AUTORITEIT
PERSOONSGEGEVENS

Onderzoeksrapport definitieve bevindingen

Nippon Express (Nederland) B.V. Gebruik van ID scanner

z2015-00836

juni 2017

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

AUTORITEIT
PERSOONSGEGEVENS

Inhoudsopgave

Inhoud

1. Inleiding

1.1 Aanleiding onderzoek

De Autoriteit Persoonsgegevens (hierna ook: AP) heeft op grond van artikel 60 van de Wet bescherming persoonsgegevens (Wbp) een ambtshalve onderzoek ingesteld naar de verwerking van persoonsgegevens uit identiteitsdocumenten met scanapparatuur door Nippon Express (Nederland) B.V. (hierna: Nippon Express).[1] Nippon Express is een logistiek dienstverlener en houdt zich onder meer bezig met transport, overslag, opslag en distributie.

De Autoriteit Persoonsgegevens heeft de laatste jaren een aantal signalen ontvangen van vrachtwagenchauffeurs over Nippon Express.[2] Vrachtwagenchauffeurs zouden bij het laden bij Nippon Express verplicht zijn hun identiteitsdocument (ID) te laten scannen.[3] [4] Nippon Express zou hierbij onder andere de pasfoto en het burgerservicenummer (BSN) scannen. Door de scans lopen vrachtwagen-chauffeurs mogelijk een verhoogd risico op identiteitsfraude. Het risico op onregelmatigheden, zoals identiteitsfraude, neemt toe indien identiteitsdocumenten worden gescand en wanneer de gescande persoonsgegevens bewaard of zelfs verzonden worden naar een externe partij.

Volgens één signaal maakt Nippon Express bij het scannen van de identiteitsdocumenten gebruik van de diensten en de scanapparatuur van [naam leverancier] B.V. (hierna: [naam leverancier]).

Medewerkers van Nippon Express zouden op de verschillende locaties van Nippon Express met scanapparatuur van [naam leverancier] de identiteitsdocumenten van vrachtwagenchauffeurs scannen. Deze scans verzendt Nippon Express vervolgens elektronisch aan [naam leverancier]. [naam leverancier] zou met de aldus ontvangen scans voor Nippon Express de echtheid van de identiteitsdocumenten controleren.

De thema's bijzondere persoonsgegevens en beveiliging van persoonsgegevens kregen in 2016 extra aandacht van de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens heeft vanuit haar toezichthoudende rol naar aanleiding van het bovenstaande een onderzoek ingesteld naar de verwerking van persoonsgegevens bij Nippon Express.

Dit rapport bevat de resultaten van het ambtshalve onderzoek dat de Autoriteit Persoonsgegevens bij Nippon Express heeft uitgevoerd.

1.2 Doel onderzoek

Het onderzoek heeft zich geconcentreerd op de volgende vragen:

1. Welke persoonsgegevens verwerkt Nippon Express door middel van ID-scanners?
2. Wat is de grondslag voor deze verwerking?

[1] Nippon Express (Nederland) B.V., vestigingsadres: Cessnalaan 24, 1119 NL Schiphol-Rijk. Webadres: http://nipponexpress.com, KvK inschrijfnummer: 34047815
[2] e2013-00299, e2013-002297, t2014-00176, e2014-00561, t2015-00255
[3] In 2014 ontving het College bescherming persoonsgegevens (CBP) tien signalen van chauffeurs die hierover klaagden.
[4] Sinds 1 januari 2016 wordt het CBP in het maatschappelijk verkeer aangeduid als: Autoriteit Persoonsgegevens.

3. Verwerkt Nippon Express in strijd met het verwerkingsverbod van artikel 16 Wbp bijzondere persoonsgegevens?
4. Verwerkt Nippon Express in strijd met artikel 24 Wbp het burgerservicenummer (BSN)?
5. Heeft Nippon Express voor de toegang tot (bijzondere) persoonsgegevens via internet (*webbased*) passende organisatorische en technische maatregelen getroffen zoals bepaald in artikel 13 Wet bescherming persoonsgegevens (Wbp)?
6. Bewaart Nippon Express de gescande persoonsgegevens langer dan noodzakelijk in de zin van artikel 10, lid 1 Wbp?

Het onderzoek richt zich aldus op toetsing van de artikelen 1, onder a, van de Wbp (definitie persoonsgegeven), artikel 1, onder b, van de Wbp (definitie verwerking van persoonsgegevens), artikel 1, onder d, van de Wbp (definitie verantwoordelijke), artikel 8 (grondslag), artikel 10, lid 1, Wbp (bewaartermijn), artikel 13 Wbp (beveiliging van persoonsgegevens), artikel 16 juncto artikel 18 Wbp (bijzondere persoonsgegevens omtrent iemands ras) en artikel 24 Wbp (beperking gebruik wettelijk identificatienummer).

De doelstelling van dit ambtshalve onderzoek is om aan de hand van de onderzoeksvragen te controleren of de verantwoordelijke persoonsgegevens verwerkt in overeenstemming met de Wbp.

1.3 Procedure

De Autoriteit Persoonsgegevens heeft Nippon Express bij brief van 21 januari 2016 geïnformeerd over het ambtshalve onderzoek naar de verwerking van persoonsgegevens. In dezelfde brief heeft de Autoriteit Persoonsgegevens een onderzoek ter plaatse aangekondigd.

De Autoriteit Persoonsgegevens heeft het onderzoek ter plaatse op het vestigingsadres van Nippon Express (Nederland) B.V. uitgevoerd op 3 februari 2016. Tijdens het onderzoek ter plaatse is een aantal documenten alsmede aanvullende informatie opgevraagd. Op 8 februari 2016 ontving de Autoriteit Persoonsgegevens een deel van de gevraagde informatie. Bij brief van 11 februari 2016 heeft de Autoriteit Persoonsgegevens de openstaande vragen en nog te ontvangen informatie onder de aandacht gebracht bij Nippon Express en een reactie gevraagd. Op dinsdag 22 februari 2016 heeft de Autoriteit Persoonsgegevens telefonisch contact met Nippon Express gehad. Tijdens dit gesprek heeft Nippon Express aangegeven de openstaande vragen in de loop van die week te zullen beantwoorden. Bij brief van 1 maart 2016 heeft de Autoriteit Persoonsgegevens het verzoek van 22 februari 2016 herhaald. Op 7 maart 2016 ontving de Autoriteit Persoonsgegevens de gevraagde informatie en het antwoord op de openstaande vragen. Bij brief van 29 juni 2016 verzocht de Autoriteit Persoonsgegevens aan Nippon Express nog enkele vragen te beantwoorden. Nippon Express beantwoordde deze op 4 juli 2016 per e-mail.

Bij brief van 2 december 2016 deed de Autoriteit Persoonsgegevens aan Nippon Express het rapport voorlopige bevindingen toekomen, waarbij het bedrijf in de gelegenheid werd gesteld zijn zienswijze op de bevindingen te geven. Op 29 december 2016 verzocht Nippon Express (Nederland) om uitstel van de reactietermijn op de zienswijze. Bij brief van 29 december 2016 verleende de Autoriteit Persoonsgegevens uitstel tot en met 12 januari 2017.

Op 12 januari 2017 ontving de Autoriteit Persoonsgegevens de zienswijze op de voorlopige bevindingen. Op 21 februari 2017 heeft de Autoriteit Persoonsgegevens Nippon Express in de gelegenheid gesteld om een aanvulling op zijn zienswijze te geven. Op 8 maart 2017 verzocht Nippon Express om uitstel van de reactietermijn op laatstgenoemde brief. Bij brief van 8 maart 2017 verleende de Autoriteit

Persoonsgegevens uitstel tot en met 22 maart 2017. Bij e-mail van 20 maart 2017 ontving de Autoriteit Persoonsgegevens de gevraagde toelichting.

2. Uitwerking van het wettelijk kader

2.1 Verantwoordelijke

Op grond van artikel 1, onder d, Wbp is de verantwoordelijke: *de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.*

De wetsgeschiedenis geeft hierover aan: "*Het begrip 'verantwoordelijke' knoopt in eerste instantie aan bij de vaststelling van het doel van de verwerking. De vraag is wie uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerking, van welke persoonsgegevens en voor welk doel. Tevens is van belang wie beslist over de middelen voor die verwerking: de vraag op welke wijze de gegevensverwerking zal plaatsvinden.* […] *Bij de beantwoording van de vraag wie de verantwoordelijke is, dient enerzijds te worden uitgegaan van de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen, anderzijds – in aanvulling daarop – van een functionele inhoud van het begrip.*"[5]

2.2 Persoonsgegevens

Volgens artikel 1, aanhef en onder a, van de Wbp wordt onder een 'persoonsgegeven' verstaan: "*elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.*"

De definitie bevat een aantal elementen die expliciet aandacht vragen. Allereerst moet het gaan om informatie 'betreffende' een natuurlijke persoon ('any information relating to'). Voorts moet deze persoon zijn geïdentificeerd of althans identificeerbaar zijn ('identified or identifiable'). Als er aan één van beide elementen niet is voldaan, dan is er geen sprake van persoonsgegevens en is de wet niet van toepassing. Hoewel het gaat om twee onderscheiden beoordelingsmomenten, staan zij niet los van elkaar.[6]

2.3 Verwerking van persoonsgegevens

Verwerking van persoonsgegevens is gedefinieerd in artikel 1, aanhef en onder b, van de Wbp en omvat: "*elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.*"

Het object van regeling is de verwerking van persoonsgegevens. Het is conform de richtlijn gedefinieerd als elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, uitwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.[7]

[5] Kamerstukken II 1997/98, 25 892, nr. 3, p. 55.
[6] Kamerstukken II 1997/98, 25 892, nr. 3, p. 46.
[7] Kamerstukken II 1997/98, 25 892, nr. 3, p. 50.

2.4 Grondslag van een verwerking

Artikel 8 Wbp bepaalt: "*Persoonsgegevens mogen slechts worden verwerkt indien:*
a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert."

Artikel 8 bevat een limitatieve opsomming van de gronden die een gegevensverwerking rechtvaardigen.[8]

Artikel 8, onder a, Wbp vereist dat de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend. De toestemming dient een vrije, specifieke en op informatie berustende wilsuiting te zijn, waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.[9] Een "toestemming" kan alleen rechtsgeldig zijn als de betrokkene een werkelijke keuze heeft en er geen sprake is van bedrog, intimidatie of dwang en de betrokkene ook niet het risico van aanzienlijke negatieve gevolgen loopt wanneer hij niet toestemt. Wanneer de gevolgen van toestemming de keuzevrijheid van de betrokkene beperken, kan er geen sprake zijn "vrije" toestemming.[10]

Artikel 8, onder b, Wbp bepaalt dat een gegevensverwerking toelaatbaar is indien deze noodzakelijk is om contractuele verplichtingen na te komen. Daarbij geldt als voorwaarde dat de betrokkene partij is bij de desbetreffende overeenkomst. Tevens is een gegevensverwerking geoorloofd indien deze noodzakelijk is in de precontractuele fase.[11]

Artikel 8, onder c, Wbp bepaalt dat de verantwoordelijke gerechtigd is gegevens te verwerken indien dit noodzakelijk is ter uitvoering van een wettelijke verplichting die op hem rust.[12]

Artikel 8, onder d, Wbp bepaalt dat er een geldige verwerkingsgrond is indien er een dringende medische noodzaak is om de gegevens van de betrokkene te verwerken. Het moet gaan om een zaak van leven of dood.[13]

[8] Kamerstukken II 1997/98, 25 892, nr. 3, p. 80.
[9] Kamerstukken II 1997/98, 25 892, nr. 3, p. 80 en artikel 1, onder i, Wbp.
[10] Opinie WP29 15-2011, p.14, 15.
[11] Kamerstukken II 1997/98, 25 892, nr. 3, p. 80, 81.
[12] Kamerstukken II 1997/98, 25 892, nr. 3, p. 82.
[13] Kamerstukken II 1997/98, 25 892, nr. 3, p. 83, 84.

Artikel 8, onder e, maakt gegevensverwerking mogelijk voor zover deze noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het betreffende bestuursorgaan dan wel het bestuursorgaan aan wie de gegevens worden verstrekt.[14] Daarmee is deze grondslag alleen van toepassing op de publieke sector.

Artikel 8, onder f, Wbp schrijft voor dat de gegevensverwerking noodzakelijk moet zijn voor de behartiging van het gerechtvaardigd belang van de verantwoordelijke. Uit deze bepaling vloeien de volgende drie voorwaarden voort:
- gerechtvaardigd belang;
- noodzakelijkheidseis, waaronder proportionaliteit en subsidiariteit, en
- het belang van de verantwoordelijke prevaleert boven het belang of de fundamentele rechten en vrijheden van de betrokkene, in dit geval een vrachtwagenchauffeur.

Een gerechtvaardigd belang van de verantwoordelijke kan aanwezig worden geacht in het geval dat de betreffende verwerking noodzakelijk is om zijn reguliere bedrijfsactiviteiten te verrichten.[15] Ook ten aanzien van gegevensverwerkingen die weliswaar geen onderdeel uitmaken van de reguliere bedrijfs-activiteiten van de verantwoordelijke maar deze wel in wezenlijke zin ondersteunen, kan in de regel worden aangenomen dat de verantwoordelijke een gerechtvaardigd belang heeft. Als voorbeeld kan worden genoemd de gegevensverwerking in het bedrijf in het kader van fraudebestrijding.[16]

Voor een geslaagd beroep op de grondslag gerechtvaardigd belang is voorts vereist dat de gegevensverwerking noodzakelijk voor het gerechtvaardigd belang moet worden beschouwd. Kan het belang van de verantwoordelijke anderszins of met minder ingrijpende middelen worden gediend, dan is de voorgenomen gegevensverwerking niet toegestaan.[17]

De derde voorwaarde voor een geslaagd beroep op een gerechtvaardigd belang behelst een nadere afweging, waarbij de belangen van de betrokkene een zelfstandig gewicht in de schaal leggen tegenover het belang van de verantwoordelijke.[18]

2.5 Bewaartermijn

Artikel 10 lid 1 Wbp bepaalt: "*Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.*"

Persoonsgegevens mogen niet langer dan noodzakelijk worden bewaard. De Wbp[19] kent geen afzonderlijke regels voor de bewaring van gegevens. De verantwoordelijke dient zich af te vragen of er redenen zijn op grond waarvan gegevens vastgelegd kunnen blijven. Zijn er voldoende redenen dan kan hij bepalen welke termijnen gelden om die gegevens te bewaren. Zijn die termijnen verlopen dan zal hij de gegevens niet

[14] Kamerstukken II 1997/98, 25 892, nr. 3, p. 84.
[15] Kamerstukken II 1997/98, 25 892, nr. 3, p. 86.
[16] Kamerstukken II 1997/98, 25 892, nr. 3, p. 87.
[17] Kamerstukken II 1997/98, 25 892, nr. 3, p. 87.
[18] Kamerstukken II 1997/98, 25 892, nr. 3, p. 87.
[19] De Memorie van Toelichting spreekt hier van de Wet Persoonsregistraties (WPR). Dezelfde redenering geldt voor de opvolger van de WPR, de Wbp.

meer mogen verwerken, tenzij voor een ander, daarmee verenigbaar doel, bij voorbeeld statische archivering.[20]

2.6 Beveiliging

Artikel 13 Wbp bepaalt: "*De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.*"

In het begrip 'passende' ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip 'passend' duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naarmate bij voorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekent, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Er moet sprake zijn van een adequate beveiliging.[21]

De richtsnoeren 'Beveiliging van persoonsgegevens'[22] vormen "*de verbindende schakel tussen enerzijds het juridisch domein, met daarbinnen de eisen uit de Wbp, en anderzijds het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen.*

Dat betekent dat de richtsnoeren in samenhang moeten worden gebruikt met algemeen geaccepteerde beveiligings-standaarden binnen de praktijk van de informatiebeveiliging, zoals de Code voor Informatiebeveiliging of de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum."[23]

Om te beoordelen wat een passende mate van beveiliging is , wordt hieronder een overzicht gegeven hoe het begrip 'passend' wordt ingevuld binnen de praktijk van de informatiebeveiliging.

Eén van de algemeen geaccepteerde beveiligingsstandaarden is de veel gebruikte Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2007 nl).[24] Hierin staat:

"*Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.*"[25]
en
"*Waar krachtige authenticatie en verificatie van de identiteit nodig zijn, behoren andere authenticatiemethoden dan wachtwoorden te worden gebruikt, zoals cryptografische hulpmiddelen, smartcards, 'tokens' of biometrische hulpmiddelen. De sterkte van de gebruikersidentificatie en authenticatie behoort geschikt te zijn voor de gevoeligheid van de informatie waartoe toegang wordt verleend.*"[26] (Onderstreping toegevoegd door de Autoriteit Persoonsgegevens.)

20 Kamerstukken II 1997/98, 25 892, nr. 3, p. 95.
[21] Kamerstukken II 1997/98, 25 892, nr. 3, p. 98-99
[22] Deze richtsnoeren zijn uitgebracht door het College Bescherming Persoonsgegevens, de voorloper van de Autoriteit Persoonsgegevens, en te vinden op webadres: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf
[23] Richtsnoeren Beveiliging van persoonsgegevens, p. 2.
[24] Deze standaard is verkrijgbaar bij NEN (http://www.nen.nl/).
[25] NEN-ISO/IEC 27002:2007 nl, p. 76. Deze norm is recentelijk aangescherpt (NEN-ISO 27002:2017)
[26] NEN-ISO/IEC 27002:2007 nl, p. 80. Deze norm is recentelijk aangescherpt (NEN-ISO 27002:2017)

Hieruit volgt dat naarmate de gegevens een gevoeliger karakter hebben, worden zwaardere eisen gesteld aan de authenticatiemethoden.

Andere beveiligingsstandaarden onderschrijven dit. Volgens ICT-Beveiligingsrichtlijnen voor webapplicaties Deel 2, van het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Veiligheid en Justitie, geldt de volgende beveiligingsrichtlijn ten aanzien van toegangsbeveiliging[27]:

"*Welk authenticatiemechanisme moet worden toegepast om een webapplicatie te beschermen moet zijn gebaseerd op een risicoanalyse (classificatie van informatie),* […]." In het algemeen geldt dat hoe groter de gevoeligheid van de informatie is, des te hoger de eisen zijn die worden gesteld aan authenticatie.

Authenticatie is gebaseerd op verschillende 'factoren'. Een factor beschrijft op welke manier een gebruiker zich moet authenticeren. Dat kan op basis van iets dat de gebruiker weet (bijvoorbeeld een wachtwoord of pincode), iets dat de gebruiker heeft (bijvoorbeeld een token of smartcard), of iets dat de gebruiker 'is' (bijvoorbeeld een vingerafdruk).[28]

Om de kans op het omzeilen van het authenticatiemechanisme te voorkomen, wordt het in de praktijk als passend geaccepteerd om minimaal twee verschillende factoren te combineren.[29] Hieronder volgen drie voorbeelden uit andere landen en sectoren van gangbare beveiligingsstandaarden waarin meerfactor–authenticatie is uitgewerkt.

1. Het National Institute of Standards and Technology (NIST) is een Amerikaanse wetenschappelijke instelling die onder de federale overheid van de Verenigde Staten valt. Recentelijk publiceerde dit instituut een richtlijn over digitale authenticatie.[30] Ook het NIST stelt voor gevoelige gegevens meerfactor–authenticatie verplicht.[31]

2. Voor de gezondheidszorg, waar veel met bijzondere persoonsgegevens wordt gewerkt, gelden de *best practices* van NEN-7510. NEN-7510 geeft aanwijzingen voor het toepassen van de Code voor informatiebeveiliging ISO/IEC 27002 in de gezondheidszorg. [32] Deze norm stelt de volgende eis: "*Informatiesystemen, die patiëntgegevens verwerken, behoren authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken.*"[33]

[27] Deel 2, januari 2012, p. 33, webadres: https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties/6/ICT+Beveiligingsrichtlijnen+voor+Webapplicaties+++oude+versie+2012.pdf. De laatste versie is te vinden op webadres: https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties/3/ICT%2BBeveiligingsrichtlijnen%2Bvoor%2BWebapplicaties%2B%2B%2BVerdieping%2B%2B%2BLeesversie.pdf
[28] Deel 2, januari 2012, p. 33, webadres: https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties/6/ICT+Beveiligingsrichtlijnen+voor+Webapplicaties+++oude+versie+2012.pdf. Zie ook: ICT-Beveiligingsrichtlijnen voor webapplicaties Verdieping, versie 2015, p. 35. Webadres: https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties/3/ICT%2BBeveiligingsrichtlijnen%2Bvoor%2BWebapplicaties%2B%2B%2BVerdieping%2B%2B%2BLeesversie.pdf
[29] Idem.
[30] Webadres: https://pages.nist.gov/800-63-3/sp800-63b.html
[31] Webadres: https://pages.nist.gov/800-63-3/sp800-63b.html, zie hoofdstuk 4.
[32] De AP merkt op dat de NEN-7510 is bijgewerkt in NEN-ISO/IEC 27799:2016.
[33] NEN-7510 (2011), p. 98.

3. Ook bij de overheid geldt bij gevoelige gegevens meerfactorauthenticatie. In 'Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten'[34] worden de verschillende niveaus van authenticatie uitgewerkt. Hierin wordt gesteld dat de verwerking van bijzonder persoonsgegevens een verwerking van persoonsgegevens in risicoklasse II of III betreft.[35] Hiervoor is tenminste een betrouwbaarheidsniveau 3 vereist. Dit betrouwbaarheidsniveau vereist "*striktere methoden voor de verificatie van de geclaimde identiteit van de gebruiker. Deze moeten een hoge mate van zekerheid bieden.* […] *Als type middel is 2-factor authenticatie vereist. Voorbeelden daarvan zijn 'soft' certificaten of 'one-time-password'-tokens.*"[36]

Uit de bovengenoemde algemeen geaccepteerde beveiligingsstandaarden vloeit voort dat ten aanzien van authenticatie bij de toegang tot applicaties die specifiek zijn gericht op het verwerken van gevoelige informatie en waarbij toegang wordt verschaft via het internet, de verantwoordelijke tenminste gebruik dient te maken van meerfactorauthenticatie.

Serverconfiguratie

Bij de serverconfiguratie geldt eveneens dat er de beveiliging 'passend' moet zijn, dat wil zeggen in overeenstemming is met de stand van de techniek. Evenals in de vorige paragraaf dient te worden aangesloten bij algemeen aanvaarde beveiligingsstandaarden. Volgens twee van dergelijke standaarden, de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van het NCSC, en de 'National Vulnerability Database' van het National Institute of Standards and Technology, zijn zowel protocol SSLv3 als versleutelingsmethoden RC4-SHA en RC4-MD5 verouderde en daarom onveilige technieken.

2.7 Bijzondere persoonsgegevens

Artikel 16 Wbp bepaalt: *"De verwerking van persoonsgegevens betreffende iemands* […] *ras* […] *is verboden behoudens het bepaalde in deze paragraaf.* […]*"*

In de wetsgeschiedenis is aangegeven dat het begrip 'ras' dezelfde betekenis heeft als in artikel 1 van de Grondwet en mede in het licht moet worden gezien van het Internationaal Verdrag inzake de uitbanning van alle vormen van rassendiscriminatie. *"Het begrip moet ruim worden opgevat en omvat ook huidskleur, afkomst en nationale of etnische afstamming".*[37]

Uitzonderingsgrond verwerking persoonsgegevens betreffende iemands ras

Artikel 18 Wbp bepaalt: *"Het verbod om persoonsgegevens betreffende iemands ras te verwerken als bedoeld in artikel 16, is niet van toepassing indien de verwerking geschiedt:*
a. met het oog op de identificatie van de betrokkene en slechts voor zover dit voor dit doel onvermijdelijk is;
b. met het doel personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen ten einde feitelijke nadelen verband houdende met de grond ras op te heffen of te verminderen en slechts indien:
1°. dit voor dat doel noodzakelijk is;
2°. de gegevens slechts betrekking hebben op het geboorteland van de betrokkene, van diens ouders of grootouders, dan wel op andere, bij wet vastgestelde criteria, op grond waarvan op objectieve wijze vastgesteld kan worden of iemand tot een minderheidsgroep als bedoeld in de aanhef van onderdeel b behoort, en
3°. de betrokkene daartegen geen schriftelijk bezwaar heeft gemaakt."

[34] Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, Forum Standaardisatie2014, versie 3. Webadres: https://www.forumstandaardisatie.nl/sites/default/files/atoms/files/HR-Betrouwbaarheidsniveaus-v3-2014.pdf
[35] Idem, p. 22 en 27.
[36] Idem, p. 22.
[37] Kamerstukken II 1997/98, 25 892, nr. 3, p. 104.

Verwerking van persoonsgegevens betreffende iemands ras dient slechts in zeer uitzonderlijke gevallen te worden toegestaan. Hiertoe wordt in beginsel slechts de mogelijkheid gecreëerd indien het de verwerking van gegevens omtrent ras voor identificatiedoeleinden betreft, dan wel in het kader van een voorkeursbeleid ten aanzien van bepaalde minderheidsgroeperingen. In beginsel is er alleen in die gevallen een zwaarwegend algemeen belang in de zin van artikel 8, vierde lid, van de richtlijn, dat verwerking van dergelijke gegevens kan rechtvaardigen.[38]

Verwerking van beeldmateriaal en bijzondere persoonsgegevens
Het verwerken van beeldmateriaal kan een verwerking van bijzondere persoonsgegevens inhouden, bijvoorbeeld omdat het ras of de gezondheid van de persoon is af te leiden uit het beeldmateriaal.

De Autoriteit Persoonsgegevens merkt beeldmateriaal niet aan als een bijzonder persoonsgegeven in de zin van artikel 16 Wbp als:

- het doeleinde van de verwerking niet gericht is op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven;
- het voor de verantwoordelijke redelijkerwijs niet voorzienbaar is dat de verwerking zal leiden tot het maken van onderscheid; en
- de verwerking van die bijzondere persoonsgegevens onvermijdelijk is bij die verwerking.

In de wetsgeschiedenis wordt opgemerkt dat met hantering van de term 'onvermijdelijk' een aanscherping is beoogd van het noodzakelijkheidscriterium.[39]

Indien de verwerking van beeldmateriaal echter identificatie tot doel heeft, wordt dit beeldmateriaal wel als een rasgegeven aangemerkt.[40]

2.8 Gebruik wettelijk identificatienummer

Artikel 24, eerste lid, Wbp bepaalt: "*Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.*"

In de wetsgeschiedenis van dit artikel is het volgende aangegeven: "*De bepaling is ontstaan vanuit de gedachte dat een persoonsidentificerend nummer een persoonsgegeven is: het is een gegeven waarmee een individuele natuurlijke persoon kan worden geïdentificeerd. Uit een oogpunt van bescherming van de persoonlijke levenssfeer werd het noodzakelijk geacht om aan het gebruik van dergelijke nummers beperkingen te stellen. Vast staat immers dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen.* [...] *De voorgestelde bepaling laat in de eerste plaats toe dat een wettelijk voorgeschreven persoonsnummer wordt verwerkt ter uitvoering van de wet waarin het voorschrift over het nummer is opgenomen. De praktijk leert evenwel dat dergelijke nummers ook voor andere doeleinden worden verwerkt. Onder omstandigheden is dit gerechtvaardigd, in andere gevallen echter niet. Algemene randvoorwaarde is dat*

[38] Kamerstukken II 1997/98, 25 892, nr. 3, p. 104.
[39] Kamerstukken II 1997/98, 25 892, nr. 3, p. 105.
[40] Beleidsregels Cameratoezicht, p. 26,
webadres: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf

persoonsgegevens niet worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (artikel 9). Uiteraard geldt dit ook voor persoonsnummers. Omdat het gebruik van persoonsnummers – zoals hierboven beschreven – extra risico's met zich mee kan brengen voor de bescherming van de persoonlijke levenssfeer, wordt in het onderhavige artikel daarenboven bepaald dat de uitvoering van de betreffende wet alleen mogelijk is voor zover dat bij wet is bepaald. Aldus is een afweging op het niveau van de formele wet in beginsel gegarandeerd."[41]

"*Ook het sofi-nummer is uiteraard een wettelijk voorgeschreven nummer als hier bedoeld."*[42]

"*Omdat het gebruik van persoonsnummers - zoals hiervoor beschreven - extra risico's met zich kan brengen voor de bescherming van de persoonlijke levenssfeer, wordt in het onderhavige artikel daarenboven bepaald dat verwerking van persoonsnummers voor andere doeleinden dan de uitvoering van de betreffende wet alleen mogelijk is voor zover dat bij de wet is bepaald. Aldus is een afweging op het niveau van de formele wet in beginsel gegarandeerd. Daarbij is er voor gekozen om op dit punt geen delegatie door de formele wetgever toe te staan. Eventuele andere gebruiksdoeleinden dienen derhalve door de formele wetgever zelf te worden vastgesteld."*[43]

[41] Kamerstukken II 1997/98, 25 892, nr. 3, p. 127 ev.
[42] Idem, p. 128.
[43] Idem, p. 128.

3. Feiten

3.1 Inleiding

Nippon Express is logistiek dienstverlener en houdt zich onder meer bezig met transport, overslag, opslag en distributie. Nippon Express had in 2014 een omzet van € 145 miljoen.

Dagelijks komen ongeveer 250 vrachtwagenchauffeurs uitgaande vracht ophalen bij Nippon Express. De vrachtwagenchauffeurs komen uit heel Europa. Om met zekerheid de juiste lading aan de juiste chauffeur mee te geven, controleert en scant Nippon Express de identiteitsdocumenten van de chauffeurs. Deze procedure is verplicht. Indien de chauffeur dit weigert of op andere wijze geen medewerking verleent, dan wordt het laadproces beëindigd.[44]

Op het kantoor van Nippon Express wordt de chauffeur gevraagd om zich te identificeren met een geldig identiteitsdocument. Op een formulier registreert Nippon Express onder andere zijn naam, het kenteken van de vrachtwagen en de laadreferentie. Vervolgens wordt zijn identiteitsdocument, dat wil zeggen voor Nederlandse chauffeurs het paspoort, de identiteitskaart of het rijbewijs, gescand. Bij buitenlandse chauffeurs controleert en scant Nippon Express het paspoort of de identiteitskaart.

Het personeel op het kantoor van Nippon Express controleert aan de balie of de chauffeur lijkt op de persoon op de foto op het identiteitsdocument. Ook wordt de chauffeur gecontroleerd op leeftijd, lengte en handtekening. Verder wordt het document gecontroleerd op zichtbare onregelmatigheden. Het personeel maakt vervolgens een scan van het identiteitsdocument.

Bij het scannen van het identiteitsdocument gebruikt Nippon Express apparatuur van [naam leverancier B.V.] (hierna: [naam leverancier]). Een medewerker van Nippon Express legt het identiteitsdocument onder het scanapparaat dat beheerd wordt door [naam leverancier]. Met de technologie van [naam leverancier] controleert Nippon Express een aantal echtheidskenmerken van de identiteitsdocumenten. Zo vergelijkt het systeem de houdergegevens op de houderpagina van het paspoort met de gegevens in de Machine Readable Zone (MRZ) onderaan de houderpagina. Deze controle vindt in de meeste gevallen geautomatiseerd plaats, maar soms handmatig. Het systeem geeft als reactie: 'ok', of 'niet ok'. Bij 'ok' wordt een groene vink over de afbeelding van het identiteitsdocument geplaatst. Bij 'niet ok' een rood kruis.

Als het personeel van Nippon Express twijfels heeft over de identiteit van de bestuurder (bijvoorbeeld na controlevragen) of het systeem geeft als reactie 'niet ok', dan neemt het personeel van Nippon Express contact op met de Expert Helpdesk van [naam leverancier]. Een medewerker van deze Helpdesk controleert het gescande document dan handmatig. Ook dit resulteert in 'ok' of 'niet ok'. Bij 'niet ok' zendt [naam leverancier] het gescande document langs elektronische weg naar de Koninklijke Marechaussee (KMAR), bureau falsificaties. De KMAR onderzoekt het document en koppelt het resultaat terug aan [naam leverancier]. [Naam leverancier] meldt aan Nippon Express of het ID 'ok' of 'niet ok' is. Bij 'niet ok' schakelt Nippon Express de politie in. Dit heeft sinds de invoering van het scansysteem, ongeveer vijf jaar geleden, volgens Nippon Express drie keer geleid tot een aanhouding.

[44] Intern document Nippon Express: WI-Security-002-General Loading procedure (GENERAL) version: 6, p. 2.

3.2 Verantwoordelijke

Tijdens het onderzoek ter plaatse deelde Nippon Express aan de Autoriteit Persoonsgegevens mede dat zijzelf de verantwoordelijke is voor de verwerking met de [naam leverancier] documentscanner, omdat Nippon Express het doel en de middelen van de verwerkingen bepaalt, te weten echtheidscontrole van de identiteitsdocumenten om vast te stellen dat Nippon Express de vracht aan de juiste chauffeur meegeeft. Volgens Nippon Express is [naam leverancier] een bewerker.

Daarnaast heeft de Autoriteit Persoonsgegevens tijdens het onderzoek ter plaatse vastgesteld dat Nippon Express in de instellingen van de [naam leverancier] software de te scannen persoonsgegevens kan (laten) aan- of uitzetten. In de ochtend kondigde Nippon Express aan dat hij zojuist had besloten dat hij de BSN's in de houderinformatie niet meer wilde uitlezen. In de middag constateerde de Autoriteit Persoonsgegevens dat het BSN inderdaad niet meer op het beeldscherm te zien was, en dat de eerder uitgelezen BSN's ook niet meer zichtbaar waren.[45]

Nippon Express heeft de verwerking met de [naam leverancier] documentscan gemeld bij (de voorloper van) de Autoriteit Persoonsgegevens.[46] Nippon Express heeft zich in deze melding als verantwoordelijke voor de verwerking gesteld.

3.3 Persoonsgegevens

De scanapparatuur en -software lezen onder meer de MRZ uit en de chip die in het identiteitsdocument zit. De MRZ is een strook op het identiteitsdocument met onder andere letter- en cijfertekens die geautomatiseerd kunnen worden uitgelezen.[47] Niet alle identiteitsdocumenten hebben een MRZ.[48]

Figuur 1: De MRZ is de groen gemarkeerde regel onderaan (doorhalingen Autoriteit Persoonsgegevens).

[45] Het gaat hier om de BSN's in de houderinformatie op het identiteitsdocument. Het BSN in de MRZ wordt echter nog wel verwerkt. Overigens heeft de Autoriteit Persoonsgegevens de verwijdering alleen geverifieerd op het beeldscherm, en niet gecontroleerd in bijvoorbeeld de backup.

[46] Meldingsnummer: m1457126

[47] Zie bijvoorbeeld Werkgroep Identificatie (2010, pp 21-22). "*De MRZ bestaat uit twee of drie regels met de letters van het alfabet en de cijfers van 0 tot 9. Spaties worden weergegeven met het teken <. De letters en cijfers van de MRZ in alle documenten zijn van exact hetzelfde type. In de MRZ wordt een aantal persoons- en documentgegevens herhaald (naam, nummer e.d).*" Webadres: https://zoek.officielebekendmakingen.nl/blg-79109.pdf (laatst bezocht 11 februari 2015). Overigens kan de [naam leverancier] scanner middels Optical Character Recognition ook de gegevens van de houder van het paspoort uitlezen, ondanks dat dit niet van het genoemde lettertype is.

[48] Vanaf 1 oktober 2006 geeft de Rijksdienst voor het wegverkeer rijbewijzen uit in creditcard formaat. Deze bevatten een barcode. Sinds 19 januari 2013 zitten er in nieuwe uitgegeven rijbewijzen naast een barcode ook een verkorte MRZ, waarin geen BSN is opgenomen. Vanaf 14 november 2014 bevat het rijbewijs een MRZ, een Quick Response (QR)-code en een RFID-chip. Op de RFID-chip staan de houdergegevens en het BSN in aparte datagroepen, respectievelijk DG1 en DG11. Bron: RDW.

De chip in het identiteitsdocument wordt uitgelezen door middel van Radio Frequency Identification (RFID). RFID is een draadloze techniek waarmee elektronisch opgeslagen gegevens, zoals een BSN nummer of een pasfoto, uit een RFID-tag gelezen kunnen worden. (Een RFID-tag bestaat uit een kleine chip en een antenne.) Niet alle identiteitsdocumenten hebben een RFID-tag.[49]

Bij de scan worden de volgende gegevens verwerkt:[50]

- type identiteitsdocument (MRZ- en houderinformatie)
- land van uitgifte identiteitsdocument (MRZ)
- naam en voornamen van de houder (MRZ- en houderinformatie)
- nummer identiteitsdocument (MRZ- en houderinformatie)
- nationaliteit (MRZ- en houderinformatie)
- geboortedatum (MRZ- en houderinformatie)
- geslacht (MRZ- en houderinformatie)
- verloopdatum van het document (MRZ- en houderinformatie)
- pasfoto in zwart-wit (houderinformatie)
- pasfoto in kleur en in hoge resolutie (RFID)[51]
- burgerservicenummer (MRZ)

Gewijzigd feit na de voorlopige bevindingen

In zijn reactie op de voorlopige bevindingen, verklaarde Nippon Express bij brief van 12 januari 2017 de werkwijze te hebben aangepast:

"[…] *het BSN nummer* [wordt] *niet meer door ons verwerkt. Het [naam leverancier] systeem wordt gebruikt voor het bepalen van de echtheid van het aangeboden ID document. Wij accepteren van de Nederlandse chauffeurs uitsluitend het rijbewijs. Bij het scannen wordt het BSN nummer afgeplakt waardoor deze geen onderdeel meer is van het gescande document. Het rijbewijs heeft geen MRZ code waardoor ook hier geen BSN nummer meer herleidbaar is. Er vindt dus geen enkele verwerking meer plaats van het BSN nummer.*"

3.4 Verwerking van persoonsgegevens

[Naam leverancier] controleert de identiteitsdocumenten aan de voorzijde, de achterzijde en op de tussenlagen van de pagina's van het identiteitsdocument. Er wordt gecontroleerd op type document, documentnummer, land van uitgifte, lettertype, beeld van de voor/achterkant, infrarood beeld (tussenlaag 1) en ultraviolet beeld (tussenlaag 2). Deze beelden worden na het scannen opgeslagen en bewaard. Ook wordt gecontroleerd of het document is verlopen of niet. Verder wordt de MRZ uitgelezen en met RFID datagroep 2 waarin de kleurenpasfoto in hoge resolutie staat. De MRZ bevat onder andere enkele controlegetallen waarmee nagegaan kan worden of er tekens zijn gewijzigd. Ook die controle wordt door [naam leverancier] uitgevoerd.[52]

Zoals gezegd is de MRZ een strook op het identiteitsdocument met een lettertype dat speciaal ontworpen is om geautomatiseerd te worden uitgelezen. Het proces is als volgt. Eerst maakt een scanner een digitale

[49] Vanaf 1 oktober 2006 geeft de Rijksdienst voor het wegverkeer rijbewijzen uit in creditcard formaat. Deze bevatten een barcode. Sinds 19 januari 2013 bevatten nieuwe uitgegeven rijbewijzen naast een barcode ook een MRZ. Vanaf 14 november 2014 bevat het rijbewijs een MRZ, een Quick Response (QR)-code en een RFID-chip. Op de RFID-chip staan de houdergegevens en het BSN in aparte datagroepen, respectievelijk DG1 en DG11. Bron: RDW.
[50] Vastgesteld door de AP tijdens het onderzoek ter plaatse.
[51] Paspoorten en identiteitskaarten: datagroep 2; rijbewijzen uitgegeven sinds 14 november 2014: in datagroep 6.
[52] Verklaard door Nippon Express tijdens onderzoek ter plaatse. Zie ook:

afbeelding van de MRZ. Vervolgens wordt de digitale afbeelding gelezen met zogenaamde Optical Character Recognition (OCR) software. Deze software zet de digitale afbeelding om in cijfers en letters (datastring). Vervolgens vinden er twee controles plaats. De eerste is een vergelijking tussen de MRZ en de algemene houdergegevens. De tweede controle is de verificatie van de controlegetallen in de MRZ. De MRZ bevat meerdere controlegetallen ('checksum digits'), die elk de uitkomst zijn van een rekenkundige formule gebaseerd op een deel van de gegevens in de MRZ.[53]

RFID is een draadloze techniek waarmee elektronisch opgeslagen gegevens gelezen kunnen worden, zoals een BSN of een pasfoto uit een RFID-tag. Nippon Express heeft verklaard dat de scanner alleen datagroep 2 van de RFID uitleest. Deze datagroep bevat de pasfoto in hoge resolutie en in kleur. Nippon Express leest niet datagroep 1 uit, die dezelfde gegevens als de MRZ bevat, waaronder het BSN.[54]

Gewijzigd feit na het conceptrapport met onderzoeksbevindingen

In zijn reactie op het conceptrapport met onderzoeksbevindingen, verklaarde Nippon Express bij brief van 12 januari 2017 de werkwijze te hebben aangepast:

"[…] *het BSN nummer* [wordt] *niet meer door ons verwerkt.* […] *Wij accepteren van de Nederlandse chauffeurs uitsluitend het rijbewijs. Bij het scannen wordt het BSN nummer afgeplakt waardoor deze geen onderdeel meer is van het gescande document.*

3.5 Grondslag van de verwerking

Nippon Express stelt dat een controle op echtheid van identiteitsdocumenten niet mogelijk is zonder gebruik van de [naam leverancier] scanner en diensten. De reden hiervoor is dat Nippon Express chauffeurs ontvangt van veel verschillende nationaliteiten. Van elk land zijn bovendien verschillende versies van paspoorten en identiteitskaarten in omloop.[55] Vanwege het grote aantal ID's is het voor Nippon Express niet mogelijk om aan de balie goed te kunnen controleren op de verschillende echtheids-kenmerken van de identiteitsdocumenten. Bovendien vindt Nippon Express dat hij niet in staat is om per land de ontwikkelingen op het gebied van identiteitsdocumenten te volgen.

De chauffeurs zijn verplicht om zich aan de controleprocedure te onderwerpen. Nippon Express controleert het kenteken, de vrachtwagen en het identiteitsdocument. Indien de chauffeur hieraan geen medewerking verleent, dan wordt het laadproces beëindigd.[56]

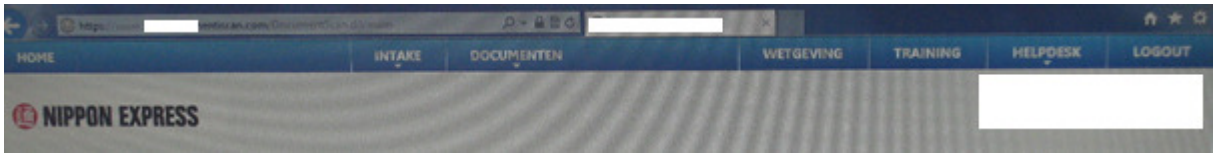
3.6 Bewaartermijn

De gescande documenten worden twintig dagen bewaard. Hierna worden de gegevens automatisch gewist. Tijdens het onderzoek ter plaatse stelde de Autoriteit Persoonsgegevens echter vast dat er in het systeem zeven dossiers stonden die na twintig dagen niet waren verwijderd. Het oudste dossier dateerde van medio 2013. Nippon Express gaf aan deze zeven dossiers handmatig te hebben verwijderd. In totaal stonden er ten tijde van het onderzoek ter plaatse 359 gescande identiteitsdocumenten van Nippon Express in het [naam leverancier] systeem.[57]

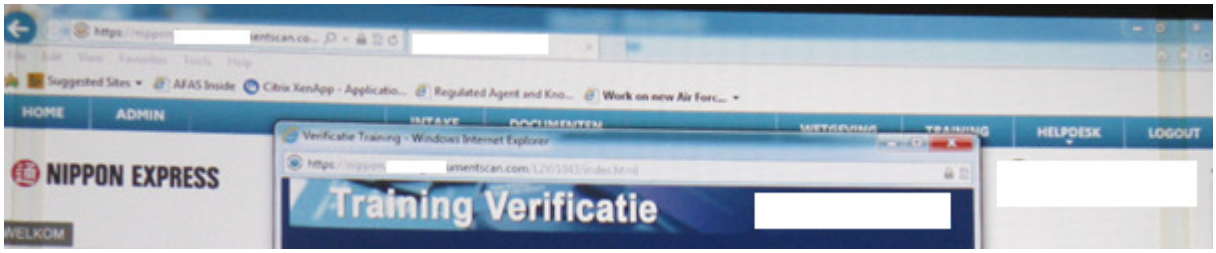
[53] ISO/IEC 7501-1:2008. Webadres: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45562
[54] Verklaring Nippon Express tijdens het onderzoek ter plaatse.
[55] Zie voor een idee van het grote aantal ID's dat in Europa in omloop is: webadres: http://www.edisontd.net/
[56] Intern document Nippon Express: WI-Security-002-General Loading procedure (GENERAL) version: 6, p. 2.
[57] Forensisch vastgelegd door de Autoriteit, afbeelding IMG_3001.

3.7 Beveiliging

Medewerkers van Nippon Express kunnen met de scanapparatuur van [naam leverancier] het controlesysteem van [naam leverancier] via het internet benaderen (afbeelding 1).[58] Tijdens het onderzoek ter plaatse is tevens toegang tot het systeem verkregen via het internet via een alternatief webadres (afbeelding 2).[59] Voorts verklaarde Nippon dat er geen toegangsbeperking op IP adres is als beveiligingsmaatregel om de toegang tot de persoonsgegevens te beperken.



Afbeelding 1. Screenshot (IMG_2997.jpg, 3 februari 2016, 14h10) met het webadres https://nippon.[naam leverancier]authentiscan.com, dat gebruikt wordt door de medewerkers van Nippon Express aan de balie.



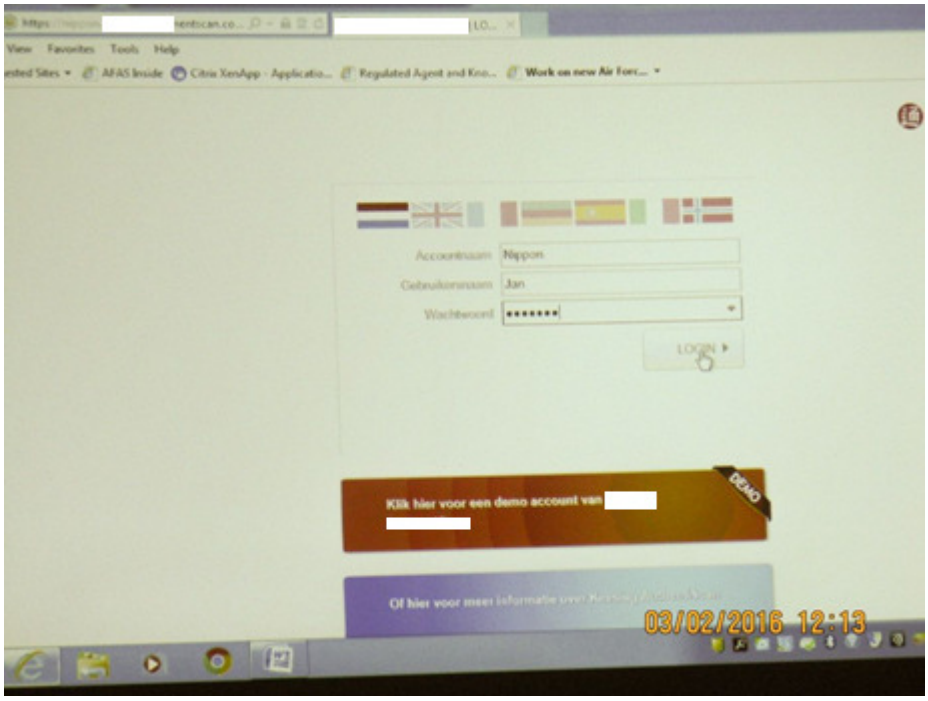
Afbeelding 2. Screenshot (IMG_2839.jpg, 3 februari 2016, 12h13) met het webadres https://nippon.[naam leverancier]documentscan.com, dat gebruikt werd tijdens het onderzoek ter plaatse.

De Autoriteit Persoonsgegevens heeft op 16 februari, 3 maart, 6 april 2016, 4 oktober 2016 en 1 juni 2017 de verbinding naar de webadressen (nippon.[naam leverancier]documentscan.nl en nippon.[naam leverancier]authentiscan.com) bekeken.[60] Op de vier onderzochte momenten constateerde de Autoriteit Persoonsgegevens dat de webadressen:
(1) voor iedereen bereikbaar zijn vanaf het internet
(2) gebruik maken van de cipher-methoden RC4-SHA en RC4-MD5
(3) gebruik maken van het protocol SSLv3[61]

De toegang vindt plaats met een accountnaam, een gebruikersnaam, en een wachtwoord.

De accountnaam is 'Nippon', de gebruikersnaam is de voornaam van een medewerker van Nippon Express.

[58] Webadres: https://nippon.[naam leverancier]authentiscan.com
[59] Webadres: https://nippon.[naam leverancier]documentscan.com
[60] Schermafdruk vastgelegd door de Autoriteit Persoonsgegevens op (onder meer) 1 juni 2017.
[61] Het testresultaat van internet.nl is toegankelijk via de permalink Webadressen: https://internet.nl/site/nippon.[naam leverancier]documentscan.com/19759, https://internet.nl/site/nippon.[naam leverancier]authentiscan.com/41370/.



Afbeelding 3. Screenshot (IMG_2836.jpg, 3 februari 2016, 12h13)

Gewijzigd feit na het conceptrapport met onderzoeksbevindingen

Nadat de Autoriteit Persoonsgegevens het conceptrapport met onderzoeksbevindingen aan Nippon Express stuurde, stelt de Autoriteit Persoonsgegevens vast dat Nippon Express de configuratie van de websites heeft aangepast. Nippon Express maakt niet langer gebruik van de cipher-methoden RC4-SHA en RC4-MD5 en het protocol SSLv3.

3.8 Gebruik wettelijk identificatienummer

Bij de controle met de [naam leverancier] scanapparatuur wordt de MRZ uitgelezen. Dit uitlezen gebeurt door Optical Character Recognition (OCR) software. Deze software zet de digitale afbeelding om in cijfers en letters (datastring). De MRZ van Nederlandse identiteitsdocumenten bevat de volgende gegevens: achternaam en voornamen, geboortedatum, de geldig-tot-datum, het documentnummer, en ook het burgerservicenummer (BSN). Naast genoemde gegevens bevat de MRZ onder andere een drietal controlegetallen, die elk de uitkomst zijn van een rekenkundige formule gebaseerd op de voorafgaande set cijfers en letters in de MRZ.[62] Door de controlegetallen is de MRZ volgens Nippon Express een belangrijk controlemiddel om de echtheid van identiteitsdocumenten vast te stellen.

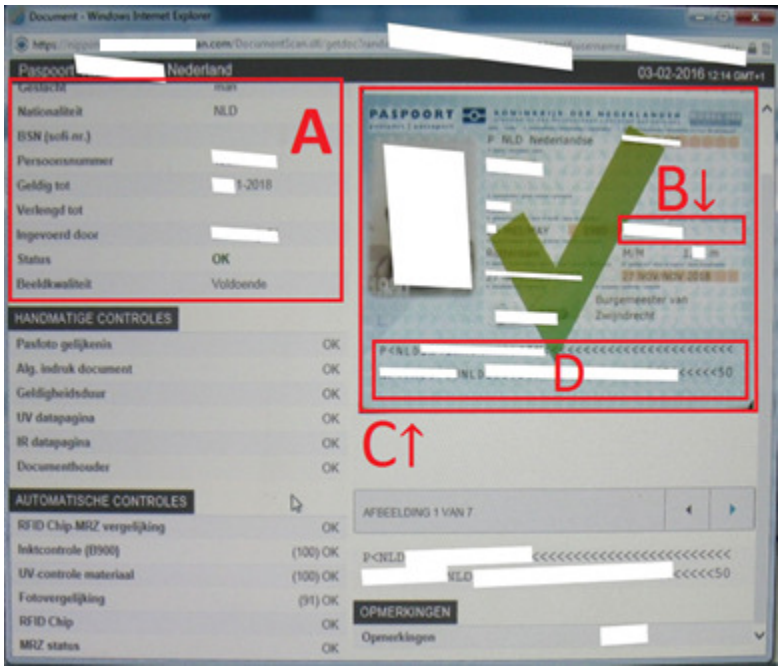
Als een chauffeur zijn BSN op het identiteitsdocument afschermt, geeft Nippon Express de lading niet vrij voor het transport, zo verklaarde Nippon Express tijdens het onderzoek ter plaatse.

Tijdens het onderzoek ter plaatse heeft de Autoriteit Persoonsgegevens vastgesteld dat er op een computerscherm met het functionerende systeem scans van identiteitsdocumenten te zien zijn. Hiervan zijn schermafbeeldingen genomen. Links van de afbeelding van (de houderpagina[63] van) het identiteitsdocument bevond zich op het scherm een kolom met gegevens. In deze kolom was onder andere

[62] Webadres: https://en.wikipedia.org/wiki/Machine-readable_passport
[63] De harde dikke pagina in het paspoort waarop de pasfoto, biografische en documentinformatie staat.

het BSN opgenomen (dus naast de scan van het paspoort). Het BSN stond zowel bij de scans van paspoorten vermeld als bij de scans van identiteitskaarten.[64]

Tijdens het onderzoek ter plaatse van de Autoriteit Persoonsgegevens verklaarde Nippon Express in de middag dat het BSN niet (meer) werd opgenomen in de kolom met gegevens die op de linkerzijde van het scherm werd afgebeeld naast de afbeelding van de houderpagina van het identiteitsdocument. De Autoriteit Persoonsgegevens stelde hierop vast dat het BSN niet meer op de linkerhelft van het scherm te zien was en dat de daar eerder getoonde BSN's waren verwijderd.[65] De Autoriteit Persoonsgegevens stelde voorts vast dat de afbeelding van de houderpagina van het identiteitsdocument met de MRZ (met daarin het BSN) onveranderd zichtbaar was op de rechterzijde van het scherm. Bij sommige afbeeldingen van het identiteitsdocument was het BSN ook buiten de MRZ opgenomen.



Schermafbeelding [naam leverancier] Document Scan met groene vink

A: Gedeelte van de uitgelezen houder informatie

B: Burgerservicenummer (BSN)

C: Afbeelding van de houderpagina

D: Machine Readable Zone

[64] In het Nederlandse paspoort, model 2011, staat het BSN op de houderpagina én afzonderlijk én verwerkt in de MRZ. Op de Nederlandse identiteitskaart, model 2011, staat het BSN voorop de houderpagina. Zie Kenmerken Nederlandse Reisdocumenten, blz. 3, te vinden via webadres: https://www.rvig.nl/reisdocumenten/documenten/brochures/2011/11/02/kenmerkenfolder-2011 .
Vanaf 2014 staat het BSN niet langer voorop , op de houderpagina, maar op de achterzijde van de houderpagina. De MRZ, met daarin het BSN, staat ongewijzigd op de voorzijde van de houderpagina. Zie webadres: https://www.rijksoverheid.nl/documenten/brochures/2015/12/04/kenmerken-nederlandse-paspoorten-en-nederlandse-identiteitskaart

[65] De Autoriteit Persoonsgegevens heeft geen nader onderzoek gedaan naar de vraag of het BSN buiten de afbeeldingen van identiteitsdocumenten feitelijk nog wordt verwerkt.

4. Beoordeling

4.1 Verantwoordelijke

Op grond van artikel 1, aanhef en onder d, van de Wbp is de verantwoordelijke:
"*de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.*"

Volgens Nippon Express is Nippon Express zelf de verantwoordelijke voor de verwerking met de [naam leverancier] documentscanner. Het doel van de gegevensverwerking met de scanner is identificatie en authenticatie van de chauffeurs. Deze doelen zijn door Nippon Express bepaald.[66] Nippon Express heeft voor het realiseren van deze doelen gekozen voor de [naam leverancier] documentscanner en bijbehorende dienstverlening.[67] Daarnaast heeft de Autoriteit Persoonsgegevens geconstateerd dat Nippon Express in de instellingen van de [naam leverancier] software de persoonsgegevens die worden gescand zelf kan (doen) in- of uitschakelen.

Ten slotte heeft Nippon Express de verwerking met de [naam leverancier] documentscan als verantwoordelijke gemeld bij de Autoriteit Persoonsgegevens.[68]

Nippon Express bepaalt derhalve doel en middelen van de verwerking en is daarmee de verantwoordelijke voor de verwerking met de scanapparatuur, als bedoeld in artikel 1, aanhef en onder d, van de Wbp.

4.2 Verwerking van persoonsgegevens

Volgens artikel 1, aanhef en onder a, van de Wbp wordt onder een 'persoonsgegeven' verstaan: "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon."

De definitie bevat een aantal elementen die expliciet aandacht vragen. Allereerst moet het gaan om informatie 'betreffende' een natuurlijke persoon ('any information relating to'). Voorts moet deze persoon zijn geïdentificeerd of althans identificeerbaar zijn ('identified or identifiable'). Als er aan één van beide elementen niet is voldaan, dan is er geen sprake van persoonsgegevens en is de wet niet van toepassing. Hoewel het gaat om twee onderscheiden beoordelingsmomenten, staan zij niet los van elkaar. Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon moeten als persoonsgegevens worden beschouwd.

Nippon Express gebruikt scanapparatuur van [naam leverancier] om de voorzijde, achterzijde en tussenlagen van de houderpagina in het identiteitsdocument van vrachtwagenchauffeurs te scannen.

De gegevens die met de scanapparatuur worden gescand zijn:
- type identiteitsdocument (MRZ- en houderinformatie)
- land van uitgifte identiteitsdocument (MRZ)

[66] Aldus verklaard door Nippon Express tijdens het onderzoek ter plaatse.
[67] Aldus verklaard door Nippon Express tijdens het onderzoek ter plaatse.
[68] Meldingsnummer: m1457126

- naam en voornamen van de houder (MRZ- en houderinformatie)
- nummer identiteitsdocument (MRZ- en houderinformatie)
- nationaliteit (MRZ- en houderinformatie)
- geboortedatum (MRZ- en houderinformatie)
- geslacht (MRZ- en houderinformatie)
- verloopdatum van het document (MRZ- en houderinformatie)
- burgerservicenummer (MRZ)
- pasfoto in zwart-wit (houderinformatie)
- pasfoto in kleur en in hoge resolutie (datagroep 2 van de RFID)

Bovenstaande gegevens kunnen op zichzelf dan wel in combinatie informatie verschaffen over een geïdentificeerde natuurlijke persoon. Daarom moeten zij als persoonsgegevens worden beschouwd als bedoeld in artikel 1, aanhef en onder a, Wbp.

'Verwerking van persoonsgegevens' is gedefinieerd in artikel 1, aanhef en onder b, van de Wbp en omvat onder meer het verzamelen, vastleggen, bewaren, opvragen, raadplegen, gebruiken en afschermen van persoonsgegevens.

Het scannen van het identiteitsdocument door Nippon Express kan gezien worden als het technisch raadplegen of opvragen en vastleggen van persoonsgegevens en geldt derhalve als het verwerken van persoonsgegevens zoals bedoeld in artikel 1, aanhef en onder b, van de Wbp.

4.3 Bijzondere persoonsgegevens

Artikel 16 Wbp bepaalt: *"De verwerking van persoonsgegevens betreffende iemands* […] *ras* […] *is verboden behoudens het bepaalde in deze paragraaf.* […]*"*

Verwerking nationaliteit
De Autoriteit Persoonsgegevens heeft vastgesteld dat Nippon Express de nationaliteit van de houder van het identiteitsdocument scant.

Informatie over nationaliteit zegt in veel gevallen iets over de etnische afkomst van iemand. In de wetsgeschiedenis staat: *"Het begrip* [ras] *moet ruim worden opgevat en omvat ook huidskleur, afkomst en nationale of etnische afstamming".*[69] Dat betekent dat nationaliteit vaak overeen komt met nationale afstamming. In die gevallen moet het als gegeven over ras wordt aangemerkt.

Volgens artikel 16 Wbp is het verboden persoonsgegevens betreffende iemands ras te verwerken, tenzij één van de uitzonderingen geldt die genoemd worden in paragraaf 2 van de Wbp.

De enige uitzonderingen die mogelijk van toepassing zijn, staan in artikel 18, aanhef en onder a, Wbp[70] en artikel 23 Wbp.[71]

[69] Kamerstukken II 1997/98, 25 892, nr. 3, p. 104.
[70] De uitzondering genoemd in artikel 18, aanhef en onder b, Wbp heeft betrekking op het doel personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen ten einde feitelijke nadelen verband houdende met de grond ras op te heffen of te verminderen.
[71] Lid 1

Artikel 18 Wbp bepaalt: *"Het verbod om persoonsgegevens betreffende iemands ras te verwerken als bedoeld in artikel 16, is niet van toepassing indien de verwerking geschiedt:*
a. met het oog op de identificatie van de betrokkene en slechts voor zover dit voor dit doel onvermijdelijk is;
[...]"

Ter identificatie van de chauffeur scant Nippon Express diens identiteitsdocument. Gezien de vele verschillende identiteitsdocumenten die de chauffeurs aan Nippon Express kunnen overleggen, is het ondoenlijk voor dat bedrijf om de echtheidscontroles van deze documenten handmatig uit te voeren. Om deze reden gebruikt Nippon Express als hulpmiddel de scanapparatuur van [naam leverancier]. Op het identiteitsdocument staat de nationaliteit van de houder. Het is daarom niet vermijdbaar om iemand aan de hand van diens identiteitsdocument te identificeren, zonder de nationaliteit te verwerken. Daarom voldoet deze verwerking aan het vereiste van artikel 18, onder a, Wbp, en is het een geoorloofde verwerking van persoonsgegevens betreffende iemands ras.

Verwerking pasfoto
De Autoriteit Persoonsgegevens heeft voorts vastgesteld (zie paragraaf 3.3) dat bij het scannen van de identiteitsdocumenten onder andere met behulp van RFID, datagroep 2 uit de chip wordt uitgelezen. Deze datagroep bevat de pasfoto in kleur en in hoge resolutie. Bij het uitlezen van de chip wordt de pasfoto in kleur en in hoge resolutie verwerkt. Deze scans van de MRZ en van de RFID-chip worden doorgezonden naar [naam leverancier] en daar verder verwerkt.

Omdat uit een foto op een identiteitsdocument het ras van de houder van het identiteitsdocument kan worden afgeleid, kan ook de pasfoto als een gegeven over ras worden aangemerkt.[72] Het verwerken van bijzondere persoonsgegevens over ras is behoudens uitzonderingen verboden.

Voorafgaand aan de afgifte van de lading meldt de vrachtwagenchauffeur zich aan de balie van Nippon Express. Aan de balie wordt de chauffeur gevraagd om zich te identificeren met een geldig identiteitsdocument.

Nippon Express heeft een procedure om vast te stellen of de chauffeur is wie hij zegt te zijn. Nippon Express controleert aan de balie of de chauffeur lijkt op de persoon op de foto op het identiteitsdocument. Ook kan de chauffeur worden gecontroleerd op leeftijd, lengte en handtekening. Verder wordt het document gecontroleerd op zichtbare onregelmatigheden. Het personeel maakt vervolgens een scan van het identiteitsdocument voor controle van de echtheidskenmerken. Voor die controle maakt Nippon Express gebruik van de scanapparatuur van [naam leverancier]. Deze apparatuur vergelijkt onder meer de zwartwit pasfoto op de houderpagina[73] van het identiteitsdocument met de pasfoto in kleur in de RFID-tag. Dit gebeurt geautomatiseerd.

Onverminderd de artikelen 17 tot en met 22 is het verbod om persoonsgegevens als bedoeld in artikel 16, te verwerken niet van toepassing voor zover:
a. dit geschiedt met uitdrukkelijke toestemming van de betrokkene;
b. de gegevens door de betrokkene duidelijk openbaar zijn gemaakt;
c. dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte;
d. dit noodzakelijk is ter verdediging van de vitale belangen van de betrokkene of van een derde en het vragen van diens uitdrukkelijke toestemming onmogelijk blijkt;
[...]

[72] Memorie van Toelichting, Tweede Kamer, vergaderjaar 1997-1998, 25 892, nr. 3, blz. 105

[73] De harde dikke pagina in het paspoort waarop biografische en documentinformatie staat.

De vergelijking van de twee pasfoto's is gericht op echtheidscontrole van het identiteitsdocument. Door onderlinge vergelijking van de foto's kan worden vastgesteld of de zichtbare foto op het identiteitsdocument origineel (niet vervangen) is. Dit is onderdeel van de identificatie.

Het verwerken van beeldmateriaal kan een verwerking van bijzondere persoonsgegevens inhouden, bijvoorbeeld omdat het ras van de persoon is af te leiden uit het beeldmateriaal.

Het verwerkingsverbod van persoonsgegevens betreffende iemands ras als bedoeld in artikel 16 Wbp, is niet van toepassing indien de verwerking geschiedt met het oog op identificatie van de betrokkene en slechts voor zover dit voor dit doel onvermijdelijk is (artikel 18, onder a, Wbp).

Ook hier geldt dat het voor Nippon Express ondoenlijk is om de echtheidscontroles van deze documenten handmatig uit te voeren. Om deze reden gebruikt Nippon Express als hulpmiddel de scanapparatuur. Het is daarom niet vermijdbaar om iemand aan de hand van diens identiteitsdocument te identificeren, zonder de afbeeldingen te verwerken bij de echtheidscontrole. Daarom voldoet deze verwerking aan het vereiste van artikel 18, onder a, Wbp, en is het een geoorloofde verwerking van persoonsgegevens betreffende iemands ras.

4.4 Gebruik wettelijk identificatienummer

Artikel 24, eerste lid, Wbp bepaalt: *"Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald."*

Zoals hierboven aangegeven is in de Memorie van Toelichting op artikel 24 Wbp opgenomen dat omdat het gebruik van persoonsnummers extra risico's met zich kan brengen voor de bescherming van de persoonlijke levenssfeer dit artikel bepaalt dat verwerking van persoonsnummers voor andere doeleinden dan de uitvoering van de betreffende wet alleen mogelijk is voor zover dat bij de wet is bepaald. Hiermee is, aldus de Memorie van Toelichting, een afweging op het niveau van de formele wet gegarandeerd. De regeling ziet derhalve op het gebruik van het Nederlandse BSN.

Tijdens het onderzoek ter plaatse stelde de Autoriteit Persoonsgegevens vast dat het BSN tweevoudig werd uitgelezen: uit de specifieke weergave op de houderpagina en uit de MRZ. In de middag van het onderzoek ter plaatse stelde de Autoriteit Persoonsgegevens vast dat het BSN niet meer op de linkerhelft van het scherm te zien was en dat de daar eerder getoonde BSN's waren verwijderd.[74] De Autoriteit Persoonsgegevens stelde voorts vast dat de afbeelding van de houderpagina van het identiteitsdocument met de MRZ (met daarin het BSN) onveranderd zichtbaar was op de rechterzijde van het scherm.[75] Bij sommige afbeeldingen van het identiteitsdocument was het BSN ook buiten de MRZ opgenomen.

[74] De Autoriteit Persoonsgegevens heeft geen nader onderzoek gedaan naar de vraag of het BSN buiten de afbeeldingen van identiteitsdocumenten feitelijk nog wordt verwerkt.

[75] In het Nederlandse paspoort, model 2011, staat het BSN op de houderpagina én afzonderlijk én verwerkt in de MRZ. Op de Nederlandse identiteitskaart, model 2011, staat het BSN voor op de kaart. Zie Kenmerken Nederlandse Reisdocumenten, blz. 3, te vinden via webadres: https://www.rvig.nl/reisdocumenten/documenten/brochures/2011/11/02/kenmerkenfolder-2011.
Vanaf 2014 staat het BSN niet langer voorop op de houderpagina, maar op de achterzijde van de houderpagina. De MRZ, met daarin het BSN, staat ongewijzigd op de voorzijde van de houderpagina. Zie webadres:

Artikel 24 Wbp bepaalt dat een wettelijk voorgeschreven persoonsnummer slechts wordt gebruikt ter uitvoering van de wet waarin het voorschrift over een persoonsnummer is opgenomen. Het burgerservicenummer is volgens de Wet algemene bepalingen burgerservicenummer een persoonsnummer als bedoeld in artikel 24 Wbp.

Eén van de persoonsgegevens in de MRZ is het BSN. Omdat het gebruik van het BSN extra risico's met zich kan brengen voor de bescherming van de persoonlijke levenssfeer, wordt in bovengenoemd wetsartikel daarenboven bepaald dat verwerking van persoonsnummers voor andere doeleinden dan de uitvoering van de betreffende wet alleen mogelijk is voor zover dat bij de wet is bepaald.

Uit artikel 1, aanhef en onder b, Wbp volgt dat het uitlezen en controleren van de MRZ, waar het BSN deel van uitmaakt, een verwerking van het BSN is. Ook het opnemen van het BSN (buiten de MRZ) in de afbeelding van het identiteitsdocument is een verwerking van het BSN. De Autoriteit Persoonsgegevens stelt vast dat Nippon Express het BSN verwerkt van vrachtwagenchauffeurs en dat Nippon Express daartoe niet gerechtigd is. Op grond van artikel 24 Wbp is het verwerken van het BSN alleen toegestaan als er een wettelijke grondslag bestaat. Nippon Express beschikt niet over een wettelijke grondslag voor het verwerken van het BSN.

Voormalige beoordeling

Nippon Express heeft door het scannen van het BSN (in de MRZ) van het identiteitsdocument en het verder (laten) verwerken van het BSN derhalve in strijd gehandeld met artikel 24, eerste lid, Wbp.

Zienswijze Nippon Express

Bij brief van 12 januari 2017 heeft Nippon Express het volgende verklaard ten aanzien van de verwerking van het BSN.

"[…] *het BSN nummer* [wordt] *niet meer door ons verwerkt. Het [naam leverancier] systeem wordt gebruikt voor het bepalen van de echtheid van het aangeboden ID document. Wij accepteren van de Nederlandse chauffeurs uitsluitend het rijbewijs. Bij het scannen wordt het BSN nummer afgeplakt waardoor deze geen onderdeel meer is van het gescande document. Het rijbewijs heeft geen MRZ code waardoor ook hier geen BSN nummer meer herleidbaar is. Er vindt dus geen enkele verwerking meer plaats van het BSN nummer. Wij menen dat wij hiermee niet meer in strijd handelen van met artikel 24, eerste lid, Wbp.*"

Oordeel van de AP op de zienswijze van Nippon Express

De Autoriteit Persoonsgegevens concludeert uit bovenstaande zienswijze dat Nippon Express niet meer het BSN verwerkt en daarmee niet langer in strijd handelt met artikel 24, eerste lid, Wbp.

---

https://www.rijksoverheid.nl/documenten/brochures/2015/12/04/kenmerken-nederlandse-paspoorten-en-nederlandse-identiteitskaart.

4.5 Grondslag van de verwerking

Artikel 8 Wbp bepaalt: "*Persoonsgegevens mogen slechts worden verwerkt indien:*
a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert."

Artikel 8 Wbp bevat een uitputtende opsomming van verwerkingsgronden.[76]

Ondubbelzinnige toestemming
Artikel 8, onder a, Wbp vereist dat de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend. De toestemming dient een vrije, specifieke en op informatie berustende wilsuiting te zijn, waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.[77] Een "toestemming" kan alleen rechtsgeldig zijn als de betrokkene een werkelijke keuze heeft en er geen sprake is van bedrog, intimidatie of dwang en de betrokkene ook niet het risico van aanzienlijke negatieve gevolgen loopt wanneer hij niet toestemt. Wanneer de gevolgen van toestemming de keuzevrijheid van de betrokkene beperken, kan er geen sprake zijn "vrije" toestemming.[78]

De controleprocedure van het kenteken, de vrachtwagen, en de scan van het identiteitsdocument die Nippon Express van de chauffeurs verlangt, is verplicht. Indien de chauffeur hieraan geen medewerking verleent, dan wordt het laadproces beëindigd en krijgt de chauffeur de lading niet mee.[79] De chauffeur heeft geen ruimte om niet mee te werken aan de controleprocedure. Hij is immers als chauffeur in uitoefening van zijn beroep, en heeft de taak gekregen om de lading mee te nemen.

Gezien het bovenstaande wordt niet voldaan aan het vereiste dat de toestemming die Nippon Express aan de chauffeur vraagt, een vrije wilsuiting van de chauffeur is. Daarmee is de grondslag van artikel 8, onder a, Wbp niet van toepassing.

Uitvoering van een overeenkomst
Artikel 8, onder b, Wbp bepaalt dat een gegevensverwerking toelaatbaar is indien deze noodzakelijk is om contractuele verplichtingen na te komen. Daarbij geldt als voorwaarde dat de betrokkene partij is bij de desbetreffende overeenkomst. Tevens is een gegevensverwerking geoorloofd indien deze noodzakelijk is in de precontractuele fase.

[76] Kamerstukken II 1997/98, 25 892, nr. 3, p. 5-6.
[77] Artikel 1, onder i, Wbp
[78] Opinie WP29 15-2011, p.14, 15.
[79] Intern document Nippon Express: WI-Security-002-General Loading procedure (GENERAL) version: 6, p. 2.

Artikel 8, aanhef en onder b, Wbp gaat over overeenkomsten waarbij betrokkene partij is. Hier zien de overeenkomsten tussen betrokkene (de chauffeur) en een andere partij (de andere partij kan Nippon Express zijn, de werkgever van betrokkene of een andere opdrachtgever), primair op het vervoeren van lading. De verplichting tot scannen van ID's vloeit hier niet uit voort. Dit betekent dat artikel 8, aanhef en onder b Wbp, ook om deze reden geen geldige grondslag voor de verwerking van persoonsgegevens kan zijn.

Wettelijke verplichting
Artikel 8, onder c, Wbp bepaalt dat de verantwoordelijke gerechtigd is gegevens te verwerken indien dit noodzakelijk is ter uitvoering van een wettelijke verplichting die op hem rust. Er is geen wettelijke verplichting als gevolg waarvan Nippon Express de echtheidskenmerken van de identiteitsdocumenten met behulp van de scanapparatuur moet controleren. Daarom kan deze verantwoordelijke hier geen beroep op doen.

Vitaal belang
Artikel 8, onder d, Wbp is een geldige verwerkingsgrond indien er een dringende medische noodzaak is om de gegevens van de betrokkene te verwerken. Het moet gaan om een zaak van leven of dood. Ook van deze grondslag is geen sprake.

Vervulling publiekrechtelijke taak
Een grondslag op basis van artikel 8, onder e, Wbp is alleen van toepassing op de publieke sector.

Gerechtvaardigd belang
Uit bovenstaande volgt dat de enige mogelijke grondslag voor de verwerking met de scanner van persoonsgegevens die op de identiteitsdocumenten staan, artikel 8, onder f, Wbp kan zijn: een gerechtvaardigd belang.

Artikel 8, onder f, Wbp vergt een belangenafweging; wat is noodzakelijk voor het gerechtvaardigd belang van de verantwoordelijke en hoe verhoudt dit zich tot de belangen van de betrokkenen, zoals de fundamentele rechten en vrijheden van personen. Als de verantwoordelijke aanvullende waarborgen heeft getroffen kan dit de afweging ten gunste van de verantwoordelijke doen uitslaan. Hierbij gaat het bijvoorbeeld om: beveiliging, anonimiseren, een goede belangenafweging en het goed informeren van betrokkenen over de verwerkingen.[80]

Uit artikel 8, onder f, Wbp vloeien derhalve de volgende drie voorwaarden voort:
A. de verantwoordelijke moet een gerechtvaardigd belang hebben bij de verwerking;
B. de verwerking dient noodzakelijk te zijn voor het doel (proportionaliteit en subsidiariteit), en
C. het belang of de fundamentele rechten van de betrokkenen prevaleert niet boven het gerechtvaardigd belang van de verantwoordelijke.

Onderstaand wordt achtereenvolgens nagegaan of Nippon Express een gerechtvaardigd belang heeft, of de verwerking noodzakelijk is voor het doel en of het belang van Nippon Express prevaleert boven het belang van de chauffeurs.

[80] Opinion 06-2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95-46-EC, pag. 42 e.v.

Voorwaarde 1: heeft Nippon Express een gerechtvaardigd belang?
In de eerste plaats vereist artikel 8, aanhef en onder f, Wbp dat sprake is van een gerechtvaardigd belang van de verantwoordelijke of van een derde. Een gerechtvaardigd belang van de verantwoordelijke kan aanwezig worden geacht in het geval dat de betreffende verwerking noodzakelijk is om zijn reguliere bedrijfsactiviteiten te verrichten.[81] Ook ten aanzien van gegevensverwerkingen die weliswaar geen onderdeel uitmaken van de reguliere bedrijfsactiviteiten van de verantwoordelijke maar deze wel in wezenlijke zin ondersteunen, kan in de regel worden aangenomen dat de verantwoordelijke een gerechtvaardigd belang heeft.[82]

Het controleren van de identiteitsdocumenten van de vrachtwagenchauffeurs om te voorkomen dat - kostbare - lading wordt afgegeven aan de verkeerde personen, is een activiteit die de reguliere bedrijfsactiviteit van Nippon Express ondersteunt.

Uit bovenstaande vloeit voort dat Nippon Express een gerechtvaardigd belang heeft bij het verwerken van persoonsgegevens ten behoeve van het genoemde doeleinde.

Voorwaarde 2: Is de gegevensverwerking noodzakelijk voor het doel?
Voor een geslaagd beroep op de grondslag gerechtvaardigd belang is voorts vereist dat de gegevens-verwerking als noodzakelijk voor het doel moet worden beschouwd. Dat wil zeggen: staat het middel in verhouding tot het doel en kan het belang van de verantwoordelijke anderszins of met minder ingrijpende middelen worden gediend.[83]

Nippon Express heeft tijdens het onderzoek ter plaatse aan de AP verklaard dat een controle op echtheid van identiteitsdocumenten niet mogelijk is zonder gebruik van de [naam leverancier] scanner en diensten. De reden hiervoor is dat Nippon Express chauffeurs ontvangt van veel verschillende nationaliteiten. Van elk land zijn bovendien verschillende typen en modellen paspoorten en andere identiteitskaarten in omloop. Vanwege het grote aantal in omloop zijnde paspoorten en identiteitskaarten acht de AP het aannemelijk dat het voor Nippon Express niet mogelijk is om aan de balie de diverse identiteitsdocumenten goed te kunnen controleren op de verschillende echtheidskenmerken. Bovendien vindt Nippon Express dat zij niet in staat is om per land de ontwikkelingen op het gebied van identiteitsdocumenten te volgen.

Het is voor Nippon Express ondoenlijk om alle kenmerken van de verschillende versies van identiteits-documenten die in omloop zijn bij te houden. Bovendien zijn sommige echtheidskenmerken alleen met hulpmiddelen als UV-licht, infraroodlicht of een RFID-scanner te controleren,[84] zodat controle met de hand niet voldoet. Controle van echtheidskenmerken die alleen onder UV-licht of infraroodlicht te zien zijn, is alleen mogelijk door middel van technische hulpmiddelen. Ook is het niet mogelijk om zonder technisch hulpmiddel de digitale pasfoto op de RFID chip op te vragen om die te vergelijken met de pasfoto die op de houderpagina staat. Daarmee staat vast dat deze gegevensverwerking als noodzakelijk voor het doel moet worden beschouwd.

Op een ID staat een aantal gevoelige gegevens, zoals de nationaliteit en de pasfoto. In paragraaf 4.3 bleek dat de nationaliteit en de pasfoto bijzondere persoonsgegevens zijn, maar dat het verwerkingsverbod van

[81] Kamerstukken II 1997/98, 25 892, nr. 3, p. 86.
[82] Kamerstukken II 1997/98, 25 892, nr. 3, p. 87.
[83] Kamerstukken II 1997/98, 25 892, nr. 3, p. 87.
[84] Zie webadres: https://www.rvig.nl/binaries/rvig/documenten/brochures/2014/03/07/model-2014-paspoort-en-nederlandse-identiteitskaart/web-100887-kenmerkendoc-2017-ned.pdf

persoonsgegevens betreffende iemands ras als bedoeld in artikel 16 Wbp, niet van toepassing is omdat de verwerking geschiedt met het oog op identificatie van de betrokkene en dit voor dit doel onvermijdelijk is.

Gezien bovenstaande moet de gegevensverwerking als noodzakelijk voor het doel moet worden beschouwd en kan dit belang van de verantwoordelijke niet anderszins of met minder ingrijpende middelen dan een ID-scanner worden gediend.

Hierna wordt gekeken of er maatregelen mogelijk zijn die de impact voor betrokkene minder maken.

Voorwaarde 3: Prevaleert het belang van de verantwoordelijke?
De derde voorwaarde voor een geslaagd beroep op een gerechtvaardigd belang behelst een nadere afweging, waarbij de belangen van de betrokkenen een zelfstandig gewicht in de schaal leggen tegenover het belang van de verantwoordelijke.

Het belang van Nippon Express is om te voorkomen dat de lading aan een verkeerde partij wordt meegegeven, met alle grote negatieve financiële consequenties daarbij. Het belang van de chauffeur is dat er zo min mogelijk inbreuk op zijn persoonlijke levenssfeer wordt gemaakt. Het belang van de chauffeur kan worden gerealiseerd door bijvoorbeeld het aantal verwerkte persoonsgegevens te beperken en door maatregelen te nemen die de kans verkleinen dat betrokkene slachtoffer wordt van identiteitsfraude. Bij het scannen van de identiteitsdocumenten, wordt een aantal persoonsgegevens uitgelezen en opgeslagen. Met de gescande ID's en de persoonsgegevens kan identiteitsfraude gepleegd worden. Dit risico voor de betrokkenen op identiteitsfraude kan Nippon Express verminderen door maatregelen te nemen.

De Rijksoverheid heeft maatregelen gepubliceerd[85] om de kans op fraude met identiteitsdocumenten te verminderen. Een voorbeeld van zo'n maatregel is om op de kopie te vermelden voor welke organisatie de kopie is bedoeld. Een ander voorbeeld is het vermelden van een einddatum van de geldigheid van de kopie. Met dergelijke waarborgen, die niet veel hoeven te kosten, wordt de kopie onbruikbaar voor andere doeleinden. Nu Nippon Express er niet voor gekozen heeft om maatregelen te nemen waardoor de kans op identiteitsfraude wordt gereduceerd, kan het belang van Nippon Express niet prevaleren boven het belang van de betrokken chauffeurs. In de belangenafweging is Nippon Express onvoldoende ver gegaan in het treffen van waarborgen teneinde de risico's voor de betrokkenen te adresseren.

Concluderend
Uit bovenstaande blijkt dat Nippon Express geen geslaagd beroep kan doen op de grondslag gerechtvaardigd belang, zoals bedoeld in artikel 8 aanhef en onder f, Wbp, voor het gebruik van de scanner van [naam leverancier], omdat door het ontbreken van voldoende waarborgen die tegemoet komen aan de belangen van de betrokken chauffeurs, het belang van Nippon Express niet prevaleert over het belang van de betrokkene.

Nippon Express kan ook geen geslaagd beroep doen op één van de andere grondslagen in artikel 8 Wbp. Derhalve handelt Nippon Express door de verwerking van persoonsgegevens met de ID-scanner in strijd met artikel 8 Wbp.

[85] Zie webadres: https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/fraude-voorkomen-met-kopie-id-bewijs

4.6 Beveiliging

Artikel 13 Wbp bepaalt: "*De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.*"

Uit het juridisch kader (zie hoofdstuk 2) blijkt dat bij het beantwoorden van de vraag of beveiligingsmaatregelen 'passend' zijn, zoals de Wbp eist, moet worden aangesloten bij algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging, zoals de 'ICT-beveiligingsrichtlijnen' van het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie, en het Amerikaanse National Institute of Standards and Technology.

Serverconfiguratie
Nippon heeft verklaard dat er geen IP-adrestoegangsbeperking wordt toegepast. Dit betekent dat toegang tot de websites nippon.[naam leverancier]documentscan.com en nippon.[naam leverancier]authentiscan.com mogelijk is voor een ieder met een webbrowser en toegang tot het internet. De Autoriteit Persoonsgegevens heeft vastgesteld dat toegang tot nippon.[naam leverancier]documentscan.com en nippon.[naam leverancier]authentiscan.com mogelijk is vanaf haar eigen internetverbinding.[86]

In het systeem staan duizenden gescande identiteitsdocumenten. Deze zijn benaderbaar vanaf elke computer met internettoegang. Met gescande identiteitsdocumenten kan identiteitsfraude worden gepleegd. Deze scans moeten daarom goed beveiligd worden.

De Autoriteit Persoonsgegevens heeft op 16 februari 2016, 3 maart 2016, 6 april 2016 en 4 oktober 2016 geconstateerd dat de configuratie van de websites nippon.[naam leverancier]documentscan.com en nippon.[naam leverancier]authentiscan.com het gebruik van het protocol SSLv3 toe staan, en ook de cipher-methoden RC4-SHA en RC4-MD5.

Volgens algemeen aanvaarde beveiligingsstandaarden als 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van het NCSC, en 'National Vulnerability Database' van het National Institute of Standards and Technology, zijn zowel protocol SSLv3[87] als versleutelingsmethoden RC4-SHA[88] en RC4-MD5[89] verouderde en daarom onveilige technieken.

[86] Zie paragraaf 3.7.
[87] https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls/1/ICT+beveiligingsrichtlijnen+voor+Transport+Layer+Security++TLS+++leesversie+.pdf, p.15.
Zie ook: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566.
[88] https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls/1/ICT+beveiligingsrichtlijnen+voor+Transport+Layer+Security++TLS+++leesversie+.pdf, p.16.
Zie ook: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566
[89] https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls/1/ICT+beveiligingsrichtlijnen+voor+Transport+Layer+Security++TLS+++leesversie+.pdf, p.16.
Zie ook: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2761

Voormalige beoordeling

Nu Nippon Express verouderde beveiligingstechnieken heeft gebruikt in zijn communicatie over het internet, heeft hij onvoldoende passende maatregelen genomen ter voorkoming van het risico op onrechtmatige verwerking. Ook heeft Nippon Express geen IP-adres beperking ingesteld, waardoor het inlogscherm van de ID-scanner vanaf elke computer met internettoegang te benaderen is. Daarmee heeft Nippon Express artikel 13 Wbp overtreden.

Meerfactorauthenticatie

De Autoriteit Persoonsgegevens heeft op 3 februari 2016 voorts vastgesteld dat de identificatie en authenticatie voor de websites nippon.[naam leverancier]documentscan.com en nippon.[naam leverancier]authentiscan.com plaatsvindt op basis van drie gegevens: (1) accountnaam, (2) gebruikersnaam en (3) wachtwoord.

Authenticatie is het proces waarbij wordt nagegaan of een gebruiker die wil inloggen in een applicatie of een systeem daadwerkelijk is wie hij beweert te zijn. Het invoeren van een gebruikersnaam en wachtwoord is een voorbeeld van authenticatie middels één factor, namelijk het wachtwoord. (Het invoeren van een gebruikersnaam, password en een sms-code is een voorbeeld van meerfactor-authenticatie.) Andere vormen van meerfactorauthenticatie zijn mogelijk.

Nippon Express gebruikt de accountnaam mogelijk als tweede factor. Omdat de accountnaam hier gelijk is aan de bedrijfsnaam (afbeelding 3), is er in deze context geen sprake van een tweede factor die bijdraagt aan een passend beveiligingsniveau.

Zoals hierboven onder paragraaf 2.6 is aangegeven moet volgens algemeen geaccepteerde beveiligings-standaarden bij toegang via internet tot applicaties met gevoelige of bijzondere persoonsgegevens tenminste gebruik worden gemaakt van meerfactorauthenticatie.

Doordat Nippon geen gebruik maakt van meerfactorauthenticatie bij de toegang tot gevoelige (bijzondere) persoonsgegevens via internet, wordt gehandeld in strijd met de vereisten ten aanzien van de beveiliging zoals die volgen uit artikel 13 Wbp.

Zienswijze Nippon Express

Bij brief van 12 januari 2017 heeft Nippon Express het volgende verklaard ten aanzien van de beveiliging van persoonsgegevens.

"*De verwerking van de scans vindt plaats door een verbinding te leggen met de [naam leverancier] website middels een verificatie van account, user en password. Elke gebruiker krijgt zijn/haar eigen inlog waarbij in de toegangsrechten wordt bepaald wat iemand wel of niet mag. Als standaard staat ingesteld dat gebruikers uitsluitend toegang hebben tot de documenten die door deze gebruiker zijn gescand en dat er geen toestemming is om rapportages af te drukken. In de schermen is het ID bewijs onbruikbaar gemaakt door daar een kenmerk overheen te zetten (een groene vink). Met deze maatregel is het voor de gebruiker niet mogelijk om een copy van een ID te verkrijgen zonder dat deze onbruikbaar is gemaakt. Met deze maatregelen denken wij geen inbreuk maken op artikel 13 Wbp.*"

Oordeel van de AP op de zienswijze van Nippon Express

Ten aanzien van de cryptografische bescherming van de toegang tot uw website stelt de Autoriteit Persoonsgegevens vast dat Nippon Express de configuratie van de websites heeft aangepast. Nippon

Express maakt niet langer gebruik van de cipher-methoden RC4-SHA en RC4-MD5 en het protocol SSLv3. Hierdoor handelt Nippon Express op dit punt niet langer in strijd met artikel 13 Wbp.

De Autoriteit Persoonsgegevens constateert dat Nippon Express in zijn zienswijze niet ingaat op de authenticatie. Dit betekent dat Nippon Express nog steeds geen meerfactorauthenticatie gebruikt bij de toegang tot gevoelige (bijzondere) persoonsgegevens via internet. Bovendien is de website nog steeds voor iedereen bereikbaar vanaf het internet. De groene vink doet daar niet aan af.[90] Hierdoor handelt Nippon Express in strijd met de vereisten ten aanzien van de beveiliging zoals die volgen uit artikel 13 Wbp.

4.7 Bewaartermijn

Artikel 10, lid 1, Wbp bepaalt: "*Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.*"

De verantwoordelijke dient persoonsgegevens niet langer te bewaren dan noodzakelijk is.

Nippon Express verklaarde dat hij gegevens twintig dagen bewaarde.[91]

Uit artikel 10 Wbp volgt dat Nippon Express de persoonsgegevens niet langer dient te bewaren dan noodzakelijk is voor de verwerkelijking van het doel waarvoor hij worden bewaard. Het doeleinde van de verwerking is dat Nippon Express met voldoende zekerheid de juiste lading aan de juiste chauffeur wil meegeven. Hiertoe verwerkt Nippon Express de persoonsgegevens van de identiteitsdocumenten van de chauffeurs. De identiteitsdocumenten worden hierbij gecontroleerd op de echtheidskenmerken. Deze controle neemt enige momenten (waarbij moet worden gedacht in minuten en niet in dagen) in beslag. Niet valt in te zien waarom de vollédige set persoonsgegevens na deze controle zou moeten worden bewaard. Door de volledige set persoonsgegevens niet aanstonds na de controle te verwijderen (compare and forget), maar deze twintig dagen te bewaren, overtreedt Nippon Express artikel 10 Wbp.

Zienswijze Nippon Express

Bij brief van 12 januari 2017 heeft Nippon Express het volgende verklaard ten aanzien van de bewaartermijn.

"*Met betrekking tot de bewaartermijn zijn wij van mening dat wij een belang hebben om de documenten voor langere tijd (20 dagen) beschikbaar te hebben. Wij gebruiken het [naam leverancier] systeem voor de controle van de identiteitsbewijzen van chauffeurs welke goederen komen ophalen welke eigendom zijn van onze klanten waar wij de verantwoordelijkheid voor dragen. Deze verantwoordelijkheid verplicht ons om ons er van te overtuigen als een goed huisvader, dat wij de goederen meegeven aan de juiste persoon. Bij onregelmatigheden in het transport zullen wij moeten aantonen dat wij aan deze verplichting hebben voldaan. Onze controles zijn daar dan ook een integraal onderdeel van. Op het moment dat er een ernstige onregelmatigheid heeft plaatsgevonden kunnen wij met de beschikbaarheid van deze informatie aantonen op de juiste wijze gehandeld te hebben en mogelijke aanknopingspunten bieden bij een justitieel*

[90] De groene vink kan waarschijnlijk met een beeldverwerkingsprogramma verwijderd worden. Maar ook als dat niet kan, is de afbeelding van het ID nog te gebruiken. Voor maatregelen om fraude met identiteitsdocumenten te voorkomen, zie URL: https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/fraude-voorkomen-met-kopie-id-bewijs

[91] Overigens trof de Autoriteit Persoonsgegevens bij het onderzoek ter plaatse zeven dossiers aan die ouder waren. De oudste dateerde van medio 2013. Nippon Express heeft later bevestigd deze dossiers te hebben verwijderd.

onderzoek. De termijn van 20 dagen is een reële termijn waarbinnen eventuele onregelmatigheden bij ons kenbaar moeten zijn gemaakt."

Bij brief van 20 maart 2017 heeft Nippon Express op nadere onderbouwing van zijn zienswijze gegeven op het punt van de op de bewaartermijn van 20 dagen van scans van identiteitsdocumenten.

"Noodzaak
De werkzaamheden van Nippon Express bestaan uit het ontvangen, opslaan en verladen van goederen welke niet ons eigendom zijn. Wij zijn een logistieke organisatie welke namens derden (onze cliënten) de goederenvoorraad beheren. Onze cliënten houden ons aansprakelijk voor onregelmatigheden welke binnen dit totale proces kunnen plaatsvinden. Zoals wellicht bekend kampt onze sector met door frauduleuze praktijken waaronder het doen ophalen van goederen middels valse identiteitsbewijzen en/of valse kentekens.

[VERTROUWELIJK] *Uit het oogpunt van een financieel verantwoorde bedrijfsvoering op zichzelf als vanuit cliënten, is aangedrongen op aanscherping van onze processen en beheersmaatregelen. Door het vaststellen en controleren van de identiteit van de persoon welke de goederen van ons in ontvangst nemen beperken wij het risico.* [VERTROUWELIJK]

Wat betreft de bewaartermijn merken wij op dat de verzending van goederen plaatsvindt via een vrachtauto al dan niet gecombineerd met andere modaliteiten van transport [VERTROUWELIJK]. *Indien het wel zover is dat een cliënt een onregelmatigheid kan constateren, zal deze in eerste instantie ons aansprakelijk stellen en dienen wij een onderbouwd verweer te voeren. Door het voorhanden hebben van de ID scans (met daarbij de datum en tijd van controle) kunnen wij in ieder geval aantonen een controle te hebben uitgevoerd. Om deze reden achten wij een bewaartermijn van 20 dagen noodzakelijk."*

Oordeel van de AP op de zienswijze van Nippon Express

Met zijn (aanvullende) zienswijze heeft Nippon Express voldoende aangetoond dat een zorgvuldige controle van identiteitsdocumenten noodzakelijk is, en dat de gevolgen van gestolen lading voor Nippon Express zeer ernstig kunnen zijn. Voor de zorgvuldige controle maakt Nippon Express gebruik van geavanceerde scanapparatuur.

[VERTROUWELIJK] Daarmee lijkt de scanner een effectief middel om de echtheid van identiteitsdocumenten te controleren.

[VERTROUWELIJK] Nippon Express hanteert daarbij een termijn van twintig dagen.

Indien er sprake is van ladingdiefstal, kan Nippon Express aansprakelijk worden gesteld voor de schade. Nippon Express dient dan te kunnen aantonen dat hij de identiteitsdocumenten heeft gecontroleerd. Nippon Express stelt dat hij alleen met de volledige set gedetailleerde scans (waarop de datum en tijd van controle staat) kan aantonen het identiteitsdocument op echtheid te hebben gecontroleerd.

De Autoriteit Persoonsgegevens ziet echter niet in waarom Nippon Express de volledige set gedetailleerde scans (waaronder een afbeelding van het identiteitsdocument) nodig heeft om – achteraf – aan te kunnen tonen dat hij het identiteitsdocument op echtheid heeft gecontroleerd. Daarvoor zouden een overzicht van gecontroleerde echtheidskenmerken en een beperkte set persoonsgegevens voldoende moeten zijn.

Voorts stelt Nippon Express dat bij ladingdiefstal de scans mogelijke aanknopingspunten bieden bij een justitieel onderzoek.

Echter voor opsporingsambtenaren zijn persoonsgegevens als voor- en achternaam, geboortedatum en documentnummer voldoende. Met die informatie kunnen opsporingsambtenaren andere gegevens zoals pasfoto's in hun systemen opvragen.

Hoewel het aannemelijk is dat het voor Nippon Express noodzakelijk is een overzicht van gecontroleerde echtheidskenmerken alsmede een beperkte set persoonsgegevens gedurende twintig dagen te bewaren, heeft het bedrijf niet aangetoond dat die noodzaak tevens geldt voor de afbeeldingen van de identiteitsdocumenten. Door de afbeeldingen van de identiteitsdocumenten niet aanstonds na de controle te verwijderen, maar deze twintig dagen te bewaren, handelt Nippon Express in strijd met artikel 10 Wbp.

5. Conclusie

Nippon Express controleert de identiteitsdocumenten van vrachtwagenchauffeurs die goederen komen laden. Nippon Express maakt daarbij gebruik van scanapparatuur en diensten van het bedrijf [naam leverancier].

Nippon Express verwerkt de volgende persoonsgegevens: type identiteitsdocument, nummer identiteitsdocument, land van uitgifte, naam en voornamen van de houder, controlegegevens (welke controles zijn gedaan door het systeem en met welk resultaat), documentstatus (verlopen of niet verlopen), geboortedatum, pasfoto in kleur en hoge resolutie, en tot voor kort het burgerservicenummer. Deze gegevens zijn gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Nippon Express verwerkt persoonsgegevens zoals bedoeld in artikel 1, aanhef en onder a en b, Wbp.

Burgerservicenummer

Ten tijde van het onderzoek ter plaatse, las Nippon Express bij het scannen van de Machine Readable Zone (MRZ) het burgerservicenummer (BSN) uit en verwerkte deze als bedoeld in artikel 1, aanhef en onder b, Wbp. Indien het BSN ook buiten de MRZ is opgenomen, werd ook dit BSN gescand. Ook hiermee verwerkte Nippon Express het BSN als bedoeld in artikel 1, aanhef en onder b Wbp.

Het BSN is een wettelijke identificatienummer als bedoeld in artikel 24 Wbp, waarvoor geldt dat het verboden is een dergelijk nummer te verwerken tenzij de verantwoordelijke over een wettelijke grondslag beschikt. Nippon Express heeft echter geen wettelijke grondslag voor het verwerken van het BSN. Met het verwerken van het BSN in de MRZ en buiten de MRZ in de afbeelding van het identiteitsdocument handelde Nippon Express derhalve in strijd met artikel 24, eerste lid, Wbp.

Nadat de Autoriteit Persoonsgegevens aan Nippon Express het onderzoeksrapport met voorlopige bevindingen stuurde, heeft Nippon Express het verwerken van het BSN gestaakt. Daarmee handelt Nippon Express niet langer in strijd met artikel 24 Wbp.

Grondslag

Iedere verwerking van persoonsgegevens dient te berusten op tenminste één van de in artikel 8 Wbp limitatief opgesomde grondslagen. Voor de verwerking van persoonsgegevens met behulp van de identiteitsdocumentscanner, is de grondslag genoemd in artikel 8, aanhef en onder f, Wbp bepalend. Dit betekent dat de gegevensverwerking noodzakelijk moet zijn voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleren. Nippon Express heeft op zichzelf een gerechtvaardigd belang, te weten het controleren van echtheid van identiteitsdocumenten. Het hebben van een gerechtvaardigd belang is echter niet voldoende. De gegevensverwerking is alleen dan rechtmatig indien zij voor dat doel noodzakelijk is en het belang of de fundamentele rechten van de betrokkene niet prevaleert. Het belang van Nippon Express is om te voorkomen dat de lading aan een verkeerde partij wordt meegegeven, met alle grote negatieve financiële gevolgen van dien. Het belang van de chauffeurs is onder meer om geen slachtoffer te worden van identiteitsfraude. Door het ontbreken van voldoende waarborgen teneinde dit risico voor betrokkene te adresseren, prevaleert het belang van Nippon Express niet over het belang van de betrokkene. Derhalve handelt Nippon Express door de verwerking van persoonsgegevens met de ID-scanner in strijd met artikel 8 Wbp.

Beveiliging

Nippon Express verwerkt in een computersysteem scans van identiteitsdocumenten. De website met het inlogscherm van dit computersysteem is benaderbaar vanaf elke computer met internettoegang. Met gescande identiteitsdocumenten kan identiteitsfraude worden gepleegd. Deze scans moeten daarom goed zijn beveiligd. Uit artikel 13 Wbp volgt een aantal beveiligingsvereisten, waar Nippon Express niet aan voldoet. Zo beschikt het bedrijf niet over beveiligingsmaatregelen, zoals IP-adrestoegangsbeperking, waarmee het risico bestaat dat iedereen met een browser en internet toegang kan krijgen tot het systeem van [naam leverancier]. Bovendien was ten tijde van het onderzoek ter plaatse de webserver geconfigureerd met beveiligingstechnieken waardoor verbindingen mogelijk zijn met een verouderd beveiligingsprotocol (SSLv3) en verouderde ciphermethoden (RC4, SHA1).

Nippon Express gebruikt voorts bij het inloggen op de website van [naam leverancier] geen meerfactorauthenticatie, waardoor een 'enigszins deskundige' derde relatief gemakkelijk toegang kan krijgen tot de identiteitsdocumenten die Nippon Express heeft gescand. Dit zijn beveiligingsrisico's.

Naar aanleiding van het onderzoeksrapport met voorlopige bevindingen heeft Nippon Express de de cryptografische bescherming van de toegang tot zijn website aangepast. Hierdoor handelt Nippon Express op dit punt niet langer meer in strijd met artikel 13 Wbp.

Nippon Express gebruikt echter geen meerfactorauthenticatie en ook geen IP-adrestoegangsbeperking, waardoor de beveiliging van de gescande identiteitsdocumenten nog steeds niet voldoet aan het vereiste van artikel 13 Wbp.

Bewaartermijn

Nippon Express gebruikt het scansysteem van [naam leverancier] voor de controle van echtheidskenmerken van de identiteitsdocumenten. Deze controle neemt enige momenten in beslag. Niet valt in te zien waarom de volledige set gescande persoonsgegevens na deze controle nog zou moeten worden bewaard. Door scans (volledige afbeeldingen) van gescande identiteitsdocumenten niet aanstonds na de controle te (doen) verwijderen (compare and forget), maar deze twintig dagen te (doen) bewaren, overtreedt Nippon Express artikel 10 Wbp.

Contactgegevens

Bezoekadres
(alleen volgens afspraak)
Bezuidenhoutseweg 30
2594 AV DEN HAAG

Let op: bij bezoek aan de Autoriteit Persoonsgegevens moet u een geldig identiteitsbewijs laten zien.

Postadres
Postbus 93374
2509 AJ DEN HAAG

Telefonisch spreekuur
Op onze website Autoriteit Persoonsgegevenspersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de bescherming van persoonsgegevens. Heeft u op deze website geen antwoord op uw vraag gevonden?
Dan kunt u contact opnemen met de publieksvoorlichters van de Autoriteit Persoonsgegevens tijdens het telefonisch spreekuur via telefoonnummer **0900-2001 201**. De publieksvoorlichters zijn bereikbaar op maandag, dinsdag, donderdag en vrijdag van 10.00 tot 12.00 uur. (5 cent per minuut, plus de kosten voor het gebruik van uw mobiele of vaste telefoon).

Persvoorlichting
Journalisten en redacteuren kunnen met vragen terecht bij de woordvoerders van de Autoriteit Persoonsgegevens via telefoonnummer **070-8888 555**.

Zakelijke relaties
Bent u een zakelijke relatie van de Autoriteit Persoonsgegevens, zoals een leverancier, dan kunt u ons telefonisch bereiken via telefoonnummer **070-8888 500**.