COMMISSIE MEIJERS
PERMANENTE COMMISSIE VAN DESKUNDIGEN IN
INTERNATIONAAL VREEMDELINGEN-, VLUCHTELINGEN-
EN STRAFRECHT

CM1706 Note on the EU law aspects of PNR in public transport

I. Introduction

The Belgian law on the processing of passenger data (Wet betreffende de verwerking van passagiersgegevens) of 25 December 2016 does not only implement the EU PNR Directive (2016/681), but also widens the scope of the obligations on the storage and use of PNR data. The Directive only applies to air transport, whereas the Belgian law also applies to international trains, international buses and maritime transport.

A Working Group of representatives of Belgium, France, the Netherlands and the United Kingdom is exploring this wider scope also beyond Belgian territory, with the possible outcome of a binding legal instrument.

PNR data are data provided by passengers at the occasion of the reservation of a means transport (they may be provided to a travel agency, to a web based service provider – like booking.com - or directly to a carrier). PNR data are not equal to identification data (passport or ID-card, also known as API), but provide a variety of information (travel history, payment data, meals preference, accompanying travellers). Normally, the identity of the traveller is not verified by the intermediary or the carrier.

A PNR regime would normally require commercial organisations in the travel sector to collect these data and to keep them available for law enforcement purposes, under conditions aiming at the protection of the individuals' privacy. Such regime may also set rules for the access to and the use of these data by public authorities. The EU PNR Directive provides for the setting up of national Passenger Information Units (PIUs) with a central role in the latter context.

This note gives an overview of aspects of EU law that should be taken into account in case the Dutch government, be it or not together with other Member States, would consider the adoption of national law extending the scope of application of its PNR rules beyond the air transport sector, or would conclude an agreement with these Member States on this issue.

This note aims at informing the decision making process, by providing elements for a legal assessment. The note concludes that the Meijers Committee is not convinced that national instruments extending the scope of application of PNR rules beyond the air transport sector would be in accordance with all requirements of EU law. This being said, the note also specifies the main issues that should, in any event, be resolved in the decision making process.

II. Elements for a legal assessment

1. Directive 2016/681 and the scope of EU law.

    a. The Directive should be implemented by the Member States by 25 May 2018. It applies to flights to and from third countries, but allows the Member States to extend the scope of the PNR rules to intra-EU flights. However, the directive is silent about other forms of (international) traffic.

    b. The Directive finds its legal basis in the TFEU provisions on police cooperation (particularly, Articles 82 and 87). However, its content is closely related to the EU mandate on the protection of personal data (Art 16 TFEU). The Directive includes rules on the protection of personal data. Advocate-General Mengozzi even argues – in the context of an international agreement between the EU and Canada - that rules on the protection and use of PNR data should also be based on Art 16 TFEU.

    c. Arguably, all national rules on PNR (for trains, buses and boats) fall within the scope of EU law. This is not so much the result of Directive 2016/681, but because these rules fall within the scope of Art 16 TFEU, following the opinion of Advocate-General Mengozzi. The EU has a general competence on data protection (the EU lays down "the" rules on data protection) and prohibits the Member States to adopt such rules, unless this is explicitly allowed under EU data protection law. But, also in the domains where this is allowed, these national rules remain within the scope of EU law. The ruling of the Court of Justice in *Tele2 Sverige and Watson* on national rules requiring the retention of telecommunications data supports this conclusion.

    d. Arguably, EU law does, as such, not prohibit Member States to adopt rules on PNR as the recent Belgian legislation mentioned above. The rules on PNR do only cover air transport and the EU data protection legislation opens up for this type of national rules. The rules on the collection and use of PNR data can be qualified as legal ground for data processing (Art 6 of the General Data Protection Regulation) and certain other rules can be seen as derogations to data protection rules under Art 23 GDPR. Art 23 GDPR mandates Member States to adopt national rules derogating from the GDPR for certain public interests (such as combat of crime and national security). As said (at c above), these rules fall within the scope of EU law.

e. The scope of EU law is relevant, because it ensures that the EU Fundamental Rights Charter is applicable and that the stringent case law of the CJEU on the fundamental rights to privacy and data protection and on surveillance for public policy purposes can be directly applied.

f. Moreover, we should explore to what extent these rules are compliant with the free movement provisions of the TFEU.

2. Free movement and rules applicable only to trans-border transport.

a. Another relevant perspective of EU law relates to free movement in the internal market. National PNR rules applicable to trans-border transport within the EU have an effect on the free movement of persons and on the free movement of services, by subjecting cross border transit and delivery of services to preliminary requirements. These rules must be justified by a public interest and be proportional. We also refer to the directives on free movement for EU Citizens (2004/38/EC) and on free movement for services (2006/123/EC).

b. Whereas the national PNR rules applicable to trans-border transport may be justified by the public interest of the combat of terrorism, we have serious doubts about their proportionality, particularly since the rules do only apply to specific trains and buses.

c. The effect on free movement would even be more evident if these provisions would also require passengers to book trains in advance and/or to identify themselves and/or would prohibit minors to travel without parents.

d. Another complication arises when these provisions would solely apply to cross border transport. This would not only set higher standards for compliance with the free movement rules, but could also be qualified as entry and exit controls being de facto border controls within the Schengen area, which are prohibited.

e. The Belgian law of 25 December does not use the perspective of cross border transport itself, but addresses the type of service: high speed train or non-stop bus. Although this seems a different criterion, in practice these means of transport are mainly used for international transport and only cross border transport would be affected; hence the law would be an indirect obstacle to the free movement of persons, which is for EU citizens guaranteed by Article

21 TFEU.

f. Finally, a specific complexity may arise if the Member States would conclude an agreement with the UK, which would be intended to remain valid after Brexit. A specific aspect that might become relevant after Brexit is the administrative cooperation with a non EU Member State, which would require the exchange of personal data outside the EU.

3. Compliance with EU data protection law and with the Charter.

a. The PNR rules should be compliant with the General Data Protection Regulation (GDPR) (in relation to the airlines and probably the administrative bodies analyzing the data) and the Directive for data protection in the Police and Justice Sectors (2016/680/EU), as far as police or judicial authorities are concerned.

b. As said, EU data protection legislation does, as such, not prohibit this type of measures. However, storage and access interferes with EU Charter rights (Art 7 and 8 of the Charter, on privacy and data protection) and must be necessary for a public interest and be proportional. These criteria (necessity and proportionate in a democratic society) are also mentioned in Art 23 GDPR (on restrictions on data protection) and in more tailored provisions on the limitations to data protection rights in Directive 2016/680 (f.i. in Art 15 and Art 16 thereof).

c. The CJEU specified in its ruling in *Digital Rights Ireland and Seitlinger* a proportionality test. Acts must be "appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives" (at 47).

d. The CJEU distinguishes in its ruling in *Tele2 Sverige and Watson* storage of data by private companies and the access and use of the data by public authorities. Art 7 and 8 of the Charter on privacy and data protection are applicable in both stages, but the requirements are not the same. The main concerns relate to the duration of the storage, the access and use by public authorities.

4. A closer look at necessity and proportionality

This section gives some elements for a necessity and proportionality test that should be considered as part of the decision making process.

a. A proportionality test demonstrating that existing legal instruments are not sufficient.
    i. An inventory of existing legal instruments should be the starting point.
b. Necessity for a public interest.
    i. It should be demonstrated that the measure is necessary to serve a public interest.
    ii. The public interest should be specifically defined as the combat of serious crime, terrorism or in broader sense threat to national security.
    iii. It should also be defined that the public necessitates the identification of unknown suspects (cfm data retention of telecommunications data).
c. Limitations. Any legal measure should clearly delimit the impact of the mechanism on the individual whose data are processed.
    i. In principle, there should be no obligation for service providers to obtain additional data than required for commercial purposes.
    ii. Strict purpose limitation/limitation of the use of PNR data to specific crimes or threats, on a case-by-case. The purpose should be limited to terrorist-related crimes and in any event not be extended to all serious crime.
    iii. Limitation of the amount of data to be collected, excluding sensitive data (race, religion, political opinion, health, sexual life or orientation. PNR Directive, Recital 15).
    iv. Authorities should ask carriers to push (provide) the data on case-by-case basis, not pull data from databases of carriers. Authorities should not have access to those databases.
    v. A clearly limited retention period and a depersonalisation of data after

a certain period is needed. The duration of the retention period should be based on evidence.

vi. A prohibition of data mining or profiling.

vii. A prohibition of automated decisions significantly affecting citizens;

viii. appropriate mechanisms for independent review, judicial oversight and democratic control. National data protection authorities should monitor the system.

ix. Use restrictions and security requirements.

III. Conclusion

The Meijers Committee is not convinced, in view of the elements specified under II, that national instruments extending the scope of application of PNR rules beyond the air transport sector would be in accordance with all requirements of EU law. As a general point, the Meijers Committee argues that the Member States have no competence to adopt these rules under Article 16 TFEU.

In any event, before decisions on such measures are taken, the following issues should be considered:

- In order to ensure that the stringent case law of the CJEU on the fundamental rights to privacy and data protection and on surveillance for public policy purposes is respected, a privacy impact assessment should be conducted prior to the adoption of any legislative instrument. The impact assessment as foreseen by the Working Group of the four countries should contain a separate assessment on privacy, modelled along the lines of the Data protection impact assessment (DPIA) of Art 35 GDPR.
- An instrument should not be mainly directed at intra EU cross border transport since it affects the right to free movement. Such an instrument would not be proportional, unless there is compelling evidence that threats to public security are specifically caused by cross border transport. Within the Schengen area, such an instrument could easily be qualified as de facto border control.
- Art 7 and 8 of the Charter are applicable to both storage by private companies and access by public authorities. The main concerns relate to the duration of the storage, the access and use by public authorities. These concerns should be addressed.
- A necessity and proportionality test should be conducted, taking into account the

elements of Section II.4. Special attention should be given to:

- Strict purpose limitation/limitation of the use of PNR data to specific crimes or threats, on a case-by-case. The purpose should be limited to terrorist-related crimes and in any event not be extended to all serious crime.
- Limitation of the amount of data to be collected, excluding sensitive data (race, religion, political opinion, health, sexual life or orientation. PNR Directive Recital 15).
- Authorities should ask carriers to push (provide) the data on case-by-case basis, not pull data from databases of carriers. Authorities should not have access to those databases.
- A clearly limited retention period and a depersonalisation of data after a certain period. The duration of the retention period should be based on evidence provided by national authorities.
- Appropriate mechanisms for independent review, judicial oversight and democratic control. National data protection authorities should monitor the system.
- Use restrictions and security, considering the pros and cons of linking to Passenger Information Units (PIUs) as established under PNR Directive.

Reference documents:

- Directive (EC) 2004/38 of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States, OJ L 158/77.
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89.
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119/132.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April

2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119/1.

- EDPS, Opinion 5/2015, Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
- CJEU, 8 April 2014, Joint cases *Digital Rights Ireland and Seitlinger and Others*, (C-293/12 and C-594/12).
- Advocate General Mengozzi's Opinion of 8 September 2016 in the Request for an Opinion to the CJEU (1/15, PNR Agreement EU-Canada).
- CJEU, 21 December 2016, Joint cases *Tele2 Sverige and Watson a.o*. (C-203/15 and C-698/15).