaat met gegevens over de reizigers in stations.

Resultaten tot nu toe en vervolgstappen

In het voorjaar van 2013 heeft NPC de definitieve versie van SMART Station in opdracht van ProRail voor het eerst toegepast. Aanleiding is het voornemen om station en stationsgebied van Groningen te verbeteren, waarvoor ProRail als spoorbeheerder de initiatiefnemer is. De resultaten van de metingen en de bruikbaarheid in de herontwikkeling van het station zien er veelbelovend uit.[5] Zo is uit de metingen duidelijk zichtbaar geworden welke voorkeuren reizigers hebben voor looproutes. De inzet van SMART Station trok veel media-aandacht, waardoor het concept ook wat het privacybelang van passanten betreft, de vuurdoop heeft doorstaan. De media-aandacht geeft maar aan dat we steeds alert moeten blijven op privacy.
Op dit moment is de toepassingen van SMART Station op station Utrecht Centraal in voorbereiding. Dit met het oog op de verbouwing, die in het najaar een fase ingaat waarbij de transferruimte tijdelijk kleiner moet worden gemaakt om ruimte te maken voor de bouwwerkzaamheden. SMART Station helpt ons aan de inzichten die nodig zijn om dat zo klantvriendelijk mogelijk te doen. Naast de toepassingen in operatie en projecten levert SMART Station veel gegevens voor wetenschappelijk onderzoek. Een van de auteurs promoveert aan de Technische Universiteit Delft op het ontwerp en management van de transferfunctie van stations.
Ook vanuit de markt worden de ontwikkelingen gevolgd. Vanwege de kwaliteit van de oplossing, de relatief lage kosten en toepassing van *Privacy by Design*, is er veel interesse vanuit diverse sectoren uit binnen- en buitenland. Voor NS en NPC is het de uitdaging om SMART Station tijdens de toepassing op stations en daarbuiten te blijven verbeteren. De ontwikkelingen in techniek gaan immers razendsnel. Dit biedt kansen om reizigersmetingen steeds sneller, slimmer en goedkoper uit te voeren. Privacy helpt niet alleen om alert te blijven op risico's en knelpunten, maar blijkt ook een *driver* voor innovatie.

Conclusie

Geconcludeerd kan worden dat inzicht in het functioneren stations cruciaal is voor het verbeteren van de totale reisbeleving van reizigers die van deur tot deur reizen en op de stations overstappen. Het meten van looproutes, looptijden, wachtplaatsen en reizigersaantallen vormt hiervoor de basis. Geautomatiseerde reizigersmetingen bieden vanwege de relatief lage kosten en de mogelijkheid voor continu meten, een zeer aantrekkelijk alternatief voor eenmalige tellingen door mensen. Hoewel geautomatiseerde tellingen in andere (vervoer)sectoren al veel langer gemeengoed is, bestond er vanwege de zeer grote aantallen voetgangersbewegingen in een grote vrije ruimte geen geschikte oplossing voor stations.
Daarom hebben wij SMART Station ontwikkeld.

Omdat het zeer belangrijk is dat zorgvuldig met de privacy aspecten van alle gebruikers van een station wordt omgegaan, is bij de ontwikkeling van dit meetconcept de *Privacy by Design* aanpak gehanteerd. Onderdeel hiervan is niet alleen de technologie, maar ook de processen en de organisatie. De resultaten van de eerste metingen zijn positief. De eerste maatschappelijke reactie op het privacybelang was kritisch maar positief. Ook in de toekomst zullen NS en NPC alert blijven en privacy een leidende factor laten zijn in de doorontwikkeling van SMART Station.

5 Zie: http://www.prorail.nl/Pers/Persberichten/Actueel/Regionaal/Pages/ProRailmeetreizigersstromenviamobieltje.aspx

AANKONDIGINGEN

Koen Versmissen

35th International Conference of Data Protection and Privacy Commissioners.
The Polish Inspector General for Personal Data Protection. Ma. 23 t/m do. 26 september 2013, Warschau.
http://www.giodo.gov.pl/259/id_art/762/j/en

Praktijkcursus Wet Bescherming Persoonsgegevens.
Euroforum. Di. 3, 10 en (optioneel) 24 september 2013, Utrecht. € 1799; leden NVvIR en VPR € 1.499 (excl. btw).
Trainers: Gerrit-Jan Zwenne, Bart Schermer, Jeroen Terstegge, Jeroen Koëter.
http://www.euroforum.nl/juridisch/cursus-wet-bescherming-persoonsgegevens/

The 4th Annual European Data Protection and Privacy Conference.
Forum Europe. Di. 17 september 2013, Brussel. €150.
Sprekers o.a. Viviane Reding, Jan-Philipp Albrecht, Christopher Graham.
http://www.eu-ems.com/summary.asp?event_id=147

Masterclass Europese Privacy Verordening.
Studiecentrum voor Bedrijf en Overheid. Di. 24 september, Utrecht. € 699 (excl. btw).
Docenten: Gerrit-Jan Zwenne, Jeroen Terstegge, Quinten Kroes.
http://www.sbo.nl/overheid/cursus-wet-bescherming-persoonsgegevens-andere-privacywetgeving-/#masterclass

---

Training Privacy Impact Assessment voor beleidsambtenaren.
De Privacypraktijk & Martijn van der Veen Consultancy. Vr. 27 september 2013, Utrecht of Den Haag.
€ 695 (excl. btw). Docenten: Koen Versmissen & Martijn van der Veen.
http://www.deprivacypraktijk.nl/training-pia-voor-beleidsambtenaren

---

Postdoctorale Specialisatiecursus Privacy en Persoonsgegevens.
Tilburg Institute for Law, Technology, and Society / De Brauw Blackstone Westbroek / Nederland ICT.
Vr. 27 september, 4 oktober, 1 en 15 november 2013, Tilburg. € 2750.
Docenten: Corien Prins, Lokke Moerel, Peter van Schelven.
http://www.nederlandict.nl/Files/TER/Programma_%20cursus_Privacy_en_Persoonsgegevens_2013.pdf

---

Training Privacy en Wet Bescherming Persoonsgegevens.
NIBE-SVV / De Privacypraktijk. Wo. 2 oktober 2013, Amsterdam. € 706 (vrij van btw). Trainer: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20en%20Wet%20Bescherming%20Persoonsgegevens

---

Training Privacy van Werknemers.
NIBE-SVV / De Privacypraktijk. Wo. 9 oktober 2013, Amsterdam. € 706 (vrij van btw). Trainer: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20van%20werknemers

Training Privacy en Internet.
NIBE-SVV / De Privacypraktijk. Ma. 28 oktober 2013, Amsterdam. € 808 (vrij van btw).
Trainer: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20en%20internet

Training Privacy in de Praktijk.
NIBE-SVV / De Privacypraktijk. Ma. 4 november 2013, Amsterdam. € 503 (vrij van btw).
Trainer: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20in%20de%20praktijk

Training Wet Bescherming Persoonsgegevens.
PBLQ ROI. Do. 7 november 2013, Den Haag. € 790 (vrij van btw).
http://www.pblq.nl/roi/opleidingen/2013/beleids-en-bestuurskunde/bestuursrecht/wet-bescherming-persoonsgegevens

Cursus Privacy Compliance Actualia.
NIBE-SVV / De Privacypraktijk. Ma. 11 november 2013, Amsterdam. € 706 (vrij van btw).
Docent: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20Compliance%20Actualia

Privacy Compliance Masterclass.
NIBE-SVV / De Privacypraktijk. Ma. 11, 18 en 25 november 2013, Amsterdam. € 1925 (vrij van btw).
Docent: Koen Versmissen.
http://www.nibesvv.nl/Opleidingen/Privacy%20Compliance%20Masterclass

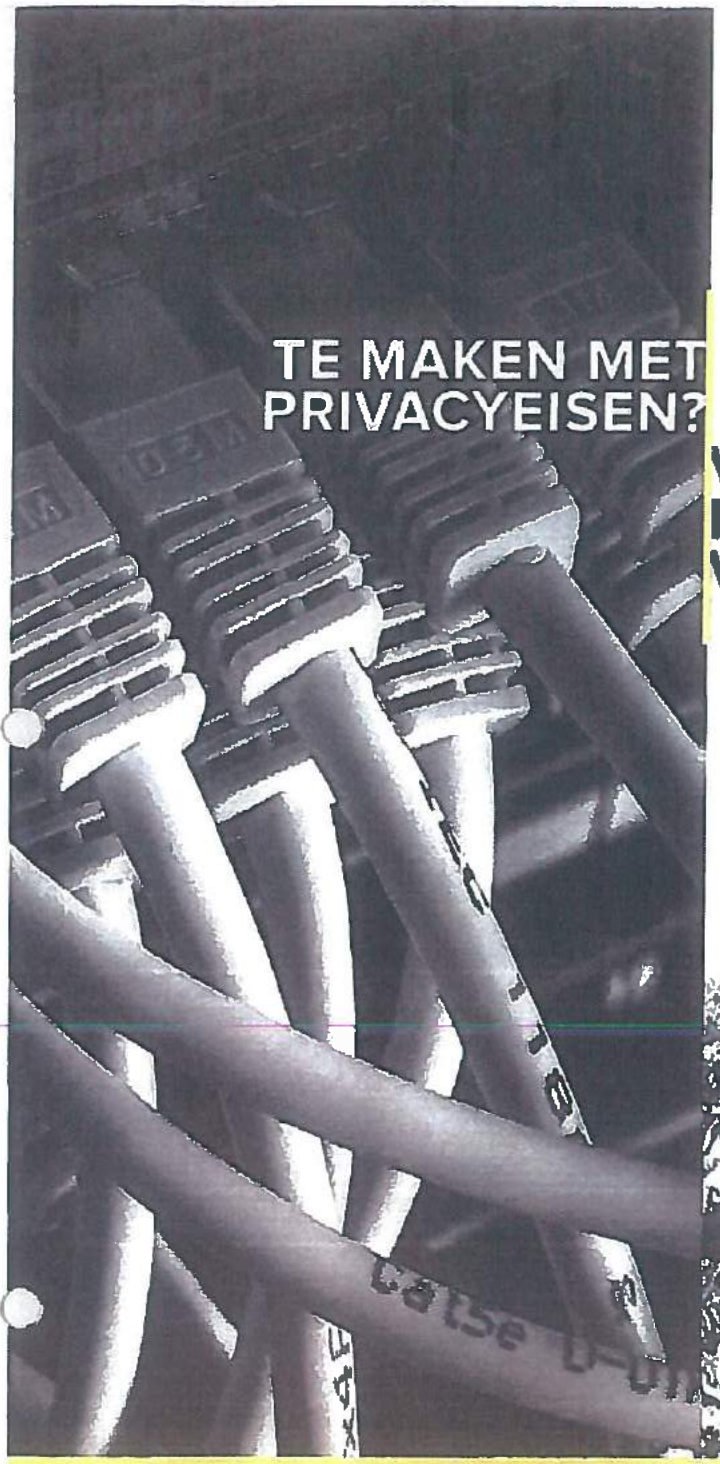
Basiscursus Wet Bescherming Persoonsgegevens.
Universiteit Leiden, Juridisch Post Academisch Onderwijs. Do. 21 en 28 november 2013, Leiden.
€ 1495 (vrij van btw). Docenten: Peter Blok, Jeroen Koëter, Gerrit-Jan Zwenne.
http://www.paoleiden.nl/cms2/index.php?option=com_content&view=article&id=565

Privacy Compliance Professional Sessiedagen.
NIBE-SVV / De Privacypraktijk. Najaar 2013. € 1995 (indicatief; vrij van btw).
Docenten: Koen Versmissen + gastdocenten. Programma wordt samengesteld in overleg met de deelnemers.
http://www.nibesvv.nl/Opleidingen/Privacy%20Compliance%20Professional%20%20sessiedagen

Het National Privacycongres.
Kluwer Opleidingen. Vr. 22 november 2013, Amsterdam.
Sprekers o.a. Lokke Moerel, Hester de Vries, Gerrit Jan Zwenne. € 795.
http://www.kluwershop.nl/opleidingen/details.asp?pr=16058

IAPP Europe Data Protection Congress 2013.
International Association of Privacy Professionals. Di. 10 t/m do. 12 december 2013, Brussel.
https://www.privacyassociation.org/events_and_programs/iapp_europe_data_protection_congress_2013

www.nibesvv.nl



TE MAKEN MET PRIVACYEISEN?

VOORBEREIDEN OP DE PRIVACYVERORDENING VAN DE EU?

NIBE-SVV biedt u dit najaar weer verschillende privacytrainingen: Privacy compliance masterclass, Privacy compliance professional sessiedagen, Privacy compliance actualia, Privacy in de praktijk, Privacy en internet, Privacy en Wet bescherming persoonsgegevens en Privacy van werknemers.

NIBE SVV
HET KENNISINSTITUUT VAN DE FINANCIËLE WERELD

De trainingen reiken u handvatten aan om te kunnen voldoen aan de huidige privacywetgeving en om u voor te bereiden op de nieuwe privacyverordening van de EU. NIBE-SVV biedt de trainingen aan in samenwerking met het gerenommeerde advies- en trainingsbureau De Privacypraktijk.

SUCCES DOEN WE SAMEN

Bijlage 3 bij raadsbesluit d.d. 17-05-2017 met kenmerk 1151/2017/12720-2

bluetooth en wifi tracking

Voor meer informatie:
www.stations.nl/privacy

Bijlage 4 bij de brief van 14-08-2017 met kenmerk NSL/2017/12426-2

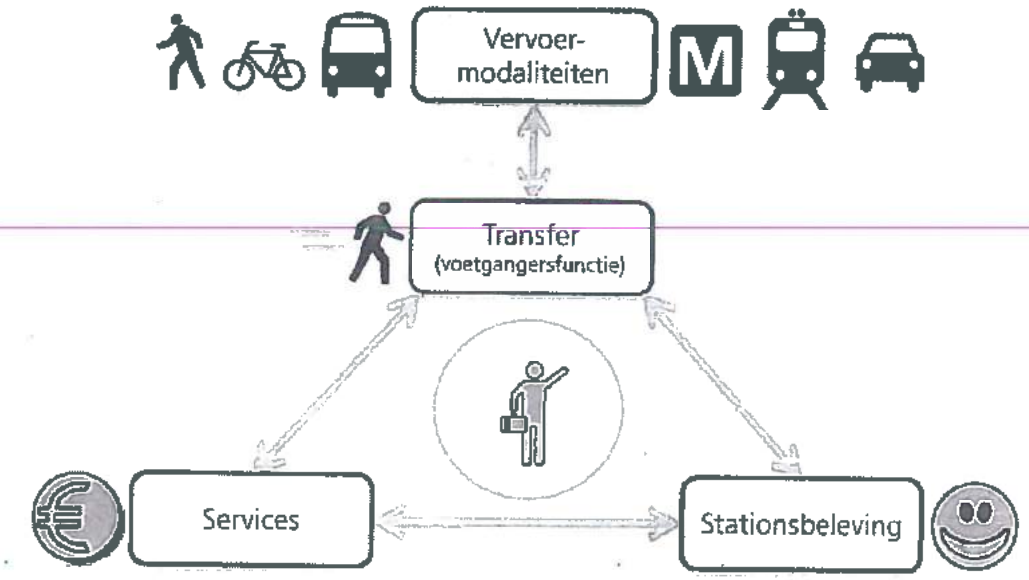
Informatiebeleidsplan en Privacy Impact Assessment SMART Station versie 2016

Inhoudsopgave

1 SMART Station

1.1 Wat is SMART Station?

Als knooppunt van voetgangersverkeer en vervoermodaliteiten is een station een bijzondere vastgoedvorm. In de vastgoedwereld geldt het gezegde dat het gaat om 'locatie, locatie, locatie' als wordt gevraagd naar de waardedrivers van vastgoed. Na zes jaar onderzoek binnen NS en ProRail met (onder andere) SMART Station data is duidelijk dat deze regel ook opgaat voor de binnenkant van een treinstation of OV-Terminal. Onze onderzoeken laten zien dat plek én dynamiek van de loopstromen - bijvoorbeeld piek-dalverhouding en de spreiding van de reizigers over tijd en ruimte - in een station bepalend zijn voor de prestatie het station en al haar componenten. Een te intensieve loopstroom resulteert - vanwege het ongemak voor de reiziger - niet alleen in een lagere stationsbeleving. Te grote drukte maakt tevens de verkeerskundige exploitatie kostbaar vanwege de aanvullende (operationele) maatregelen die nodig zijn om de verkeersafwikkeling veilig en beheersbaar te houden. En een te grote of te kleine loopstroom maakt de commerciële exploitatie van het station minder efficiënt, waardoor een groter beroep op publieke middelen moet worden gedaan om een station te (her)ontwikkelen en/of te exploiteren.



Afbeelding 1 Conceptueel model van een station

Tot 2011 bestond er voor NS Stations geen aantrekkelijke methode om loopstromen te meten. Het meten van loopstromen door handmatige tellingen was (en is) buitengewoon kostbaar: het kost al snel tienduizenden € om een beeld te krijgen van de loopstromen in een station op spits- of dagniveau. Deze hoge kosten worden veroorzaakt door het grote aantal tellers dat nodig is in combinatie met de hoge arbeidskosten (€25-€35 per uur). Tegelijk is het geleverde inzicht beperkt omdat de telresultaten slechts betrekking hebben op één of twee dagen. Hierdoor is er sprake van een grote onnauwkeurigheid in de generieke resultaten van veldonderzoek.

Vanwege gebrek aan data waren NS en ProRail bij het ontwerp en inrichting van de voetgangers-infrastructuur gewend om te rekenen met dagtotalen, bijvoorbeeld het aantal in/uitstappers per gemiddelde werkdag. De verdeling van de reizigersstromen over de ruimte werd gedaan met behulp van telcijfers van ad-hoc passantentellingen en/of postcodegegevens uit doorlopend reizigers-onderzoek (enquêtes). De verdeling van de reizigersstromen in de tijd werd gebaseerd op generieke

waarden voor spits/dal-verhoudingen en het drukste uur. Bij ontwerp, branchering en exploitatie van commercieel stationsvastgoed werd aan het bovenstaande een vuistregel voor de capture rate van een winkel(klasse) toegevoegd of er werd gekeken naar het aantal kassatransacties.

De ontwikkeling van SMART Station in de periode 2011-2016 heeft de potentie aangetoond van geautomatiseerde metingen van reizigersstromen door middel van technologie. In SMART Station worden meerdere, bestaande en nieuwe technologieën ingezet die tezamen gegevens leveren waarmee kan worden bepaald waar op ieder moment hoeveel reizigers lopen en/of verblijven. Binnen SMART Station genereren verschillende soorten tellers gedetailleerde data over de lokale intensiteiten en/of dichtheden van een loopstroom, bijvoorbeeld in een gang, op een trap of op een perrondeel. Op dit moment (eind 2016) wordt hiervoor gebruik gemaakt van drie soorten tellers: telgegevens uit OV- chipkaart poortjes, en sensoren van [redacted] en [redacted] In essentie registeren tellers de passage of aanwezigheid van passanten op één bepaalde plaats in het station (bijv. de hoofdentree van een station). De data uit deze sensoren kan op geen enkele wijze naar individuele personen worden herleid en valt daarmee buiten het bereik van het Informatiebeleidsplan.

Door middel van Bluetooth/WiFi-trackers worden routes, tijden en verblijfplekken van mobiele *devices* (bijv. mobiele telefoons) in kaart gebracht. Dit wordt ook wel aangeduid met *tracking*. Deze metingen dienen als *proxies* voor de werkelijke bewegingen van reizigers in ruimte en tijd. De sensoren meten de reizigers die Bluetooth en WiFi op hun mobiele apparatuur hebben ingeschakeld. In de praktijk komt 15 tot 25% van de totale reizigersstroom in de uiteindelijke dataset terecht. Dit percentage ligt lager dan het werkelijke aantal mobiele *devices* dat wordt gemeten, omdat er een strikte filtering plaatsvindt op daadwerkelijke aanwezigheid en logica van de metingen. Dit ter voorkoming van vervuiling van de datasets als gevolg van ruis. Op dit moment wordt gebruik gemaakt van één soort Bluetooth/WiFi-tracker, namelijk sensoren van BLIP Systems. De data uit deze sensoren kan – zonder aanvullende maatregelen – met koppelingen naar andere databronnen worden herleid naar (het gedrag van) individuele personen. Daarom valt het gebruik van deze sensoren binnen het bereik van onderhavige Informatiebeleidsplan.

Met de combinatie van tellen en *tracken* ontstaat een beeld van de intensiteiten, routes en looptijden van passantenstromen op ieder moment in en rond het station. De onderstaande figuur is een schematische weergave van het concept SMART Station.

Afbeelding 2 Schematische weergave van het concept SMART Station

Het doel van SMART Station is *het verkrijgen van inzicht op systeemniveau (1) in de loopstromen, looproutes, looptijden, verblijftijden en verblijfplaatsen van reizigers en bezoekers op stations en in stationsgebieden, en (2) werkelijke reistijden van reizigers in het netwerk van stations*. Met dit inzicht verbetert NS samen met haar partners de dienstverlening aan de reiziger, van ontwerp tot en met exploitatie van haar stations in het spoornetwerk van Nederland.

Met SMART Station wordt inzicht verkregen in de werkelijke "verkeersknelpunten" in een station (in de spoorsector aangeduid met "transferknelpunten"), waarop gericht maatregelen kunnen worden genomen. Een beter begrip van een probleem maakt het mogelijk om effectievere en meer (kosten)efficiënte oplossingen te bieden, waarbij tevens het harde bewijs kan worden geleverd aan stakeholders en financiers. Met SMART Station kan ook worden bepaald welke vervoerkundige categorieën reizigers (bijv. verbonden met een specifieke looproute van/naar een perron) relatief veel of weinig gebruik maken van de voorzieningen in een station. Deze informatie is zeer bruikbaar voor het ontwerp en/of de optimalisering van de branchering en de positionering van voorzieningen in een station. Beide componenten vormen dan ook het "verdienmodel" van SMART Station:

- **Infrastructuur/transport**: een veilige en uitnodigende transfer vanuit het perspectief van reiziger, tegen lagere kosten, met hard bewijs hiervoor richting alle stakeholders;
- **Vastgoed/commercie**: een optimale branchering van services, met meer tevreden reizigers, optimale huren en lagere exploitatiekosten als resultaat.

1.2 Waarom een informatiebeleidsplan?

NS is een groot, commercieel bedrijf met een belangrijke maatschappelijke taak, dat midden in de samenleving staat en waar veel aandacht uit politiek en media voor is. Gevolg hiervan is dat het werk bij en met NS in een glazen huis plaatsvindt. Wat betreft de privacy moeten alle stakeholders van NS er – zonder enige aarzeling - op kunnen vertrouwen dat NS zorgvuldig met de privacy van de reiziger/bezoeker omgaat.

In dit kader heeft NS een Privacybeleid. Hierin zijn zaken vastgelegd die voor heel NS gezamenlijk van belang en verplicht zijn. Deze kaders worden beheerd en bewaakt door NS Groep. Als aanvulling hierop is door NS Stations dit informatiebeleidsplan opgesteld waarin het privacybeleid specifiek voor SMART Station is uitgewerkt. In het geval van tegenstrijdigheid of onduidelijkheid is het Privacybeleid van NS Groep leidend.

Het is van belang dat een ieder die een station met SMART Station-technologie passeert, erop kan vertrouwen dat geen persoonlijke informatie wordt verkregen en opgeslagen. Dit document geeft weer hoe het proces van dataregistratie binnen de *trackers* van SMART Station verloopt, waar de privacygevoelige aspecten zitten, welke rollen de betrokkenen bij de verschillende processtappen hebben, en hoe zorgvuldig handelen wordt gecontroleerd. Doel van dit informatiebeleidsplan is dan ook het waarborgen van een zorgvuldige omgang met de gegevens die door middel van SMART Station worden ingewonnen opdat de persoonlijke levenssfeer van passanten (klanten en medewerkers) wordt gerespecteerd.

Het zijn de proceseigenaren - NS Stations, haar leveranciers van hardware, software en datadiensten, en partners die de gegevens gebruiken - die gezamenlijk dienen te zorgen voor zorgvuldige omgang met gegevens die door SMART Station zijn ingewonnen. Dit informatiebeleid vraagt van hen een proactieve handelswijze, op basis van inzicht in processen en sturing op de ijkpunten voor *good privacy governance*.

SMART Station, en met name de technologie hierbinnen, is volop in ontwikkeling. Op logische momenten in het ontwikkelproces zal dit Informatiebeleidsplan op basis van de laatste inzichten

worden geactualiseerd, waarmee eerdere versies komen te vervallen. Bij een actualisering worden de proceseigenaren door NS Stations over het nieuwe Informatiebeleidsplan geïnformeerd.

1.3 Wat zijn de wijzigingen ten opzichte van versie 1.0 (versie 2012)

De vorige, eerste versie van het informatiebeleidsplan dateerde uit 2012. Ten opzichte van deze versie zijn twee materiele wijzigingen in het informatiebeleid doorgevoerd:

1) Het (onbewerkte) MAC-adres wordt beschouwd als een persoonsgegeven. Sinds 2012 heeft het denken en handelen met betrekking tot Bluetooth/WiFi-tracking een stevige ontwikkeling doorgemaakt, zowel buiten als binnen NS. Vanuit juridisch perspectief heeft het (onbewerkte) MAC-adres van een mobiel apparaat de status van een persoonsgegeven gekregen;
2) Het MAC-adres als persoonsgegeven vormt de basis van de tweede, materiele wijziging: op locatie wordt aan passanten kenbaar gemaakt dat *trackers* operationeel zijn. De veelvuldig opgetreden berichtgeving in de media over Bluetooth/WiFi-tracking – bijvoorbeeld in winkels en winkelstraten – heeft bijgedragen aan het bekend raken van het fenomeen onder een breed publiek. Daarom wordt verwacht dat het op locatie kenbaar maken door veel passanten wordt begrepen.

Verder zijn ten opzichte van de eerste versie diverse, kleinere wijzigingen doorgevoerd, waarbij de intentie van het oorspronkelijke informatiebeleidsplan niet is gewijzigd.

Het eerste deel van de wijzigingen heeft betrekking op woordgebruik en toonzetting van de tekst. Zo zijn de sensoren inmiddels uitgerust met Bluetooth en WiFi-technologie (was: alleen Bluetooth). De voorzieningen op een station zijn we gaan aanduiden met services (was: "winkels"), waarbij de reikwijdte is uitgebreid van alleen commerciële voorzieningen naar alle voorzieningen in een station. De wijze waarop het onbewerkte MAC-adres (was: privacygevoelig; is: persoonsgegeven) in twee stappen tot onpersoonlijk "passantennummer" (was en is: geen persoonsgegeven) wordt omgezet is beter beschreven. En tenslotte is iedere verwijzing naar een specifieke leverancier uit het document verwijderd. Dit om – conform de huidige praktijk - uit te stralen dat alle leveranciers en partners op het station bij activiteiten op het gebied van *tracking* aan dit informatiebeleid moeten voldoen.

Het tweede deel van de wijzigingen heeft betrekking op de ervaringen van de afgelopen jaren. Ten eerste zijn de definities van de data in relatie tot de bewaartermijnen aangescherpt. Dit maakt eenduidig welke data heel kort mag worden bewaard (inclusief de condities), en welke data lang mag worden bewaard. Ten tweede is de termijn van een audit door een externe, gespecialiseerde consultant praktischer gemaakt (was: 2 jaar; is: 4 jaar). Met deze laatste aanpassing is beoogd een nieuwe balans te vinden tussen noodzaak/baten en inspanning/kosten, rekening houdend met de lager dan verwachte snelheid waarin de technologische mogelijkheden op het gebied van *tracking* zich ontwikkelen.

2 SMART Station & privacy

2.1 Privacygevoeligheid SMART Station

Zoals in de inleiding beschreven wordt bij SMART Station gebruik gemaakt van twee soorten sensoren: tellers en *Bluetooth/WiFi-trackers*. Met behulp van de tellers wordt inzicht verkregen in zaken als aantal unieke bezoekers, aantal bewegingen (frequentie), verblijfsduur (retentie), dichtheden van mensenmassa's, snelheden en looprichtingen binnen het scangebied van een sensor. Bij de metingen met *Bluetooth/WiFi-trackers trackers* draait het om het scannen van MAC-adressen[1] van mobiele telefoons (en andere apparatuur, bijvoorbeeld iPads of laptops) waarvan Bluetooth en/of WIFI is ingeschakeld. Door een MAC-adres te combineren met de plaats en tijd dat een individu zich op een station bevindt, kan een beeld worden verkregen van het loop-, verblijf- en wachtgedrag van deze reiziger binnen het (invloedgebied van) een station, van ketenvoorziening (bijv. fietsenstalling) tot trein, vice versa. Wanneer meerdere stations met *trackers* zijn uitgerust, is het daarnaast mogelijk een beeld te krijgen van de reis van reizigers in het netwerk van deze stations. Het MAC-adres kan dan ook worden geschouwd als een 'kentekenplaat' van een voetganger die in of rond het station loopt en/of zich in het treinnetwerk verplaatst.

Bij de privacygevoeligheid van SMART Station gaat het om het twee perspectieven:

- Juridisch perspectief, waarbij centraal staat of door SMART Station ingewonnen gegevens zijn en zo ja, of de verwerking van deze gegevens noodzakelijk (subsidiariteit) en evenredig (proportionaliteit) is ten opzichte van de doelstellingen die ermee worden nagestreefd;
- Maatschappelijk perspectief, waarbij het gaat om de beleving van reizigers en andere belangrijke stakeholders of NS zorgvuldig met de ingewonnen informatie omgaat.

2.2 Juridisch perspectief

Wat betreft privacy is de Wet Bescherming Persoonsgegevens (WBP) voor SMART Station de meest relevante wet. De WBP biedt regels voor het beschermen van persoonsgegevens en bevat criteria voor rechtmatige gegevensverwerking, die als 'vangrails' de privacybelangen van klanten en werknemers beschermen. Meestal bestaat die vangrails uit het benoemen van uitgangspunten waaraan procesvoering dient te voldoen, waarbij de wetgever flexibiliteit gunt voor eigen oplossingen. De WBP verplicht NS onder meer om passende informatiebeveiliging toe te passen.

Algemeen geformuleerd verlangt de WBP van NS dat:

- informatieverwerking over klanten en medewerkers beperkt blijft tot wat noodzakelijk is voor het realiseren van de doelstellingen van de onderneming. Ieder proces dat niet op een logische manier bijdraagt aan één van de bedrijfsdoelen, is een niet-noodzakelijk proces en daarmee in strijd met de privacywetgeving – wat betekent dat het proces gestaakt dient te worden. De bedrijfsdoelen waaraan SMART Station bijdraagt, zijn:
  - Gebalanceerde oplossingen voor klantgerichtheid en service. SMART Station biedt door middel van statistisch onderzoek inzicht in feitelijke loopbewegingen en verblijfsplekken van reizigers op en rond het station. SMART Station draagt hierdoor bij aan inzicht in gedrag van reizigers op stations. Op basis hiervan kan NS Stations samen met haar partners het functioneren van haar stations aanpassen, zowel in de ontwerp- als exploitatiefase;
  - Bedrijfsefficiëntie. Met een volwassen concept zijn de kosten van SMART Station-technologie lager zijn dan traditionele meetmethoden, in het bijzonder handtellingen.

[1] Een MAC-adres (Message Authentication Code) is een uniek hardwarenummer van iedere communicatiecomponent op een mobiele telefoon. Een mobiele telefoon met GSM/GPRS/UMTS, WIFI en Bluetooth heeft meerdere MAC-adressen

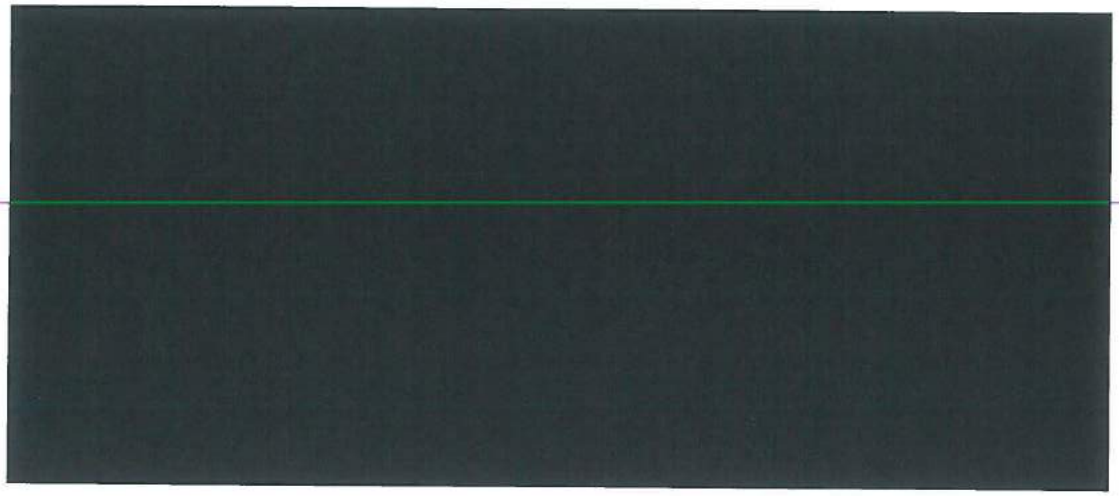
Daarnaast is de toegevoegde waarde van de verkregen informatie groter doordat de output omvangrijker is door toevoeging van componenten als tijd, route en netwerk, en door de mogelijkheid om over een langere periode te meten;

- Veiligheid. SMART Station geeft inzichten in (eventuele) bottlenecks op een station door inzichten te verschaffen in druktepatronen, wachttijden, snelheden, loopbewegingen. Hiermee is NS Stations met haar partners beter in staat tijdig oplossingen te bieden voor tijdelijke (als gevolg van verbouwingen) of structurele transferknelpunten (crowd control). Dit aspect vormt een van de kerntaken van het bedrijf;

- administratieve processen behoorlijk en zorgvuldig zijn vormgegeven om de individuele belangen van klanten en werknemers te beschermen. Om aan de eisen van de wet te voldoen, is regievoering en transparantie randvoorwaardelijk.

Om te beoordelen of de WBP van toepassing is op de gegevensverwerking van SMART Station, moet worden vastgesteld of de gegevens die met SMART Station worden ingewonnen en verwerkt, persoonsgegevens zijn:

- Tellers. Bij de metingen zijn individuen niet identificeerbaar. Dit in tegenstelling tot bijvoorbeeld camerabeelden waarbij personen herkenbaar in beeld zijn. De onderstaande figuur geeft ter illustratie het beeld van een teller op het perron van station Schiphol Airport (links) met het bijbehorende beeld uit een camera op dezelfde plek. Op dit moment zijn drie type telsensoren in gebruik die op een vergelijkbare wijze werken.



- Bluetooth/WIFI. Ten aanzien van *Bluetooth/WiFi-trackers* is het de vraag of het MAC-adressen van een mobiele telefoon of ander mobiel apparaat persoonsgegevens zijn. Verwijzend naar de rapportage van de Autoriteit Persoonsgegevens van 13 oktober 2015[2] kan deze vraag zonder twijfel positief worden beantwoord als het gaat om MAC-adressen waarop geen anonimiserende bewerkingen zijn doorgevoerd.

Het voorgaande betekent dat voor het gebruik van *Bluetooth/WiFi-trackers* een Informatiebeleid moet zijn opgesteld, geïmplementeerd en gecontroleerd waarmee wordt voldaan aan de WPB.

[2] Bronnen:
- College Bescherming Persoonsgegevens. *Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace*. Kenmerk z2014-00944. Rapport definitieve bevindingen. Openbare Versie. 13 oktober 2015.
- Autoriteit Persoonsgegevens. Last onder dwangsom. Kenmerk z2015-00981. 30 juni 2016.

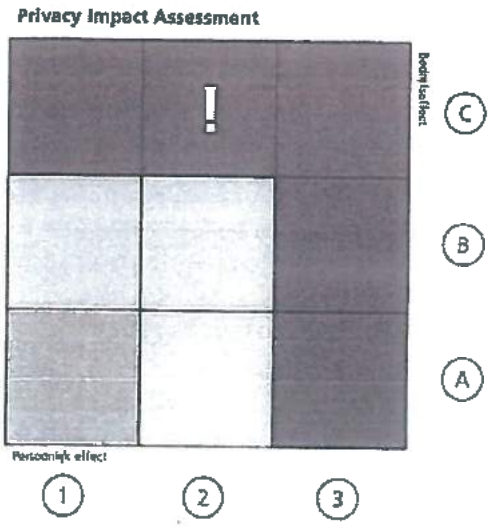
2.3 Maatschappelijk perspectief

In het maatschappelijke debat over aan technologie-gerelateerde privacy-issues is een opvallende tegenstelling zichtbaar. Aan de ene kant staan politiek en de Autoriteit Persoonsgegevens (AP), die zich steeds meer zorgen maken over de privacy van burgers. Vanuit deze zorg treedt de overheid daadkrachtig op om op te komen voor de belangen van haar burgers. Denk bijvoorbeeld aan de discussies over netneutraliteit naar aanleiding van de Deep Packet Inspection van KPN en Vodafone (2011) en het voornemen voor het gebruik van banktransactiegegevens voor marketingdoeleinden door ING (2014). Denk hierbij ook aan de last onder dwangsom van de AP tegen Google (2012/3) en de last onder dwangsom van de AP tegen Bluetrace (2015/6). Aan de andere kant staan de burgers zelf die zich, kijkend naar hun (online) gedrag, gemiddeld genomen weinig zorgen lijken te maken over hun privacy. Denk bijvoorbeeld aan het massale gebruik van de Bonuskaart van Albert Heijn, de location-based-services van Google of Apple, sociale media (bijv. Facebook) of het gemakkelijk opgeven van e-mailadressen. Tegelijk is er een toename van het belang van privacy merkbaar onder groepen en individuen binnen de bevolking.

NS vervult een belangrijke rol in het hart van de maatschappij en staat hierbij per definitie in de maatschappelijke schijnwerpers. Hierdoor is zij kwetsbaar voor negatieve beeldvorming, zeker bij (schijnbaar) onzorgvuldig handelen. Deze kwetsbaarheid vormt een extra groot risico voor NS omdat het AP al jaren zeer actief is in het agenderen van het privacyvraagstuk in het digitale tijdperk, hierbij vooral grote bedrijven op de korrel heeft, en veelvuldig gebruik maakt van de landelijke media om de maatschappelijke discussie te beïnvloeden.

2.4 Privacy Impact Assessment zonder informatiebeleid

Op basis van de huidige informatie en inzichten valt een deel van SMART Station binnen het bereik van de Wet Bescherming Persoonsgegevens (WBP). Tevens is NS, vanwege de maatschappelijke lopende discussies over privacy in combinatie met de positie van NS in de maatschappij, kwetsbaar voor negatieve beeldvorming. De privacyscore drukt de mate van aandacht uit die het proces verdient, omdat er reële persoonlijke belangen en/of bedrijfsbelangen mee gemoeid zijn. De Privacy Officer van NS Groep heeft aan de hand van de Quick Scan Privacy NS de privacy-impact score van het SMART Station-proces vastgesteld op 'C2' (zie hiernaast). Deze score vereist een gericht plan om de risico's voor zowel de personen als het bedrijf te mitigeren. Dit plan wordt in de volgende hoofdstukken uitgewerkt.



Afbeelding 3: Privacy-impact score SMART Station zonder informatiebeleid

3 Informatiebeleid

3.1 Onderdelen informatiebeleid

Het informatiebeleid van SMART Station is gebouwd op vier pijlers:

1. *Technologie*. In de techniek zijn maatregelen genomen waardoor de opgeslagen en verwerkte gegevens onomkeerbaar zijn gecodeerd. Hierdoor is geen van de partijen in staat om de verwerkte gegevens (op welke aggregatieniveau dan ook) te herleiden tot de oorspronkelijke scangegevens;
2. *Processen*. De wijze van verzenden van data van scanunits naar servers en tussen servers onderling, de opslag van data en de verwerking van de data tot informatie wordt vastgelegd in overeenkomsten in de gehele leveranciersketen. Hierin worden afspraken gemaakt over de wijze waarop de informatie wordt verwerkt;
3. *Governance*. De governance is erop gericht om regelmatig te toetsen of de processen conform de overeenkomsten plaatsvinden. Daarnaast is er een speciale governance structuur voor systeemaanpassingen en pilots;
4. *Communicatie*. Transparante communicatie naar stakeholders staat voorop. NS Stations communiceert op het station over het gebruik van *Bluetooth/WiFi-trackers* en biedt uitgebreide achtergrond informatie op een openbare website aan. Daarnaast kunnen alle geïnteresseerden – individuen, media, bedrijven of de Autoriteit Persoonsgegevens – een toelichting ontvangen waarbij voorbeelden worden getoond van hoe de gegevens worden verwerkt.

De hiervoor genoemde pijlers hebben een onderlinge hiërarchie, welke bijdraagt aan het minimaliseren van de risico's als gevolg van ongewenste verspreiding van gegevens en/of het ontstaan van een ongewenst maatschappelijk/politiek beeld. De technologie vormt de basis. Als bijvoorbeeld processen niet conform de afspraken verlopen en de governance ontoereikend is, is het nog steeds niet mogelijk om aan de hand van de gegevens uit de systemen van SMART Station de oorspronkelijke scangegevens te achterhalen.

3.2 Technologie

In iedere scanunit is – in de firmware - een niet-schakelbare, onomkeerbare 64-bits versleuteling (*unit side encryptie*) ingebouwd die zorgt voor encryptie van de MAC-adressen van gescande Bluetooth of WIFI-apparaten. De encryptie vindt plaats door het MAC-adres te hashen voordat deze wordt opgeslagen op de het geheugen van de scanunit en via een netwerkverbinding naar de server worden verzonden. Hashen ("husselen") houdt in dat door een speciaal hiervoor ontwikkeld algoritme de ingevoerde reeks aan cijfers (het MAC-adres) wordt omgezet in een deelverzameling van dit getal. Dit proces wordt ook wel aangeduid met pseudonimiseren, en moet vooral voorkomen dat "kale" MAC-adressen "op straat komen te liggen" in het geval van diefstal of hack van een sensor.

Op de server wordt de data van alle sensoren vervolgens nog een keer onomkeerbaar "gehusseld" met een indicator voor een ingestelde tijdperiode (standaard is deze nu ingesteld op "dag"). Hierdoor ontstaat een nieuw "passantennummer" , dat gedurende deze periode uniek is. Tevens is het door het toepassen van een encryptie onmogelijk om - in combinatie met een steekproefbepaling [3] - de

[3] Slechts een gedeelte van alle reizigers heeft bluetooth of WIFI ingeschakeld. Hierdoor wordt slecht een percentage van het totaal geregistreerd en is het onmogelijk zaken te koppelen aan andere informatiebronnen.

ingewonnen gegevens te combineren met de gegevens als SSID[4], payload-data[5] en IP-adressen[6], die ingewonnen zouden kunnen worden bij het gebruik van het mobiele apparaat door de reiziger. Hierbij wordt opgemerkt dat het niet mogelijk om SSID, payload-data en IP-adressen door middel van Bluetooth/WiFi-trackers op te pikken.

Omdat dit proces bij iedere scanunit op dezelfde wijze plaatsvindt, is het mogelijk om binnen de ingestelde tijdsperiode te achterhalen bij welke scanners het Bluetooth/WIFI-apparaat is opgepikt. Het versleutelde MAC-adres van een apparaat van een passant is binnen de periode immers gelijk. Deze mogelijkheid vervalt zodra de volgende periode ingaat. Hetzelfde Bluetooth/WIFI-apparaat krijgt dan een ander versleuteld MAC-adres. Vergelijking tussen periode op het niveau van Bluetooth/WIFI-apparaten is hierdoor niet mogelijk.

De basisperiode is vastgesteld op één (NS-)dag.[7] Hierdoor is eenzelfde MAC-adres (met haar houder) op een volgende dag niet meer te matchen met data uit een voorgaande periode. Looproutes binnen een station kunnen dus op dagniveau inzichtelijk worden gemaakt, maar er kan geen uitspraak worden gedaan over het terugkeerpatroon van individuele reizigers. Een code op de ene dag is bijvoorbeeld 12345678, en een volgende dag 987654321. Dit beperkt de mogelijkheid voor het leggen van verbanden tot enkel-dag-correlaties. Persoonsgegevens zijn niet meer te herleiden omdat niet de juiste MAC-adressen beschikbaar zijn.

Wanneer dit voor een specifieke projectdoelstelling wenselijk is – bijvoorbeeld om een gedetailleerder beeld te krijgen van reis-, verblijf- of wachtpatronen – kan de encryptieperiode worden gewijzigd in één week of één maand. Dit kan alleen wanneer door NS Stations een schriftelijk verzoek wordt gedaan, met aanduiding van de doelstelling. Het aanpassen van de encryptie-periode staat beschreven onder het hoofdstuk governance.

Tijdens het installeren en uitlijnen van scanunits op een station is het wenselijk om de antenneconfiguratie[8] te testen. Hiervoor is bij de leveranciers een applicatie beschikbaar waarmee van één of enkele mobiele apparaten waarvan het MAC-adres bekend is, het versleutelde MAC-adres voor de testdag kan worden bepaald. Dit is alleen mogelijk wanneer het originele MAC-adres bekend is, en is dus niet van toepassing voor apparatuur van gebruikers van het station. Bovendien is het versleutelde MAC-adres geldig voor de testdag. Immers de encryptie genereert op basis van hetzelfde MAC-adres de volgende dag al een ander identificatienummer.

[4] Willekeurig in te stellen (niet unieke)identificatie van een WIFI-netwerk.

[5] Data in het verkeer over een internetverbinding (bijvoorbeeld e-mail, websites en bestanden).

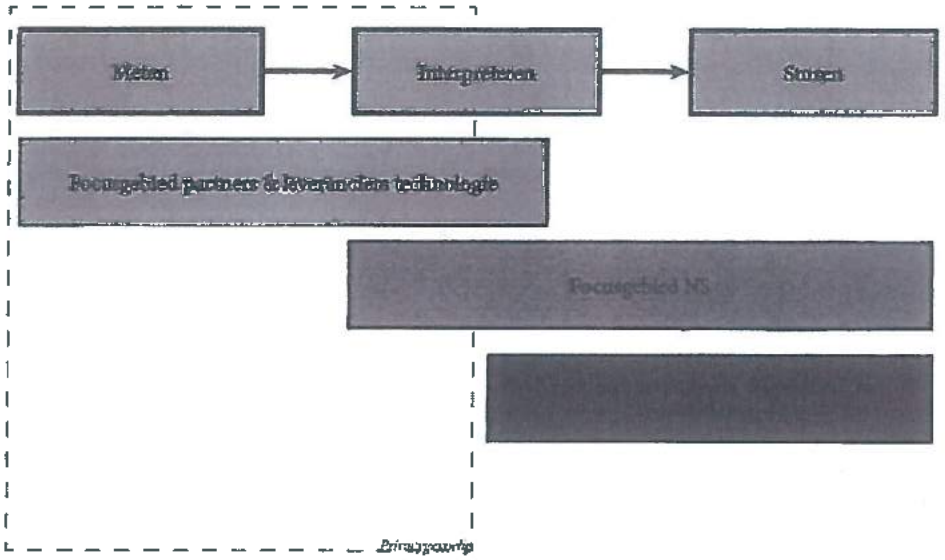
[6] Nummer van een computer die is aangesloten op het internet, waarmee deze zichtbaar is voor andere computers op het internet. De persoon achter een IP-adres is in de meeste gevallen te achterhalen.

[7] NS-dag: 4.00am tot en met 3.59am op de volgende dag

[8] Voor de SMART Station-resultaten is het van belang te weten wat je meet en dus om het meetgebied van een scanunit te bepalen.

3.3 Processen

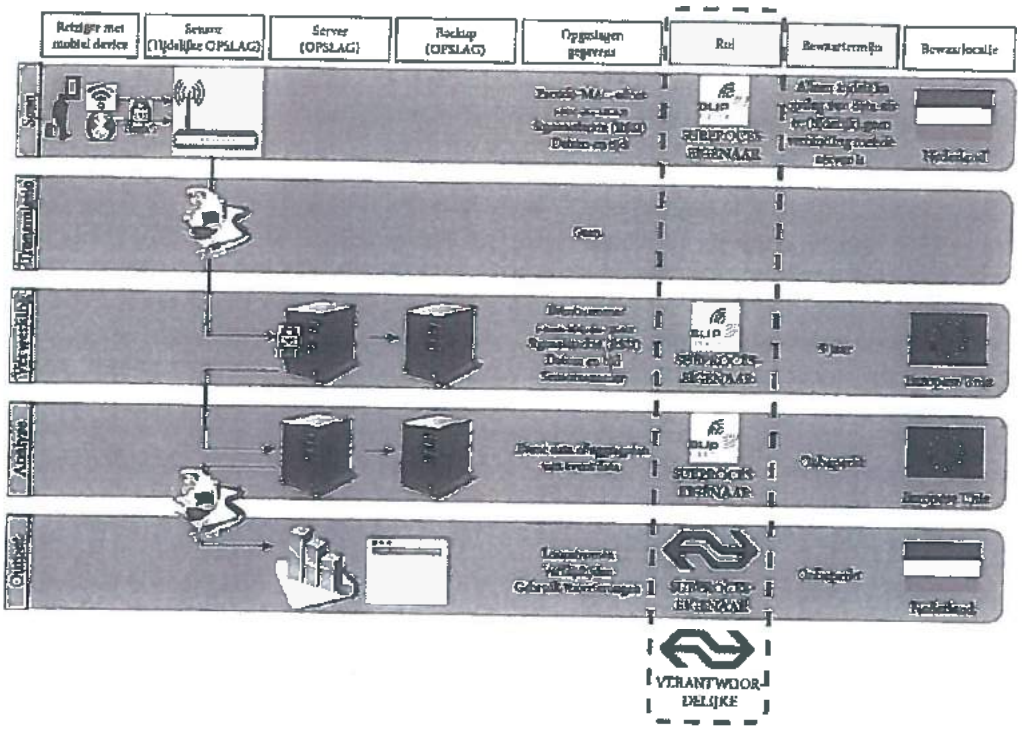
De leveranciers- en gebruikersketen ziet er grofweg als volgt uit:



Afbeelding 4: Verhoudingen betrokken partijen SMART Station

De hard- en software van *Bluetooth/WiFi-trackers* wordt geleverd door een technology partner/leverancier. Op zijn server vindt de eerste dataverwerking van de meetgegevens uit de sensoren plaats. Geautoriseerde gebruikers binnen NS – of gebruikers namens hen (partners en leveranciers van adviesdiensten) – kunnen op deze server inloggen om uitsnedes uit de bewerkte data te zien (visualisaties, bijvoorbeeld door middel van kaarten en grafieken) of om bewerkte data te downloaden. Mede op basis van de resultaten van de analyses voert NS Stations wijzigingen door in de indeling of exploitatiewijze van het station. De privacygevoeligheid is gelegen in het deel van meten tot interpreteren van data uit *Bluetooth/WiFi-trackers*. Dit zijn grofweg de processen die plaatsvinden bij de technology partner/leverancier die in opdracht van en in afstemming met NS werkt. Hierop wordt in dit procesdeel van het informatiebeleid nader ingegaan.

De inwinning, transmissie, verwerking en opslag van Bluetooth/WIFI scangegevens is onder te verdelen in vier stappen. Onderstaande figuur visualiseert dit proces, van de gegevensverwerking van de sensoren op de stations tot aan de presentatie bij geautoriseerde gebruikers.



Afbeelding 5: Proces SMART Station

Stap 1: Scanning & encryptie op scanunit

Met sensoren/scanners van de technologie partner/leverancier (nu: BLIP Systems uit Denemarken) die op strategische plekken op stations zijn geïnstalleerd, worden MAC-codes van mobiele apparatuur van passanten via Bluetooth en/of WIFI geregistreerd. Een reiziger of bezoeker die op zijn telefoon of tablet Bluetooth en/of WIFI aan heeft staan, wordt door een sensor die hij passeert, geïdentificeerd als 'event'. De MAC-adressen worden bij binnenkomst op de sensor ('unit-side') direct omgezet naar hashcodes (versleuteld met hash 1) en vervolgens als gepseudonimiseerde nummers gebufferd opgeslagen op de sensor. Daarnaast worden signaalsterkte en de tijd opgeslagen.

Stap 2: Transmissie
Vanaf de sensor worden deze drie gegevens via een datanetwerk – 3/4G, WLAN of LAN, afhankelijk van de beste oplossing – met behulp van het IP protocol- naar een centrale server van de technologie partner/leverancier doorgestuurd. Onderweg worden geen gegevens opgeslagen. Na bevestiging van ontvangst van de gegevens door de server worden de gegevens van de sensor verwijderd.

Als een sensor tijdelijk geen verbinding met de server heeft, slaat de sensor de gegevens tijdelijk op in een buffer. De MAC-adressen zijn met de eerste hash versteuteld, waardoor ze zijn gepseudonimiseerd.

Stap 3: Verwerken input scanunits
Bij de derde processtap worden de gegevens van alle scanunits op de centrale server van de technologie partner/leverancier (nu: BLIP Systems uit Denemarken) in een database opgeslagen. Bij binnenkomst worden de gepseudonimiseerde MAC-adressen met een tweede hash versteuteld. De hashcode bevat de datum van meten, waardoor eenzelfde (gepseudonomiseerd) MAC-adres op twee verschillende dagen resulteert in twee verschillende geanonimiseerde eventnummers ("passantnummers"). Naast deze eventnummers worden sensornummer, tijd en signaalsterkte opgeslagen. Van deze database wordt dagelijks een backup gemaakt.

De bewaartermijn van deze gegevens is gemaximeerd op 5 jaar. Hierdoor kunnen nieuwe bewerkingen op de ruwe data worden uitgevoerd bij ontwikkeling van nieuwe filters en algoritmes, bijvoorbeeld voor het analyseren van langjarige trends door middel van statistisch onderzoek. Een kortere periode maakt het onmogelijk om (bijvoorbeeld) effecten van veranderingen in infrastructuur van het station met behulp van de nieuwste algoritmes en filters te scheiden van omgevingsruis (bijv. seizoenspatronen). De ervaring heeft geleerd dat een periode langer dan 5 jaar niet nodig is.

Stap 4: Analyseren zodat loopstromen en verblijftijden zichtbaar worden
In de vierde stap worden de events op basis van logische (gedrags)patronen van passanten geaggregeerd. Dit genereert de gewenste datasets met loopstromen, looproutes, wachttijden en verblijfplaatsen op stations en in stationsgebieden. Voor deze (geaggregeerde) informatie geen maximale bewaartermijn. Deze informatie is immers ontdaan van alle tot een persoon herleidbare kenmerken.

Stap 5: Presentatie loopstromen en verblijftijden
Het resultaat van stap 4 wordt door middel van een rapportage – grafisch en/of in de vorm van tabellen – via een webapplicatie beschikbaar gesteld aan geautoriseerde medewerkers van NS Stations.

3.4 Governance

Verantwoordelijk
NS Stations is er verantwoordelijk voor dat alle processen op een correcte wijze plaatsvinden binnen het generieke privacybeleid van NS Groep en het specifieke informatiebeleidsplan voor SMART Station.[9] De NS Directie is als Data Controller verantwoordelijk in de zin van de Wet Bescherming Persoonsgegevens.

In de keten van leveranciers is NS Stations de hoofdproceseigenaar, waarbij de directie van NS Stations eindverantwoordelijk is voor de invulling van deze rol. Zij heeft deze zaak gedelegeerd aan Onderzoek, onderdeel van de divisie Vastgoed & Ontwikkeling van NS Stations. Insteek is een procesbewaking op een proactieve manier. Onderdeel hiervan is het actueel houden van het

[9] Bij strijdigheden tussen het privacybeleid van NS Groep en het informatiebeleidsplan SMART Station prevaleert het privacybeleid van NS Groep

informatiebeleid van SMART Station op de ontwikkeling van het meetconcept, en toezicht houden op de naleving van het beleid door partners en leveranciers.

Partners en leveranciers
Een deel van de verantwoordelijkheden wordt gedelegeerd naar partners en leveranciers (bijv. BLIP Systems), de subproceseigenaren. Om ervoor te zorgen dat zij ook in lijn met het informatiebeleid handelen, worden in overeenkomsten - bijvoorbeeld samenwerkingsovereenkomst, leveranciers-/raamovereenkomst of en Service Level Agreement - met deze partijen meetbare afspraken vastgelegd, inclusief de wijze waarop het naleven van deze afspraken wordt geëvalueerd, en hoe te handelen als deze afspraken niet worden nagekomen. Bij het delegeren naar een subproceseigenaar verliest de (hoofd)proceseigenaar zijn eigen verantwoordelijkheid niet, maar blijft verantwoordelijk voor regie en toezicht.

In de context van het informatiebeleid staan twee principes aan de basis van alle afspraken met alle leveranciers en partners:

1. **Continuïteit** van de samenwerking en dienstverlening.
    a. Vertrouwen. Er wordt alleen met partners en leveranciers samengewerkt waarin bij NS Stations het vertrouwen bestaat dat ze zorgvuldig met de belangen van NS omgaan, ook als zaken onverhoopt niet expliciet en schriftelijk zijn overeengekomen. De samenwerking wordt aangegaan voor een langere periode (meerdere jaren), zodat deze partijen ook in staat worden gesteld om hun werkwijze en processen zo in te richten dat maximaal wordt voldaan aan het informatiebeleid van SMART Station. Een voorbeeld hiervan is een investering in technologie die bijdraagt aan een zorgvuldige gegevensverwerking;
    b. Dienstverlening. De SMART Station oplossing moet altijd beschikbaar zijn, waarbij de gemaakte afspraken te allen tijde worden nageleefd, onafhankelijk van de personen die er op dat moment bij zijn betrokken. Dit betekent dat afspraken eenduidig en schriftelijk worden vastgelegd, en dat er bij overdracht van taken naar andere medewerkers door alle betrokkenen expliciet aandacht wordt besteed aan het informatiebeleid van SMART Station en de context hiervan.
2. **Control op de data vanwege bedrijfsgevoeligheid**. Het eigendom over de data ligt vanwege de bedrijfsgevoeligheid - privacy impact en commerciële waarde - te allen tijde bij NS Stations. Dit betekent dat NS Stations onder alle omstandigheden bepaalt wat er met de data gebeurt en wie er toegang toe heeft. Partners en leveranciers mogen van de data gebruik maken als dit vooraf is geregeld en schriftelijk is vastgelegd, inclusief de reden van gebruik.

Toezicht
Het toezicht op naleving van het informatiebeleid ligt bij de privacy officer van NS Groep NV:

- **Evaluatie**. Jaarlijks voert NS Stations een review uit van het informatiebeleid en de toepassing hiervan. Bijzondere aandacht gaat uit naar risico's voor NS. De resultaten worden besproken met de privacy office waarna verbeterpunten worden geformuleerd, welke door NS Stations worden geïmplementeerd;
- **Privacy Audit**. Vanwege de maatschappelijke en technologische ontwikkelingen op het gebied van privacy wordt vierjaarlijks een Privacy Audit uitgevoerd door een externe consultant (in 2012 was dit [redacted] Deze vindt plaats voorafgaand aan de jaarlijkse review zodat eventuele aandachtspunten direct als verbeterpunten kunnen worden geïmplementeerd. De privacy officer kan te allen tijde gemotiveerd een tussentijdse evaluatie verlangen als hij/zij daar aanleiding toe ziet;
- **Encryptieperiode**. De basisinstelling voor de encryptieperiode op de scanunits is één dag. De encryptieperiode kan enkel op verzoek van NS Stations worden verlengd tot één week of één maand. Voor een aanpassing wordt toestemming gevraagd aan de privacy officer. Het verzoek

tot aanpassing aan de partners en leveranciers wordt altijd schriftelijk gedaan, waarbij expliciet een doelstelling wordt geformuleerd;
- **Productontwikkeling**. Wanneer NS Stations in het kader van productontwikkeling wil afwijken van een of meerdere onderdelen van het informatiebeleid, dient de privacy officer vooraf goedkeuring te verlenen. Bij deze goedkeuring zijn doelmatigheid, subsidiariteit, proportionaliteit en risico's de toetsingscriteria;
- **Noodknop**. Als de privacy officer van NS Groep NV van mening is dat NS Stations of haar leveranciers en partners onzorgvuldig met privacy gevoelige informatie omgaan, kan zij gemotiveerd eisen dat het SMART Station systeem wordt uitgeschakeld totdat de bezwaren zijn weggenomen. Dit uitschakelen gebeurt door het afschakelen van de stroom naar de individuele scanunits.

3.5 Communicatie

NS Stations en haar partners zetten in op een proactieve communicatiestrategie. Deze communicatiestrategie is gebaseerd op drie pijlers:
1. Op het station
2. Met partners
3. Laagdrempelig en publiek toegankelijk

1. Op het station
Aan alle gebruikers van het station wordt vanaf uiterlijk medio 2017 door middel van signing ("bordjes en/of stickers") kenbaar gemaakt dat er sprake is van *Bluetooth/WiFi-tracking*. Hiermee wordt invulling gegeven aan het kenbaarheidsvereiste uit de WPB.

Het op de signing gehanteerde pictogram (figuur 6) is vergelijkbaar met de signing bij cameratoezicht. Op deze signing wordt tevens aangegeven waar geïnteresseerden meer informatie over SMART Station kunnen vinden. De toepassing van deze signing is inmiddels in voorbereiding, als onderdeel van de SMART Station projecten op de stations Amsterdam Zuid en Utrecht Centraal. Bij deze projecten is ProRail mede-opdrachtgever. Daarna volgen de bestaande SMART Stations op station Schiphol Airport, Leiden Centraal en Amsterdam Centraal.

Afbeelding 6: Pictogram Bluetooth/WiFi-tracking

2. Met partners
Bij diverse SMART Stations met *Bluetooth/WiFi-tracking* wordt met partners (vaak mede-opdrachtgevers) samengewerkt. Voorbeelden zijn Schiphol Groep (station Schiphol Airport), ProRail (stations Amsterdam Zuid en Utrecht Centraal), de gemeente Amsterdam (stations Amsterdam Centraal en Amsterdam Zuid) en huurders op het station (Utrecht Centraal, Leiden Centraal en Amsterdam Centraal).

Bij het vormgeven van dergelijke samenwerkingsverbanden is het informatiebeleid een vast bespreekpunt, waarbij het accepteren ervan door de partner voor NS Stations randvoorwaardelijk is voor een vervolg. De ervaring tot nu toe leert dat het Informatiebeleid SMART Station van NS het meest is ontwikkeld als het gaat om het beschermen van de privacy van gebruikers van (semi-) openbare ruimte. De ervaring leert ook dat een goede toelichting over de achtergronden van het Informatiebeleid voor de partners voldoende is om het vanuit bedrijfsmatig perspectief meest kritische deel van het beleid over te nemen: de tweede hash met de vermenging van de datum, waardoor terugkeerpatronen van individuele passanten niet meer inzichtelijk kunnen worden gemaakt.

Ter versterking van (de doorontwikkeling van) het meetconcept en de beeldvorming hieromtrent werkt NS Stations samen met de Technische Universiteit Delft. Deelname van de wetenschap bevordert niet alleen de kennisuitwisseling, maar draagt ook bij aan het vergroten van de maatschappelijke acceptatie van nieuwe meettechnologie voor toepassingen op het station. Tevens biedt ook de wetenschap een podium om het belang van privacy (wetenschapsethiek) te benadrukken. In deze context studeren regelmatig master studenten van de TU-Delft af op toepassingen van SMART Station. Daarnaast promoveert een medewerker van NS op de reizigerscapaciteit van treinstations. Bij dit onderzoek wordt onder andere gebruik gemaakt van data die verzameld met *Bluetooth/WiFi-tracking*.

Laagdrempelig en publiek toegankelijk
NS wordt met enige regelmaat door media of individuen benaderd met vragen over *Bluetooth/WiFi-tracking*. Verzoeken voor (meer) informatie zijn en worden zonder uitzondering positief beantwoord. Daarnaast zijn alle publicaties over SMART Station publiek toegankelijk. In 2017 wordt de vindbaarheid van de publicaties verbeterd door deze te koppelen aan dezelfde website die in het kader van de signing wordt ontwikkeld.

4 Risicomanagement

In dit hoofdstuk zijn de belangrijkste risico's benoemd, inclusief de genomen en de te nemen maatregelen om deze risico's te mitigeren.

Categorie	Risico	Maatregel	Activatie
1. Technologie	a. Een of meerdere scanunits met nog niet verzonden data wordt gestolen.	De scanunits zijn beveiligd door middel van passwords. Alleen de technologie partner/leverancier heeft toegang tot de software van de scanunit	Vooraf doorgevoerd
		De encryptie op de scanunit voorkomt dat privacygevoelige gegevens voor derden beschikbaar komen.	Vooraf doorgevoerd
		Na diefstal wordt de autorisatie van de scanunit op de server ingetrokken, waardoor geen communicatie meer mogelijk is.	Zodra risico optreedt
	b. Stroomuitval	Bij stroomuitval bij de servers en/of de verbindingen is de scanunit in staat om enige tijd de scangegevens lokaal op te slaan en deze data later te verzenden zodra de systemen en verbindingen weer online zijn. Na verzending en correcte ontvangst worden deze gegevens van de scanunit verwijderd.	Vooraf doorgevoerd
		De encryptie op de scanunit voorkomt dat privacygevoelige gegevens op een openbare plaats in het station blijven opgeslagen.	Vooraf doorgevoerd
2. Processen	a. Inbreuk op de verbinding tussen scanunit en server	De encryptie op de scanunit voorkomt dat privacygevoelige gegevens voor derden beschikbaar komen.	Vooraf doorgevoerd
		Wanneer blijkt dat een van de type verbindingen wordt gehackt, wordt overgeschakeld op een alternatieve verbinding (bijvoorbeeld WIFI > LAN of 3/4G).	Zodra risico optreedt
	b. Inbreuk op (de API van) de server van de technologie partner/leverancier met de scangegevens	De encryptie op de scanunit voorkomt dat privacygevoelige gegevens voor derden beschikbaar komen.	Vooraf doorgevoerd
	c. Inbreuk op (de webapplicatie van) de server van de	In de dienstverlening worden eisen gesteld aan de informatiebeveiliging, waarbij de algemeen geaccepteerde standaard wordt gevolgd.	Vooraf doorgevoerd

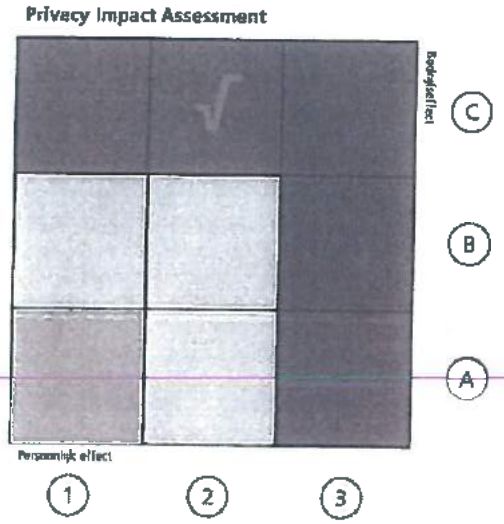
	technologie partner/leverancier	Wanneer desondanks een inbreuk in ICT-systemen plaatsvindt, wordt SMART Station helemaal uitgeschakeld totdat het beveiligingsprobleem is opgelost.	Zodra risico optreedt
	d. Leveranciers en partners gaan onzorgvuldig met privacygevoelige data om	De encryptie op de scanunit voorkomt dat privacygevoelige gegevens voor derden beschikbaar komen.	Vooraf doorgevoerd
		In overeenkomsten en service level agreements worden afspraken gemaakt over eigendom en het gebruik van data. Daarnaast wordt vooraf medewerking geregeld aan reviews en privacy impact assessment.	Vooraf doorgevoerd
		Wanneer tijdens de reguliere operatie of reviews blijkt dat afspraken herhaaldelijk niet worden nagekomen, wordt de samenwerking met de partner of leverancier in het uiterste geval verbroken.	Zodra risico optreedt
	e. NS Stations gaat onzorgvuldig met privacygevoelige data om	Het toezicht op zorgvuldig omgaan met de privacygevoelige informatie van SMART Station ligt bij de Privacy Officer van NS Groep.	Vooraf doorgevoerd
		Jaarlijks vindt een review plaats, vierjaarlijks in combinatie met een privacy impact assessment.	Vooraf doorgevoerd
		Bij onzorgvuldig handelen door NS Stations kan de privacy officer de noodknop indrukken waarbij SMART Station wordt uitgeschakeld totdat de knelpunten zijn opgelost.	Zodra risico optreedt
3. Communicatie	a. De AP start een privacy onderzoek naar SMART Station	Het privacybeleid van NS Groep is voor SMART Station vertaald in dit informatiebeleidsplan waarin maatregelen op het gebied van technologie, processen, communicatie en risicomanagement zijn beschreven.	Vooraf doorgevoerd
		Daarnaast is in de ontwikkelfase door [redacted] een Privacy Impact Assessment uitgevoerd, waarbij de verbeterpunten in SMART Station zijn opgenomen. Deze rapportage is beschikbaar.	Vooraf doorgevoerd
		Met de (proactieve) communicatiestrategie wordt beoogd vooraf openheid van zaken te geven,	Vooraf doorgevoerd

		zodat een zorgvuldig en oprecht beeld van SMART Station wordt neergezet. Als de AP desondanks toch een onderzoek start wordt daaraan volle medewerking verleend. Als de AP desondanks vaststelt dat in strijd met de wet wordt gehandeld, dan wordt opnieuw een afweging gemaakt of NS Stations doorgaat met een aangepast SMART Station of het systeem definitief wordt uitgeschakeld.	Zodra risico optreedt Zodra risico optreedt
	b. De media zetten een onjuist beeld neer van de activiteiten van SMART Station.	Met de (proactieve) communicatiestrategie wordt beoogd vooraf openheid van zaken te geven, zodat een zorgvuldig en oprecht beeld van SMART Station wordt neergezet. Er wordt gestreefd naar een samenwerking met de TU-Delft welke (naast kennisuitwisseling) de maatschappelijke acceptatie ondersteunt. Als blijkt dat er onvoldoende maatschappelijk draagvlak is voor SMART Station activiteiten en er schade aan de reputatie van NS optreedt, dan wordt het systeem uitgeschakeld.	Vooraf doorgevoerd Vooraf doorgevoerd Zodra risico optreedt
4. Overig	In het kader van opsporingsonderzoek doet de politie een vorderingsverzoek voor meetgegevens met betrekking tot locatie(s) en tijdstip(pen) van een MAC-adres van een mobiel apparaat dat object van onderzoek is.	Zodra het vorderingsverzoek is ontvangen wordt contact opgenomen met NS Security en de Privacy Officer van NS. Bij beider akkoord wordt door NS Stations op basis van het aangeleverde MAC-adres en tijdsinterval een databestand aangeleverd waarin de (gecodeerde) meetgegevens zijn opgenomen die betrekking hebben op het mobiele apparaat in het gevraagde tijdsinterval.	Zodra risico optreedt

5 Definitieve Privacy Assessment

Op basis van de huidige informatie en inzichten valt een deel van SMART Station binnen het bereik van de Wet Bescherming Persoonsgegevens (WBP). Tegelijk is NS, vanwege de maatschappelijke lopende discussies over privacy in combinatie met de positie van NS in de maatschappij, kwetsbaar voor negatieve beeldvorming. Dit informatiebeleid van SMART Station is opgesteld om te waarborgen dat alle bij SMART Station betrokken partijen aantoonbaar zorgvuldig omgaan met privacygevoelige informatie van SMART Station.

Als het pakket van maatregelen op het gebied van technologie, organisatie, communicatie en risicomanagement uit dit Informatiebeleidsplan is geïmplementeerd, worden de risico's van de privacy-score C2 in voldoende mate beheerst. Hiermee voldoet het SMART Station-programma aan het privacybeleid van NS Groep.



Afbeelding 7: Definitieve privacy score SMART Station

Bijlage 1: Publicatielijst

Voskamp, A. (2012). Measuring the influence of congested bottlenecks on route choice behavior of pedestrians at Utrecht Centraal. Master scriptie TU-Delft.

van den Heuvel, J.; Thiellier, E.; van Gerwen, N. (2013). Privacy by design bij reizigersmetingen op stations, *Privacy & Compliance* **3**, 17-21.

Van den Heuvel, J.; Voskamp, A.; Daamen, W.; Hoogendoorn, S. (2015). Using Bluetooth to estimate the impact of congestion on pedestrian route choice at train stations. *TRAFFIC AND GRANULAR FLOW '13*.

Ton, D. (2014). Navistation. A study into the route and activity location choice behaviour of departing pedestrians in train stations. Master scriptie TU-Delft.

Ton, D.; van den Heuvel, J.; Hoogendoorn, S. (2014). 'Zo kiest de treinreiziger zijn trap of roltrap. Wetenschappelijk onderzoek naar routeroute in het station.', Verkeerskunde 7, 16-17.

Ton, D.; van den Heuvel, J., Daamen, W., Hoogendoorn, S. (2015). Route and activity location choice behaviour of departing passengers in train stations. Presented at the hEART (European Association for Research in Transportation) 2015 conference, 9-11 september 2015, Copenhagen, Denmark.

van den Heuvel, J.; Ton, D.; Hermansen, K. (2016). Advances in Measuring Pedestrians at Dutch Train Stations Using Bluetooth, WiFi and Infrared Technology. *TRAFFIC AND GRANULAR FLOW '15*.

Colofon

Auteur(s)	[redacted]
Kenmerk	2016/smst/JvdH/001
Datum	29 december 2016
Versie	3
Status	Definitief

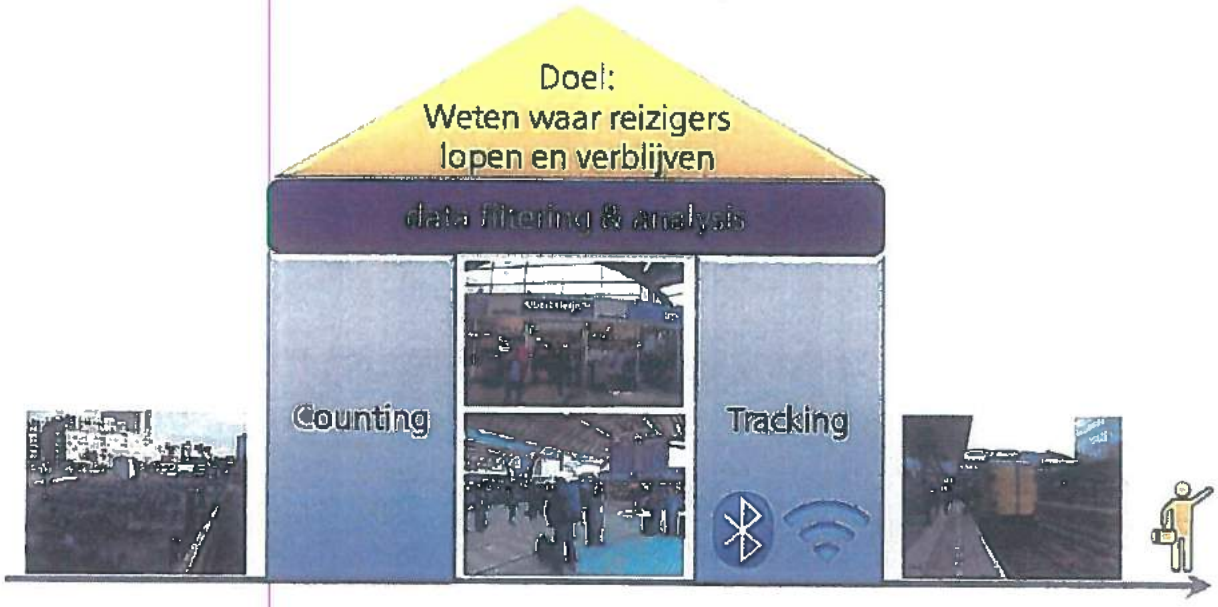
Document 15

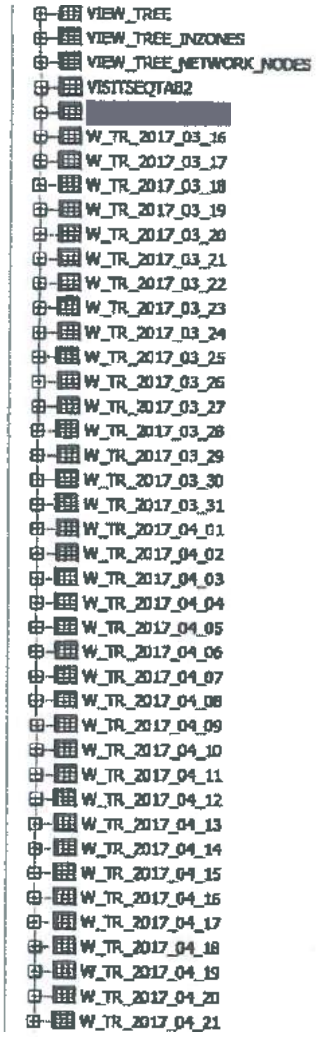
Document 16

- Rapportage in opdracht van ProRail
- Passagegegevens NS

Onderzoeksmethode: metingen door middel van SMART Station

- Uitbreiding SMART Station [redacted]
  - Automatisch door middel van sensoren
  - People Counters aan de [redacted]
  - Bluetooth/WIFI sensoren aan [redacted] (incl. doorsteek [redacted])
  - Op treinstations bewezen meetmethode, met nauwkeurigheid > 80% aan [redacted] en > 95% aan de [redacted]
- Meetperiode
  - 20 januari t/m14 februari 2015, waarvan in dataset:
    - Werkdagen: 20, 22, 23, 26 januari en 4,5,6,9,10,11,12 en 13 februari 2015
    - Weekenddagen: 21 en 31 januari, 1, 8 en 14 februari 2015
  - 24 uur per dag gemeten





Worksheet | Query Builder

```
1  select * from USER_TABLES where table_name like 'W_TR%' order by table_name asc;
2
```

Query Result ×

SQL | Fetched 50 rows in 0,126 seconds

	TABLE_NAME	TABLESPACE_NAME	CLUSTER_NAME	IOT_NAME	STATUS	PCT_FREE	PCT_USED	INI_TRANS	MAX_TRANS	INITIAL_EXTENT	NEXT_EXTENT	MIN_EXTEN
1	W_TR_2017_03_15	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
2	W_TR_2017_03_16	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
3	W_TR_2017_03_17	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
4	W_TR_2017_03_18	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
5	W_TR_2017_03_19	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
6	W_TR_2017_03_20	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
7	W_TR_2017_03_21	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
8	W_TR_2017_03_22	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
9	W_TR_2017_03_23	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
10	W_TR_2017_03_24	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
11	W_TR_2017_03_25	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
12	W_TR_2017_03_26	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
13	W_TR_2017_03_27	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
14	W_TR_2017_03_28	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
15	W_TR_2017_03_29	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
16	W_TR_2017_03_30	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
17	W_TR_2017_03_31	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
18	W_TR_2017_04_01	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
19	W_TR_2017_04_02	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
20	W_TR_2017_04_03	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	
21	W_TR_2017_04_04	NPC_ARCHIVE	(null)	(null)	VALID	10	(null)	1	255	65536	1048576	

Messages - Log

Document 18

Document 19

Document 20

Document 21

- Interne memo AP

AUTORITEIT
PERSOONSGEGEVENS

Datum
8 januari 2019

Nummer
z2017-05365

BIJLAGE 1

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-en-telecom#faq (08-01-2019)

Vragen over wifitracking en bluetoothtracking

- Mag ik als bedrijf wifitracking en bluetoothtracking inzetten?

  Met wifitracking en bluetoothtracking verwerkt u persoonsgegevens. Dat betekent dat u aan de Algemene verordening gegevensbescherming (AVG) moet voldoen. Volgens de AVG mag u alleen persoonsgegevens verwerken als u hiervoor een wettelijke grondslag heeft.

  ## Grondslag voor wifi- en bluetoothtracking

  In artikel 6 van de AVG staan 6 grondslagen genoemd. Hiervan komen 3 grondslagen mogelijk in aanmerking voor wifi- en bluetoothtracking door private partijen: toestemming, overeenkomst en gerechtvaardigd belang.

  Of u wifi- en bluetoothtracking kunt baseren op een van deze grondslagen, hangt van uw specifieke situatie af. Het kan bijvoorbeeld uitmaken of u enkel een commercieel doel heeft of niet.

- Mag ik als gemeente wifitracking en bluetoothtracking inzetten?

  Andere organisaties dan bedrijven, zoals gemeenten, kunnen via wifitracking en bluetoothtracking persoonsgegevens verwerken als dit noodzakelijk is om hun taak uit te voeren. Bijvoorbeeld het bewaken van de openbare orde of het handhaven van de veiligheid in de stad.

  ## Voorwaarden wifi- en bluetoothtracking

  Als gemeente mag u wifi- en bluetoothtracking alleen toepassen onder strikte voorwaarden. Zo moet u er een zelfstandige wettelijke grondslag voor hebben.

  Het mag ook alleen in specifieke periodes en in precies omschreven gebieden, waarin het echt nodig is. Op andere momenten en plaatsen zou de meetapparatuur uit moeten staan.

  Zie verder: AP wijst winkels en gemeenten op voorwaarden wifitracking.

- Verwerk ik als organisatie persoonsgegevens met wifitracking en bluetoothtracking?

  Ja. Met wifi- en bluetoothtracking verzamelt u een combinatie van gegevens waarmee iemand te identificeren is. En dat betekent dat deze gegevens persoonsgegevens zijn.

  Bij wifi- en bluetoothtracking verzamelt u doorgaans iemands MAC-adres (het unieke nummer van een telefoon of ander mobiel apparaat), de signaalsterkte van het geregistreerde wifi- of bluetoothsignaal, het serienummer en/of de locatie van de sensor en het tijdstip van de waarneming.

  Van direct identificerende gegevens is in dit geval geen sprake. Het gaat hier niet om gegevens als namen, adressen en telefoonnummers. Een enkel MAC-adres op zichzelf onthult ook niet direct de identiteit van een persoon.

  Toch zijn het persoonsgegevens. We noemen dit indirect identificeerbare persoonsgegevens. Dat komt omdat u de gegevens kunt combineren met elkaar of met andere gegevens. Zo kunt u de gegevens terugbrengen tot een bepaald persoon.

  Aanvullende gegevens waarmee u mensen indirect kunt identificeren zijn bijvoorbeeld camerabeelden, betalingsgegevens in winkels, inloggegevens van openbare wifi-hotspots of het gebruik van toegangspoortjes met unieke identificatoren, zoals RFID-tags.

- Ik pas bij wifitracking en bluetoothtracking hashing toe. dan zijn het toch geen persoonsgegevens meer?

  Dat klopt niet. Ook als u hashing toepast op de MAC-adressen die u verzamelt, blijven het persoonsgegevens. Dat komt omdat u met hashing de gegevens meestal niet onomkeerbaar anonimiseert.

  Alleen het hashen van MAC-adressen, zonder aanvullende maatregelen, leidt er niet toe dat u geen persoonsgegevens meer verwerkt. Er is dan namelijk geen sprake van (onmiddellijke en onomkeerbare) anonimisering, maar van pseudonimisering.

  Bijvoorbeeld omdat u zelf de hashingformule heeft. Dat betekent dat u de originele MAC-adressen opnieuw zou kunnen berekenen. De gegevens zijn dan dus niet anoniem.

Voorwaarden anonimiseren

Volgens de Algemene verordening gegevensbescherming (AVG) is er pas sprake van anonieme gegevens als persoonsgegevens zodanig anoniem zijn gemaakt dat de betrokkene niet (meer) direct of indirect identificeerbaar is.

Het loskoppelen van (in)direct identificerende persoonsgegevens en de overige gegevens moet onomkeerbaar zijn. U mag deze gegevens ook in een later stadium niet alsnog aan elkaar kunnen koppelen. Bijvoorbeeld door andere (bijkomende of nieuwe) gegevens of technieken te gebruiken, waardoor u personen toch nog zou kunnen identificeren.

[redacted]

AVG wel of niet toepassing

Zijn de persoonsgegevens daadwerkelijk geanonimiseerd? Dan is de AVG niet (meer) van toepassing op die gegevens.

[redacted]

- Kan ik als bedrijf wifi- en bluetoothtracking baseren op toestemming?

Het is niet uitgesloten dat u toestemming vraagt aan betrokkenen om hen te volgen met wifi- en bluetoothtracking. Alleen is dat praktisch en technisch gezien lastig uitvoerbaar door de voorwaarden waaraan toestemming moet voldoen.

Voorwaarden toestemming

U mag persoonsgegevens verwerken als de betrokkenen (de mensen om wie het gaat) hiervoor toestemming hebben gegeven (artikel 6, eerste lid, onder a, van de Algemene verordening gegevensbescherming).

Toestemming is echter alleen geldig als deze aan een aantal eisen voldoet.

- Kan ik als bedrijf wifi- en bluetoothtracking baseren op een overeenkomst?

Is het noodzakelijk om een betrokkene te volgen met wifi- en bluetoothtracking om een overeenkomst met hem of haar uit te voeren? Dan kunt u deze verwerking van persoonsgegevens mogelijk baseren op de grondslag 'overeenkomst' (artikel 6, eerste lid, onder b, van de Algemene verordening gegevensbescherming).

Noodzakelijk

Een betrokkene en u zijn in principe vrij om overeen te komen wat u wilt (contractsvrijheid), mits u aan het Burgerlijk Wetboek voldoet (niet in strijd met goede zeden, etc.). U kunt zich echter niet automatisch beroepen op de grondslag 'overeenkomst' als u een overeenkomst sluit met een betrokkene.

Bij de weging of de gegevensverwerking noodzakelijk is voor de te leveren prestatie, moet u vaststellen wat de exacte beweegredenen zijn voor het contract. Dat wil zeggen: de inhoud en het fundamentele doel ervan en of de gegevensverwerking daadwerkelijk noodzakelijk is voor die prestatie.

Let op: enkel het feit dat u wifi- en bluetoothtracking opneemt in de overeenkomst, wil niet zeggen dat u voldoet aan de eis dat deze verwerking noodzakelijk is om de overeenkomst uit te voeren.

Soms toestemming vereist

Krijgt u toegang tot informatie in de randapparatuur van een gebruiker door de manier waarop de wifi- of bluetoothsensoren gegevens uitlezen van randapparatuur? Zoals identifiers en locatiegegevens? Dan mag dit op grond van artikel 11.7a van de Telecommunicatiewet alleen als de gebruiker hiervoor toestemming heeft gegeven.

Is deze verwerking van informatie uit de randapparatuur van de gebruiker **niet** noodzakelijk om de overeenkomst uit te voeren? Dan geldt de toestemming alleen als de betrokkene afzonderlijk toestemming kan geven voor deze verwerking. En als u de overeenkomst ook uitvoert als de betrokkene géén toestemming geeft.

- Kan ik als bedrijf wifi- en bluetoothtracking baseren op gerechtvaardigd belang?

Dat hangt ervan af in welke omgeving u mensen wilt volgen met wifitracking en bluetoothtracking. Het maakt verschil of u dit in de openbare ruimte (zoals winkelstraten) wilt doen of in semiopenbare ruimte die privaat bezit is. Ook speelt mee wat het doel is van de wifi-en bluetoothtracking.

Gezag in de openbare ruimte

De verwerking van persoonsgegevens in de openbare ruimte valt primair onder de verantwoordelijkheid van, of moet mogelijk zijn gemaakt door, de (wetgevende) overheid. Een private partij zoals een bedrijf heeft daar doorgaans geen gezag. Daarom kan een private partij niet zonder meer een beroep doen op gerechtvaardigd belang.

Het is niet uitgesloten dat u als bedrijf een beroep op deze grondslag kunt doen. Bijvoorbeeld als wifi- en bluetoothtracking onvermijdelijk is om het private eigendom te beschermen in de openbare ruimte. Of als u een beroep kunt doen op de journalistieke exceptie.

Semiopenbare ruimte die privaat bezit is

Wilt u als bedrijf met wifitracking en bluetoothtracking mensen volgen in de semiopenbare ruimte die privaat bezit is? En heeft u geen commercieel doel, maar is uw doel om de veiligheid van passanten te waarborgen? Dan kan een beroep op gerechtvaardigd belang onder strikte voorwaarden mogelijk zijn.

De bescherming van de fysieke veiligheid van betrokkenen betreft een gerechtvaardigd belang. Om dit belang - een grondrecht - te beschermen, kan het noodzakelijk zijn om (ook) persoonsgegevens te verwerken. Bijvoorbeeld om gevaarlijke drukte op bepaalde punten te voorkomen (*crowd control*).

U voldoet daarmee aan de eerste eis om een beroep te kunnen doen op de grondslag van gerechtvaardigd belang. U moet dan nog wel voldoen aan de andere voorwaarden van artikel 6, eerste lid, onder f van de Algemene verordening gegevensbescherming. Ten eerste moet uw verwerking voldoen aan de vereisten van proportionaliteit en subsidiariteit. Ten tweede moet u uw belangen en die van de betrokkenen tegen elkaar afwegen.

Proportionaliteit en subsidiariteit

Het vereiste van proportionaliteit houdt in dat de inbreuk op de privacy van de betrokkenen in verhouding moet staan tot het doel van de wifi-of bluetoothtracking.

Het vereiste van subsidiariteit houdt in dat er niet een minder zwaar middel mogelijk mag zijn dan wifi-of bluetoothtracking, dat minder inbreuk maakt op de privacy.

Zo moet u toelichten waarom u dat gerechtvaardigde belang niet op een andere manier en zonder de verwerking van persoonsgegevens even effectief kan beschermen.

Belangenafweging

Bij de belangenafweging speelt mee of u extra waarborgen treft om de ongewenste gevolgen voor betrokkenen te voorkomen of beperken. Bijvoorbeeld door de volgende 3 maatregelen te nemen:

- de trackinggegevens onmiddellijk, op de sensor, te anonimiseren;
- per meetlocatie de gegevens telkens op een andere manier te hashen, zodanig dat er geen technische mogelijkheid is om betrokkenen door de tijd heen over meerdere locaties te volgen;
- nadere waarborgen te treffen, zoals het beperken van de metingen in ruimte en tijd tot specifieke tijden en locaties (in plaats van 24 uur per dag en 7 dagen per week meten).

Een andere mogelijke waarborg is om betrokkenen de mogelijkheid te bieden zich af te melden voor wifi-en bluetoothtracking (opt-out). Hierdoor kunnen zij zich onttrekken aan metingen in hun (privé-)omgeving. Het is hierbij belangrijk dat u de opt-outmogelijkheid duidelijk kenbaar maakt aan betrokkenen.

Datum	Nummer
8 januari 2019	z2017-05365

Bijlage 2: zie email bijlage (memo bluetooth of wifitracking 15-9)

AUTORITEIT
PERSOONSGEGEVENS

Datum
8 januari 2019

Nummer
z2017-05365

BIJLAGE 3

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-en-telecom#faq (08-01-2019)

Vragen over wifitracking en bluetoothtracking

- Mag ik als bedrijf wifitracking en bluetoothtracking inzetten?

  Met wifitracking en bluetoothtracking verwerkt u persoonsgegevens. Dat betekent dat u aan de Algemene verordening gegevensbescherming (AVG) moet voldoen. Volgens de AVG mag u alleen persoonsgegevens verwerken als u hiervoor een wettelijke grondslag heeft.

  ## Grondslag voor wifi- en bluetoothtracking

  In artikel 6 van de AVG staan 6 grondslagen genoemd. Hiervan komen 3 grondslagen mogelijk in aanmerking voor wifi- en bluetoothtracking door private partijen: toestemming, overeenkomst en gerechtvaardigd belang.

  Of u wifi- en bluetoothtracking kunt baseren op een van deze grondslagen, hangt van uw specifieke situatie af. Het kan bijvoorbeeld uitmaken of u enkel een commercieel doel heeft of niet.

- Mag ik als gemeente wifitracking en bluetoothtracking inzetten?

  Andere organisaties dan bedrijven, zoals gemeenten, kunnen via wifitracking en bluetoothtracking persoonsgegevens verwerken als dit noodzakelijk is om hun taak uit te voeren. Bijvoorbeeld het bewaken van de openbare orde of het handhaven van de veiligheid in de stad.

  ## Voorwaarden wifi- en bluetoothtracking

  Als gemeente mag u wifi- en bluetoothtracking alleen toepassen onder strikte voorwaarden. Zo moet u er een zelfstandige wettelijke grondslag voor hebben.

  Het mag ook alleen in specifieke periodes en in precies omschreven gebieden, waarin het echt nodig is. Op andere momenten en plaatsen zou de meetapparatuur uit moeten staan.

  Zie verder: AP wijst winkels en gemeenten op voorwaarden wifitracking.

- Verwerk ik als organisatie persoonsgegevens met wifitracking en bluetoothtracking?

  Ja. Met wifi- en bluetoothtracking verzamelt u een combinatie van gegevens waarmee iemand te identificeren is. En dat betekent dat deze gegevens persoonsgegevens zijn.

  Bij wifi- en bluetoothtracking verzamelt u doorgaans iemands MAC-adres (het unieke nummer van een telefoon of ander mobiel apparaat), de signaalsterkte van het geregistreerde wifi- of bluetoothsignaal, het serienummer en/of de locatie van de sensor en het tijdstip van de waarneming.

  Van direct identificerende gegevens is in dit geval geen sprake. Het gaat hier niet om gegevens als namen, adressen en telefoonnummers. Een enkel MAC-adres op zichzelf onthult ook niet direct de identiteit van een persoon.

  Toch zijn het persoonsgegevens. We noemen dit indirect identificeerbare persoonsgegevens. Dat komt omdat u de gegevens kunt combineren met elkaar of met andere gegevens. Zo kunt u de gegevens terugbrengen tot een bepaald persoon.

  Aanvullende gegevens waarmee u mensen indirect kunt identificeren zijn bijvoorbeeld camerabeelden, betalingsgegevens in winkels, inloggegevens van openbare wifi-hotspots of het gebruik van toegangspoortjes met unieke identificatoren, zoals RFID-tags.

- Ik pas bij wifitracking en bluetoothtracking hashing toe, dan zijn het toch geen persoonsgegevens meer?

  Dat klopt niet. Ook als u hashing toepast op de MAC-adressen die u verzamelt, blijven het persoonsgegevens. Dat komt omdat u met hashing de gegevens meestal niet onomkeerbaar anonimiseert.

  Alleen het hashen van MAC-adressen, zonder aanvullende maatregelen, leidt er niet toe dat u geen persoonsgegevens meer verwerkt. Er is dan namelijk geen sprake van (onmiddellijke en onomkeerbare) anonimisering, maar van pseudonimisering.

  Bijvoorbeeld omdat u zelf de hashingformule heeft. Dat betekent dat u de originele MAC-adressen opnieuw zou kunnen berekenen. De gegevens zijn dan dus niet anoniem.

Voorwaarden anonimiseren

Volgens de Algemene verordening gegevensbescherming (AVG) is er pas sprake van anonieme gegevens als persoonsgegevens zodanig anoniem zijn gemaakt dat de betrokkene niet (meer) direct of indirect identificeerbaar is.

Het loskoppelen van (in)direct identificerende persoonsgegevens en de overige gegevens moet onomkeerbaar zijn. U mag deze gegevens ook in een later stadium niet alsnog aan elkaar kunnen koppelen. Bijvoorbeeld door andere (bijkomende of nieuwe) gegevens of technieken te gebruiken, waardoor u personen toch nog zou kunnen identificeren.

[redacted]

AVG wel of niet toepassing

Zijn de persoonsgegevens daadwerkelijk geanonimiseerd? Dan is de AVG niet (meer) van toepassing op die gegevens.

[redacted]

- Kan ik als bedrijf wifi- en bluetoothtracking baseren op toestemming?

Het is niet uitgesloten dat u toestemming vraagt aan betrokkenen om hen te volgen met wifi- en bluetoothtracking. Alleen is dat praktisch en technisch gezien lastig uitvoerbaar door de voorwaarden waaraan toestemming moet voldoen.

Voorwaarden toestemming

U mag persoonsgegevens verwerken als de betrokkenen (de mensen om wie het gaat) hiervoor toestemming hebben gegeven (artikel 6, eerste lid, onder a, van de Algemene verordening gegevensbescherming).

Toestemming is echter alleen geldig als deze aan een aantal eisen voldoet.

- Kan ik als bedrijf wifi- en bluetoothtracking baseren op een overeenkomst?

Is het noodzakelijk om een betrokkene te volgen met wifi- en bluetoothtracking om een overeenkomst met hem of haar uit te voeren? Dan kunt u deze verwerking van persoonsgegevens mogelijk baseren op de grondslag 'overeenkomst' (artikel 6, eerste lid, onder b, van de Algemene verordening gegevensbescherming).

Noodzakelijk

Een betrokkene en u zijn in principe vrij om overeen te komen wat u wilt (contractsvrijheid), mits u aan het Burgerlijk Wetboek voldoet (niet in strijd met goede zeden, etc.). U kunt zich echter niet automatisch beroepen op de grondslag 'overeenkomst' als u een overeenkomst sluit met een betrokkene.

Bij de weging of de gegevensverwerking noodzakelijk is voor de te leveren prestatie, moet u vaststellen wat de exacte beweegredenen zijn voor het contract. Dat wil zeggen: de inhoud en het fundamentele doel ervan en of de gegevensverwerking daadwerkelijk noodzakelijk is voor die prestatie.

Let op: enkel het feit dat u wifi- en bluetoothtracking opneemt in de overeenkomst, wil niet zeggen dat u voldoet aan de eis dat deze verwerking noodzakelijk is om de overeenkomst uit te voeren.

Soms toestemming vereist

Krijgt u toegang tot informatie in de randapparatuur van een gebruiker door de manier waarop de wifi- of bluetoothsensoren gegevens uitlezen van randapparatuur? Zoals identifiers en locatiegegevens? Dan mag dit op grond van artikel 11.7a van de Telecommunicatiewet alleen als de gebruiker hiervoor toestemming heeft gegeven.

Is deze verwerking van informatie uit de randapparatuur van de gebruiker **niet** noodzakelijk om de overeenkomst uit te voeren? Dan geldt de toestemming alleen als de betrokkene afzonderlijk toestemming kan geven voor deze verwerking. En als u de overeenkomst ook uitvoert als de betrokkene géén toestemming geeft.

- Kan ik als bedrijf wifi- en bluetoothtracking baseren op gerechtvaardigd belang?

Dat hangt ervan af in welke omgeving u mensen wilt volgen met wifitracking en bluetoothtracking. Het maakt verschil of u dit in de openbare ruimte (zoals winkelstraten) wilt doen of in semiopenbare ruimte die privaat bezit is. Ook speelt mee wat het doel is van de wifi-en bluetoothtracking.

Gezag in de openbare ruimte

De verwerking van persoonsgegevens in de openbare ruimte valt primair onder de verantwoordelijkheid van, of moet mogelijk zijn gemaakt door, de (wetgevende) overheid. Een private partij zoals een bedrijf heeft daar doorgaans geen gezag. Daarom kan een private partij niet zonder meer een beroep doen op gerechtvaardigd belang.

Het is niet uitgesloten dat u als bedrijf een beroep op deze grondslag kunt doen. Bijvoorbeeld als wifi- en bluetoothtracking onvermijdelijk is om het private eigendom te beschermen in de openbare ruimte. Of als u een beroep kunt doen op de journalistieke exceptie.

Semiopenbare ruimte die privaat bezit is

Wilt u als bedrijf met wifitracking en bluetoothtracking mensen volgen in de semiopenbare ruimte die privaat bezit is? En heeft u geen commercieel doel, maar is uw doel om de veiligheid van passanten te waarborgen? Dan kan een beroep op gerechtvaardigd belang onder strikte voorwaarden mogelijk zijn.

De bescherming van de fysieke veiligheid van betrokkenen betreft een gerechtvaardigd belang. Om dit belang - een grondrecht - te beschermen, kan het noodzakelijk zijn om (ook) persoonsgegevens te verwerken. Bijvoorbeeld om gevaarlijke drukte op bepaalde punten te voorkomen (*crowd control*).

U voldoet daarmee aan de eerste eis om een beroep te kunnen doen op de grondslag van gerechtvaardigd belang. U moet dan nog wel voldoen aan de andere voorwaarden van artikel 6, eerste lid, onder f van de Algemene verordening gegevensbescherming. Ten eerste moet uw verwerking voldoen aan de vereisten van proportionaliteit en subsidiariteit. Ten tweede moet u uw belangen en die van de betrokkenen tegen elkaar afwegen.

Proportionaliteit en subsidiariteit

Het vereiste van proportionaliteit houdt in dat de inbreuk op de privacy van de betrokkenen in verhouding moet staan tot het doel van de wifi-of bluetoothtracking.

Het vereiste van subsidiariteit houdt in dat er niet een minder zwaar middel mogelijk mag zijn dan wifi-of bluetoothtracking, dat minder inbreuk maakt op de privacy.

Zo moet u toelichten waarom u dat gerechtvaardigde belang niet op een andere manier en zonder de verwerking van persoonsgegevens even effectief kan beschermen.

Belangenafweging

Bij de belangenafweging speelt mee of u extra waarborgen treft om de ongewenste gevolgen voor betrokkenen te voorkomen of beperken. Bijvoorbeeld door de volgende 3 maatregelen te nemen:

- de trackinggegevens onmiddellijk, op de sensor, te anonimiseren;
- per meetlocatie de gegevens telkens op een andere manier te hashen, zodanig dat er geen technische mogelijkheid is om betrokkenen door de tijd heen over meerdere locaties te volgen;
- nadere waarborgen te treffen, zoals het beperken van de metingen in ruimte en tijd tot specifieke tijden en locaties (in plaats van 24 uur per dag en 7 dagen per week meten).

Een andere mogelijke waarborg is om betrokkenen de mogelijkheid te bieden zich af te melden voor wifi-en bluetoothtracking (opt-out). Hierdoor kunnen zij zich onttrekken aan metingen in hun (privé-)omgeving. Het is hierbij belangrijk dat u de opt-outmogelijkheid duidelijk kenbaar maakt aan betrokkenen.

AUTORITEIT
PERSOONSGEGEVENS

Verslag gesprek NS-wifitracking

Aanwezig namens NS: mr. U.H. (Udo) Oelen, Functionaris Gegevensbescherming NS, mr. [redacted] Privacy Officer NS en ir. [redacted] ontwikkelaar bij de NS.
Aanwezig namens de AP: [redacted]
Datum verslag: 17 januari 2019
Opsteller verslag: [redacted]
...

Op maandag 14 januari 2019 heeft de AP een gesprek gehad met werknemers van de NS omtrent wifitracking.

Inleiding gesprek:
De AP geeft een korte toelichting op de aanleiding en doel van het gesprek.

De aanleiding van dit gesprek:
- In juni / juli 2017 heeft de AP informatie opgevraagd bij de NS omtrent bluetooth- en wifitracking op NS stations.
- In augustus 2017 heeft de NS desgevraagde informatie verstrekt.
- In november 2018 heeft de AP een normenkader over wifi- en bluetoothtracking op de website van de AP gepubliceerd.
- Naar aanleiding van dit normenkader nam de NS contact op met de AP om het e.e.a. te bespreken.

De AP deelt mee dat het doel van dit gesprek het bespreken van de huidige stand van zaken van de NS omtrent wifitracking op NS-stations is. Er is sinds de NS informatie heeft gestuurd aan de AP al zo'n 1.5 jaar verstreken en daarom is het belangrijk na te gaan of deze informatie nog correct is. Het doel is dus niet om onderzoek te doen, maar dit gesprek zou aanleiding kunnen zijn om een onderzoek te starten.

Reactie NS:
Het doel is duidelijk, maar als we de huidige stand van zaken bespreken wat is dan de status van de informatie die eerder door de NS gegeven is? Daarnaast wordt er gevraagd wat het termijn is waarin de NS duidelijkheid kan verwachten?

De AP geeft aan dat we gaan kijken hoe dit gesprek loopt en mocht dit aanleiding geven om nader onderzoek te gaan doen we de eerder gegeven antwoorden van NS zullen meenemen in het onderzoek. Verder geeft ze aan dat ze geen termijn kan geven, eerst moet het verloop van dit gesprek worden afgewacht.

Vraag:
Wat is de actuele stand van zaken met betrekking tot wifitracking bij de NS, zijn er zaken gewijzigd ten opzichte van de antwoorden gegeven in 2017?

De NS geeft aan:
De belangrijkste veranderingen zijn:
- Het sluiten van verwerkingsovereenkomsten (met Blip);

- Erkennen dat MAC-adressen persoonsgegevens zijn;
- Scherpere afspraken met verwerkers omtrent het implementeren van beveiligingsmaatregelen;
- Bluetooth-tracking staat uit;
- Er is geen wifitracking meer op station Leiden;
- Meer informeren en communiceren naar reizigers omtrent wifitracking, door specifieke stickers bij alle ingangen.

Vraag:
Hoe zit het met het aantal stations waar gebruik wordt gemaakt van wifitracking? Zijn er plannen dit aantal uit te breiden of in te krimpen?

De NS geeft aan:
De informatie op de website van de NS klopt nog steeds. Er zijn nu 5 stations waar wifitracking plaatsvindt, zijnde Amsterdam Centraal, Amsterdam Zuid, Utrecht Centraal, Schiphol en 's Hertogenbosch. Elke 3 maanden wordt geëvalueerd door [redacted] en [redacted] om na te gaan of de doelen waarvoor de wifitracking wordt gebruikt al bereikt zijn. Om deze reden is de wifitracking bij station Leiden gestopt. Het doel is bereikt, dus de wifitracking stopt.

Wat van belang is, is om te benadrukken is dat de NS wifitracking alleen inzet wanneer het echt nodig is. Dit is het geval bij complexe stations. Bij minder complexe stations zijn de gegevens van de incheckpoortjes voldoende en wordt er dus geen gebruik gemaakt van wifitracking. Er wordt dus per specifiek station gekeken wat de beste aanpak is. Zo is station Bijlmer ArenA omringd door het Ziggo Dome, de Johan Cruijff ArenA en concert hall AFAS live. Het gebeurt dat de evenementen die plaatsvinden op deze locaties rond dezelfde tijd eindigen en dit zorgt voor grote drukte op station Bijlmer ArenA. Op dit station is er echter voor gekozen om geen wifitracking in te zetten omdat het geen additionele informatie oplevert. We gebruiken op dit station telcamera's en deze zijn voldoende om de loopstromen in kaart te brengen. Een voorbeeld waarbij wifitracking wel additionele informatie oplevert is als er een grote verbouwing van een station plaats gaat vinden. Via wifitracking kan worden gekeken wat de beste en meest veilige manier is om het station in te richten zodat mensenmassa's bijvoorbeeld niet vast komen te zitten op bepaalde plekken.

Vraag:
Zijn er voorbeelden die aantonen dat 'crowd control' problemen oplevert op stations?

De NS geeft aan:
Ja, bij de roltrappen op station Bijlmer ArenA. Deze roltrappen waren soms zo overladen vol dat mensen er langs de zijkant af moesten springen. Daarnaast is spoor 5 op Utrecht Centraal dagelijks overbelast. Pro Rail heeft hiervoor ook een 'overbelastverklaring' voor afgegeven. Er zijn zoveel mensen op het perron dat het niet meer past. Dit met het gevaar dat mensen op het spoor terechtkomen. Door de drukte worden mensen steeds dichter naar het spoor gedrukt. Door wifitracking worden er werknemers van de NS ('de gele hesjes') ingezet als er sprake is van grote drukte. Deze werknemers verdelen de reizigers op het perron om gevaarlijke situaties te voorkomen.

Vraag:
Zijn het aantal sensoren dat per station hangt ongewijzigd gebleven? Op de site staat tussen de 12-34 per station?

De NS geeft aan:
Er zullen wat sensoren zijn toegevoegd, maar tussen de 12-34 is correct.

Vraag:
In hoeverre is de informatie over doeleinden en gerechtvaardigd belang in de brief van 14 augustus 2017 nog actueel?

De NS geeft aan:
De doelen zijn ongewijzigd. Het belangrijkste doel is en blijft veiligheid. De doelen zijn bijna allemaal afgeleid aan het hoofddoel 'veiligheid'. Waar het gaat om loopstromen gebruiken we deze informatie ook voor de plaatsing van retail.

Vraag:
Zijn er specifieke rapportages voor dit commerciële doel (plaatsen van retail) die niet worden gebruikt voor het veiligheidsdoel?

De NS geeft aan:
Nee, er worden rapportages gemaakt met als doel veiligheid. Deze rapportages worden hergebruikt voor commerciële doelen. Er worden dus geen aparte rapportages gemaakt voor het commerciële doel. Bovendien staan er in deze rapportages geen persoonsgegevens meer, maar louter bezoekersaantallen met een verdeling qua ruimte en tijd.

Vraag:
Hoe worden gegevens bewaard en hoe lang?

De NS geeft aan:
De 'MAC-adressen worden op de sensor gehasht. Daarna wordt de data naar de server gestuurd en nogmaals gehasht (met een willekeurig nummer: 'de salt'). Het nummer dat zo gegenereerd wordt noemen we het passantnummer. De salt wordt om 04.00 iedere dag verandert.' Dat betekent dat een MAC-adres gedurende een dag, uiterlijk tot 04.00, hetzelfde passantnummer oplevert. Hiermee kan een apparaat door de tijd heen en binnen een station gevolgd worden als het MAC-adres door meerdere WIFI-sensoren opgevangen wordt.
Passantnummers worden 5 jaar bewaard worden om passagiersstromen en trends te analyseren. Voor alle primaire (lees veiligheid) en afgeleide doelen. Het passantnummer is alleen bekend bij de verwerker en leverancier van de WIFI-sensoren: 'BLIPS'. De NS heeft geen (directe) toegang tot de gegevens. De NS kan wel opvragen hoeveel mensen er via bepaalde loopstroom naar trein X gegaan op station Y. Een voorbeeld van een afgeleid doel, op basis van de geanonimiseerde rapporten, is een commercieel doel: Station Amsterdam centraal, de trend gedurende jaar waarmee de drukte op een dag gerelateerd kan worden aan de omzet van de winkels binnen het stationsgebied.

Vraag:
Wat zijn de andere technieken?

De NS geeft aan:

In het verleden is fysiek geteld op stations. Dit is echter niet betrouwbaar en ontzettend duur. Verder zijn er telcamera's en de data van de check-in en check-out poortjes. Daarnaast wordt er data verzameld via reizigersonderzoek en klanttevredenheidsonderzoek. Dit is op vrijwillige basis.

Vraag:
Staat de wifitracking altijd aan, zo ja, waarom?

De NS geeft aan:
Ja, de wifitracking staat altijd aan. Het zou mogelijk zijn om hem 's nachts uit te zetten, maar dit is niet wenselijk. Soms zijn er bijvoorbeeld 's nachts incidenten en deze calculeer je niet altijd in. Denk aan grote feesten waardoor het 's nachts opeens erg druk is of vertraagde vluchten op Schiphol waardoor het station overladen vol raakt. Je kunt deze situaties niet altijd inschatten, maar deze data is wel erg van belang.

Vraag:
De manier van tracken, de techniek is nog steeds hetzelfde als in 2017?

De NS geeft aan:
Ja, alles is nog hetzelfde.

Vraag:
Open vraag: Wil de NS nog iets meegeven?

De NS geeft aan:
NS heeft de opdracht reizigers veilig te vervoeren, dit staat ook in de wet. We doen er alles aan om ervoor te zorgen dat de reiziger veilig van punt A naar punt B komt. Er wordt bij elke situatie gekeken wat proportioneel en substantieel is.

Afsluiting gesprek

De AP licht toe dat we contact met NS opnemen over de uitkomst van het gesprek. NS geeft aan dat als er nog onduidelijkheden zijn bij de uitwerking van de feiten we altijd kunnen bellen.

Document 23

AUTORITEIT
PERSOONSGEGEVENS

NS Groep N.V.
T.a.v. de Directie
Laan van Puntenburg
3511 ER Utrecht

Datum
08 maart 2019

Ons kenmerk
z2017-05365

Contactpersoon
[redacted]
070 8525 500

Onderwerp
Wifitracking

Geachte directie,

Op 14 januari 2019 heeft een gesprek plaatsgevonden tussen de Autoriteit Persoonsgegevens (AP) en de Nationale Spoorwegen (NS).[1] Dit gesprek vond plaats naar aanleiding van de publicatie in november 2018 op de website van de AP van een normenkader over wifi- en bluetoothtracking.[2] Eerder[3] had de NS de AP desgevraagd informatie verstrekt over wifi- en bluetoothtracking op NS treinstations.

Het doel van het gesprek was om de huidige stand van zaken te bespreken omtrent wifi- en bluetoothtracking op NS-stations mede met het oogmerk om te bepalen of de informatie uit het gesprek aanleiding zou kunnen zijn voor het starten van een onderzoek. De AP informeert u door middel van deze brief over de uitkomst van dit gesprek.

De AP is op basis van het gesprek van 14 januari jl. en de bij de AP beschikbare informatie tot de conclusie gekomen dat beide geen aanleiding vormen om een onderzoek te starten naar de verwerking van persoonsgegevens via wifitracking door de NS.

De AP wijst u niettemin op het volgende. In het gesprek heeft de NS aangegeven dat de NS sinds haar reactie aan de AP in 2017 bij alle ingangen van de stations waar gebruik wordt gemaakt van wifitracking de reiziger hier meer over informeert door middel van specifieke stickers. De AP benadrukt dat zij het van

[1] Aanwezig namens NS: mr. U.H. (Udo) Oelen, Functionaris Gegevensbescherming NS, mr. [redacted] Privacy Officer NS en ir. [redacted] ontwikkelaar bij de NS.
[2] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-en-telecom#faq.
[3] Per brief op 14 augustus 2017.

AUTORITEIT
PERSOONSGEGEVENS

Datum
06 maart 2019

Ons kenmerk
z2017-05565

groot belang vindt dat het informeren van de reiziger over de verwerking van persoonsgegevens via wifisensoren op een goede en duidelijke wijze gebeurt.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Voor eventuele vragen kunt u contact opnemen met bovengenoemd contactpersoon.

Een afschrift van deze brief wordt tevens per e-mail verstuurd aan uw Functionaris Gegevensbescherming, via het e-mailadres fg@ns.nl.

Hoogachtend,
Namens deze,

[redacted]

mr. drs. G.N.J.A. Bukkems
Directeur Klantcontact en Controlerend Onderzoek