



Aanbeveling nr 01/2010 van 17 maart 2010

Betreft: Aanbeveling over de na te leven basisbeginselen bij het gebruik van e-ticketing door de openbare vervoersmaatschappijen (A/2010/003)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 30;

Gelet op het verslag van de heer Mertens de Wilmars;

Brengt op 17 maart 2010 de volgende aanbeveling uit:

I. Inleiding

1. Het gebruik van e-ticketing door de openbare vervoersmaatschappijen, hierna de **maatschappijen**, is een fenomeen dat gestaag toeneemt. Inderdaad, zo heeft de MIVB in het Brussels gewest in 2008 haar MOBIB-systeem in gebruik genomen en overwogen de andere maatschappijen zoals De Lijn, NMBS en TEC om binnen afzienbare tijd eveneens hun toevlucht te nemen tot deze techniek. Deze techniek maakt gebruik van een RFID-chip die bevestigd is op een plastic kaart van het eID-formaat.
2. Bovendien werd zopas een gemeenschappelijk platform voor de maatschappijen ingevoerd, met name de n.v. Belgian Mobility Card, zodat een gebruiker met één chipkaart gebruik zal kunnen maken van de diensten van de vier maatschappijen.
3. Een e-ticketingsysteem bestaat uit drie belangrijke elementen:
 - Een "klantenbestand" waarin een mogelijk verschillend aantal gegevens opgeslagen zijn betreffende de natuurlijke personen die een contract hebben afgesloten met de maatschappij onder vorm van de aankoop van één of meerdere vervoerbewijzen. Een "trajectbestand" waarin bij ieder traject door de betrokkene ten minste de valideringsgegevens van één vervoerbewijs worden opgeslagen en vaak, bij uitbreiding, de gegevens met betrekking tot dit traject;
 - Een RFID-chipkaart die de validering mogelijk maakt en die ten minste de gegevens bevat die toelaten de houder van de chipkaart te identificeren en de geldigheid van het gebruikte vervoerbewijs te controleren.
4. Deze databanken vormen het onderwerp van verschillende afzonderlijke verwerkingen die telkens verbonden zijn met verschillende doeleinden die voortvloeien uit de opdracht van algemeen belang waarmee de maatschappijen zijn belast. Uit deze verwerkingen vloeien enerzijds min of meer lange bewaringstermijnen voort in functie van het beoogde doeleinde en anderzijds worden deze gegevens ofwel als dusdanig (met andere woorden verpersoonlijkt) ofwel gecodeerd of nog geanonimiseerd gebruikt.

5. De huidige aanbeveling uit eigen beweging wil een aantal principes formuleren die moeten nageleefd worden bij de opbouw en uitwerking van een e-ticketingsysteem teneinde de privacy van de gebruikers voldoende te beschermen zonder het gewettigd belang in gevaar te brengen van de maatschappij die een dergelijk systeem wenst aan te wenden om op adequate wijze te voldoen aan haar opdracht van algemeen belang.

II. De beginselen die door een e-ticketingsysteem moeten nageleefd worden ten opzichte van de privacy

1) Toepassing van de Privacywet

6. De invoering van een e-ticketingsysteem dat werkt aan de hand van een RFID-chipkaart die persoonsgegevens bevat alsook de oprichting van klanten- en trajectdatabanken, vormen verwerkingen van persoonsgegevens die binnen het toepassingsgebied vallen van de Privacywet, wat impliceert dat de verantwoordelijke voor de verwerking al beginselen van deze wet moet naleven.

7. De gegevens die door de maatschappijen verwerkt worden in het raam van de afgelegde trajecten vormen persoonsgegevens waarvan de verwerking onderworpen is aan de Privacywet.

2) Toelaatbaarheid van de verwerking

8. Artikel 5 van de Privacywet somt de hypothesen op waarin een verwerking van persoonsgegevens mag worden uitgevoerd. De invoering van een e-ticketingsysteem zou kunnen gerangschikt worden onder de hypothese bedoeld in artikel 5, b), c) en e) aangezien dit noodzakelijk is voor het uitvoeren van een contract waarbij de betrokkene één van de partijen is, noodzakelijk is voor het nakomen van een verplichting die aan de verantwoordelijke voor de verwerking werd opgelegd door een wet, een decreet of een ordonnantie en noodzakelijk is voor het uitvoeren van de opdracht van algemeen belang waarmee de verantwoordelijke voor de verwerking is belast.

3) Anoniem reizen

9. In dit opzicht is de Commissie van oordeel dat de maatschappijen noch rechtstreeks, noch onrechtstreeks persoonsgegevens mogen verwerken die zouden toelaten het traject van de gebruikers te traceren aan de hand van hun elektronisch vervoerbewijs.

4) Finaliteitsbeginsel

10. Het finaliteitsbeginsel dat vervat is in artikel 4 van de Privacywet, legt de verantwoordelijke voor de verwerking op enkel gegevens in te zamelen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en de aldus verzamelde gegevens uitsluitend te verwerken op een wijze die verenigbaar is met deze doeleinden.

11. Na onderzoek van operationele e-ticketingsystemen is de Commissie van oordeel dat uitsluitend de volgende doeleinden kunnen beschouwd worden als behorende tot de redelijke verwachtingen van een e-ticketingsysteem dat bestaat uit de drie hiervoor vermelde elementen:

- **Het vervoerbewijzenbeheer:** onder andere het beheer ingeval van verlies of diefstal van vervoerbewijzen;
- **Het fraudebeheer:** zich ervan vergewissen dat iedere gebruiker zijn rit effectief heeft betaald en *a contrario* de gebruikers opsporen die reizen zonder behoorlijk gevalideerd vervoerbewijs;
- **Het technisch beheer:** de lezers van vervoerbewijzen detecteren die onregelmatigheden vertonen;
- **Het statistisch beheer:** volgens door de Commissie ingewonnen inlichtingen heeft dit enkel betrekking op twee aspecten, namelijk:
 - De historiek van afgesloten contracten per gebruikerscategorie;
 - De historiek van het gebruik van het openbaar vervoer per gebruikerscategorie.

12. In het raam van een coördinatie met het klantenbestand worden twee doeleinden toegevoegd, met name:

- **Het klantenbeheer:** beheer van de klantenrekeningen van de klanten die een contract met de maatschappij hebben afgesloten;
- **Direct marketing:** informatieverstrekking aan de klanten met betrekking tot de evolutie van de producten en de speciale aanbiedingen door de maatschappij¹;

5) De bewaringstermijn

13. Artikel 4, § 1, 5^o van de Privacywet beperkt de bewaringstermijn van de gegevens tot de tijd die noodzakelijk is voor het verwezenlijken van de doeleinden waarvoor de gegevens werden ingezameld.

14. Gelet op de doeleinden die redelijkerwijs door de Commissie worden aanvaard in het raam van een e-ticketingssysteem, beveelt zij de bewaringstermijn voor het verwezenlijken van deze doeleinden aan als volgt:

- **Het vervoerbewijzenbeheer:** de gegevens die voor dit doeleinde worden geregistreerd mogen niet langer dan 6 maanden bewaard worden na de vervaldatum van het laatste vervoercontract dat door de gebruiker werd afgesloten. De Commissie acht een termijn van 6 maanden redelijk voor de gebruiker om eender welke klacht met betrekking tot het gebruik van het vervoerbewijs in te dienen²;
- **Het fraudebeheer:** de gegevens die voor dit doeleinde worden geregistreerd mogen niet langer bewaard worden dan de tijd die nodig is om de fraude vast te stellen. Na deze termijn moeten de te bewaren gegevens in een bijzondere databank bewaard worden waar ze kunnen bewaard worden gedurende de tijd die noodzakelijk is voor het doorlopen van de procedure die gestart werd na een gebleken fraude.

¹ De Commissie vestigt de aandacht van de maatschappijen op de aanbeveling die zij aannam op 14 oktober 2009 betreffende direct marketing en bescherming van persoonsgegevens (nr. 04/2009) en de na te leven beginselen die zij hierin bepaalde.

² Tenzij het noodzakelijk is zich te schikken naar de verplichtingen die opgelegd worden door de wet op de handelspraktijken.

- **Het technisch beheer:** de gegevens die voor dit doeleinde worden geregistreerd mogen niet langer bewaard worden dan de tijd die nodig is om het technisch probleem vast te stellen. Na deze termijn moeten de te bewaren gegevens in een bijzondere databank bewaard worden waar ze kunnen bewaard worden gedurende de tijd die noodzakelijk is voor het doorlopen van de procedure die gestart werd na een gebleken technisch probleem.
- **Het statistisch beheer:** de gegevens mogen in het raam van dit doeleinde in geen geval als dusdanig bewaard worden. Zij moeten op een daadwerkelijk geanonimiseerde wijze bewaard worden. De bewaringstermijn van de ruwe (dus nog verpersoonlijkte) gegevens zal niet langer zijn dan de tijd die nodig is om de gewenste segmentering(en) uit te voeren. De bewaringstermijn van de geanonimiseerde gegevens is daarentegen onbeperkt³.

15. Ingeval zich een coördinatie zou voordoen tussen de databanken zou de bewaringstermijn voor de gegevens als volgt kunnen bepaald worden:

- **Het klantenbeheer:** de gegevens die voor dit doeleinde geregistreerd werden mogen niet langer bewaard worden dan 12 maanden na het verstrijken van de laatste overeenkomst die werd afgesloten door een gebruiker, op voorwaarde dat hij de chip-kaart die dienst doet als drager van de vervoerovereenkomsten heeft ingeleverd;
- **Direct marketing:** de gegevens die voor dit doeleinde geregistreerd werden mogen niet langer bewaard worden na het verstrijken van de laatste overeenkomst die door de gebruiker werd afgesloten;

³ Krachtens het koninklijk besluit van 13 februari 2001 ter uitvoering van de Privacywet moeten beschouwd worden als:

- Gecodeerde persoonsgegevens : persoonsgegevens die slechts door middel van een code in verband kunnen worden gebracht met een geïdentificeerd of identificeerbaar persoon (artikel 1, 3°)
- Anonieme gegevens: gegevens die niet met een geïdentificeerd of identificeerbaar persoon in verband kunnen worden gebracht en derhalve geen persoonsgegevens zijn (artikel 1, 5°)

6) Proportionaliteitsbeginsel

16. Het proportionaliteitsbeginsel, dat vastgelegd is in artikel 4 van de Privacywet, verplicht de verantwoordelijke voor de verwerking om voor het verwezenlijken van de beoogde doeleinden uitsluitend toereikende, ter zake dienende en niet-overmatige gegevens in te zamelen. Bij de keuze van de modaliteiten voor de verwerking die moet toelaten het beoogde doeleinde te verwezenlijken moet de verantwoordelijke voor de verwerking er eveneens over waken te kiezen voor deze die het minst ingrijpend zijn voor de privacy van de betrokkenen. Een inmenging in het recht op de bescherming van de gegevens van de betrokkenen moet inderdaad proportioneel zijn in het licht van de doeleinden van de verwerking.

17. Aangezien de bewaringstermijnen reeds hierboven werden vastgesteld, kunnen de gegevens die mogen bewaard worden als volgt gedefinieerd worden:

- **Het vervoerbewijzenbeheer:** de gegevens van het klantenbeheer en de gegevens die noodzakelijk zijn om de lopende contracten te karakteriseren;
- **Het fraudebeheer:** de identificatiegegevens van de vermoedelijke fraudeur en de reisgegevens die toelaten de fraude vast te stellen;
- **Het technisch beheer:** de identificatiegegevens van de benadeelde klanten, de betrokken contracten en de trajectgegevens die verbonden zijn met het technisch euvel;
- **Het statistisch beheer:** alle klantgegevens en trajectgegevens op voorwaarde dat deze geanonimiseerd zijn;

- **De RFID-kaart:**
 - de toegelaten zichtbare gegevens zijn beperkt tot:
 - de foto van de kaarthouder;
 - het klantnummer;
 - het technisch kaartnummer;
 - de naam, voornaam en geboortedatum van de kaarthouder;
 - de toegelaten niet-zichtbare gegevens op de chip van de kaart zijn:
 - de persoonsgegevens van de klant die noodzakelijk zijn voor zijn identificatie (bij de aankoop van het vervoerbewijs of bij een controle);
 - de laatste valideringen die noodzakelijk zijn voor een coherente en efficiënte controle;
 - de aangekochte en nog geldige contracten.

18. Ingeval een verband wordt gelegd tussen het trajectbestand en het klantenbestand, zijn de gegevens die bewaard mogen worden de volgende:

- **Het klantenbeheer:** de persoonsgegevens van de klant waaraan een klantnummer gekoppeld is;
- **Direct marketing:** de personalia van de klant.

7) Veiligheidsbeginsel van de verwerking

19. De Commissie wenst het belang te onderstrepen van de naleving van het beginsel van beveiliging van de verwerkingen van persoonsgegevens dat voorzien is in artikel 16 van de Privacywet en dat de verantwoordelijke voor de verwerking verplicht tot het nemen van passende technische en organisatorische maatregelen om de persoonsgegevens die hij verwerkt te beschermen en zich te wapenen tegen afwijkingen van het doeleinde. Het passend karakter van deze veiligheidsmaatregelen hangt enerzijds af van de stand van de techniek en de hieraan verbonden kosten en anderzijds van de aard van de te beschermen gegevens en de potentiële risico's. De maatschappijen moeten rekening houden met de "Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens" die beschikbaar zijn op de website van de Commissie⁴.

⁴ <http://www.privacycommission.be/nl/static/pdf/referencemaatregelen-vs-01.pdf>

20. Indien de maatschappijen een beroep doen op een verwerker zullen zij eveneens de bepalingen moeten naleven met betrekking tot het afsluiten van een passende overeenkomst (artikel 16 van de Privacywet). In dit raam dient de verantwoordelijkheid van de verwerker vastgelegd te worden en dient uitdrukkelijk overeengekomen te worden dat de verwerker en de personen die onder zijn gezag staan in het raam van de specifieke opdracht van onderaanneming, uitsluitend mogen optreden in opdracht van de verantwoordelijke voor de verwerking.

8) Kennisgeving aan de betrokkenen

21. Artikel 9 van de Privacywet verplicht iedere verantwoordelijke voor de verwerking om de personen waarvan de gegevens worden verwerkt in kennis te stellen over de doeleinden van de verwerking, de identiteit van de verantwoordelijke voor de verwerking en de ontvangers (of categorieën van ontvangers) van de gegevens alsook over het bestaan van een recht op toegang en verbetering van de gegevens (zie punt 24 van onderhavige aanbeveling).

9) Recht op toegang voor de betrokkenen (recht op raadpleging)

22. Krachtens de artikelen 10 en 12 van de Privacywet beschikken de betrokkenen over een recht op toegang tot de hen betreffende persoonsgegevens die werden geregistreerd, het recht om de hen betreffende onjuiste persoonsgegevens te verbeteren alsook over het recht om de gegevens te laten schrappen die, rekening houdend met de doeleinden van de verwerking, onjuist zijn of waarvan de registratie, de mededeling of de bewaring verboden zijn door de wet, of die langer dan een redelijke termijn werden bewaard.

23. De Commissie wenst eveneens dat de maatschappijen (bijvoorbeeld in de algemene voorwaarden die aan de klant worden overhandigd) het aanspreekpunt zouden verduidelijken (ten minste een telefoonnummer of een specifiek e-mailadres) waar de betrokkenen de voormelde rechten kunnen uitoefenen.

III. Besluit

24. De Commissie beschouwt de onderhavige beginselen als richtlijnen die door iedere maatschappij moeten nageleefd worden bij het uitwerken en invoeren van een e-ticketingsysteem.

Voor de Administrateur m.v.,

De Voorzitter,

(get.) Patrick Van Wouwe

(get.) Willem Debeuckelaere