12 October 2023

Constitutional Court

PRESS RELEASE
JUDGMENT 131/2023

The Court partially annuls the Law that requires the communication of passenger information, and finds it for the remainder compatible with the Constitution and with EU law provided that it is interpreted in a certain manner

The Court referred ten preliminary questions to the Court of Justice of the European Union (CJEU) as part of the examination of the action for annulment instituted by the « Ligue des droits humains » against the Law that requires the communication of passenger information.
The CJEU validated the PNR (« *Passenger Name Record* ») system, upon which the contested Law is based, as to its principle, under several reservations of interpretation.
Following that judgment of the CJEU, the Court holds that it is justified that the PNR system applies to all passengers, but that the processing of PNR data is only possible to fight terrorism and serious crime, related to the carriage in question. The Court validates several contested provisions (creation of the database, *pre-screening*, period of data retention), under reservations of interpretation. The Court annuls other measures, such as the possibility for the public prosecutor and intelligence and security services to gain access to the data. Pending legislative action, the Data Protection Authority is authorized to grant such access. The Court also annuls the provisions that lay down rules for processing API (« *Advanced Passenger Information* ») data in a single database with PNR data.

1. Context of the case

The Law of 25 December 2016 « concerning the treatment of passenger information » puts carriers and travel operators under the obligation to communicate passenger information (**PNR data**). Those data are registered in a database that is managed by the Passenger Information Unit (PIU), a body within the Home Affairs FPS. That Law transposes the PNR (« *Passenger Name Record* ») Directive (EU) 2016/681. In Belgium, the PNR system applies not only to air transport (as determined by the PNR Directive), but also to train and bus transport. The above-mentioned Law also transposes the API (« *Advanced Passenger Information* ») Directive 2004/82/EC, which requires air carriers to transfer certain data, inter alia, to combat illegal immigration and to improve border control.

The NGO « Ligue des droits humains » demands the annulment of the Law of 25 December 2016. The Court validated several contested provisions in its judgment no. 135/2019. It also referred ten preliminary questions to the Court of Justice of the European Union (CJEU) on, inter alia, the interpretation and validity of the PNR and API Directives.

The CJEU answered those questions in its judgment of 21 June 2022 (C-817/19). The CJEU validates the PNR system as to its principle, but makes several reservations of interpretation in

order to ensure the conformity of the PNR Directive with the Charter of Fundamental Rights of the European Union.

2. The Court's assessment

The Court now examines the applicant's criticisms that were not examined in judgment no. 135/2019, taking the CJEU's answers into consideration.

2.1. The right to respect for private life and the right to the protection of personal data

According to the applicant, several aspects of the contested Law violate the right to respect for private life and the right to the protection of personal data.

2.1.1. The data in question (B.24-B.34)

The applicant argues that the collection of a large number of passenger data is disproportionate. Moreover, those data might reveal sensitive information.

The Court notes that the Law of 25 December 2016 pursues an **objective of general interest, i.e. safeguarding public security**. Moreover, the collected data are clearly identified and the operators and carriers already have them in principle; they must relate to a specific journey and be limited to the fight against terrorist offences and serious crime; lastly, it is guaranteed that sensitive data are not collected or retained. However, just like the CJEU, the Court specifies that **certain data** (address and contact information, payment information, information on unaccompanied minors) **must be interpreted restrictively**. Furthermore, the Court accepts the collection of data regarding the seat number and items of luggage. With those interpretations, the Court concludes that the applicant's criticisms are unfounded.

2.1.2. The concept of « passenger » (B.35-B.41)

The applicant criticizes the broad nature of the concept of « passenger », resulting in the systematic non-targeted automated processing of the data of all passengers.

The Court observes that the collection, transfer and processing of PNR data applies to each passenger, whether he committed an offence or might commit one, and whether he crosses the EU's external borders or not. The CJEU has held that **the extension of the PNR system** (which, in principle, only applies to flights crossing the EU's external borders) **to intra-EU flights is admissible provided that a present, genuine and foreseeable threat exists, which is assessed periodically by an independent body**. On those grounds, the Court considers that the terrorist threat was genuine and present when the Law was adopted and that this still is the case today, with regard to Belgium's central geographical situation and the many European and international institutions it accommodates. The Court specifies that **the legislator will have to review the Law periodically on the basis of the CUTA's threat assessment**, and that the first review should take place within three years at the most. Considering, among other things, that obligation to conduct a review, the criticisms are unfounded.

2.1.3. The purposes of PNR processing (B.42-B.56)

The applicant argues that the purposes of PNR data processing go beyond what is « strictly necessary ».

The CJEU has accepted the collection and processing of PNR data, but **only to fight terrorism and serious crime and only if there is an objective link, even if only an indirect one, with the carriage in question**.

The Court finds that some processing purposes concern serious crime, that they are clearly defined and limited to what is strictly necessary. The Court notes that other purposes are added to the purposes set out in the PNR Directive :

- The **purpose of « preventing serious offences against public security as part of violent radicalization »** is admissible provided that it is interpreted in the sense that it is strictly limited to fighting terrorism and serious crime and that it has an objective link, even if only an indirect one, with the carriage in question.

- As to the **purpose of « monitoring intended activities by the intelligence and security services »**, the Court observes that those services' missions are not limited to preventing terrorist offences and serious crime and that that purpose does not have an objective link, even if only an indirect one, with the carriage of passengers. That purpose **exceeds the limits of what is strictly necessary and must be annulled**.

- In its judgment no 135/2019, the Court accepted the processing of PNR data **in order to improve checks on persons at external borders and to combat illegal immigration**. The Court concludes that the CJEU seems to exclude this. The Court finds, however, that it cannot reconsider a final decision. Therefore, the legislator must harmonize the contested Law with the CJEU's judgment on this point. The Court specifies, though, that it will examine the criticism raised against the processing of API data further down (see below, point 2.2).

2.1.4. The management of the passenger database and the processing of data as part of the advance assessment of passengers and ad hoc searches (B.57-B.70)

The applicant criticizes the creation of the passenger database and its management by the PIU. The applicant also criticizes the connection between the databases and the *pre-screening* method and the possibility for members seconded from the competent services to rule on a request for individual access within the scope of ad hoc searches.

The Court notes that the CJEU makes the validity of the PNR Directive subject to the observance of several safeguards. As a result, the Law of 25 December 2016 must be interpreted in the sense that it contains those safeguards, and the PIU and the competent authorities will have to ensure the observance of those safeguards.

According to the Court, **the creation of a passenger database**, under the PIU's responsibility, is an essential element of the PNR system. Members of staff seconded from the VSSE (State Security) and from the police and the intelligence and security services perform their duties only under the authority of the PIU's leading officer. As a result, the PIU offers safeguards regarding expertise and independence and has the powers required to pursue only the purposes set out in the PNR Directive. The Court concludes that the measure is not disproportionate.

As regards **the advance assessment of the risk posed by passengers (*pre-screening*)**, the Court specifies that PNR data can technically only be cross-checked against databases on persons or objects sought or under alert, that those databases must be used in a non-discriminatory manner by the competent authorities, and only within the framework of terrorism and serious crime related to the carriage of passengers. The formulation of

pre-determined criteria is subject to the same limitations. The Court specifies that the PIU is not allowed to use artificial intelligence technology in self-learning systems (*machine learning*), capable of modifying without human intervention or review the assessment process. Finally, in case of a positive match (*hit*), the PIU's individual **review** must be carried out within 24 hours following clear and precise rules that guarantee a uniform administrative practice that ensures compliance with the preceding rules.

To conclude, the Court specifies that the persons involved must be informed in order to be able to decide whether to lodge a judicial appeal or not.

With regard to **ad hoc searches**, enabling the public prosecutor and intelligence and security services to gain access to passenger data, the Court holds that the members of the PIU exhibit sufficient safeguards of independence to rule on requests for access. However, the Court annuls the possibility for intelligence and security services to conduct ad hoc searches to monitor their activities, because that purpose exceeds the requirements of what is strictly necessary, as mentioned in point 2.1.3.

The CJEU has held that the communication of PNR data can only be decided on the basis of new circumstances and objective material with a view to fighting terrorism and serious crime related to the carriage of passengers. According to the Court, the Law of 25 December 2016 must be interpreted in the same way. The CJEU has also held that the communication of PNR data must be authorized by a court or by an independent administrative authority other than the PIU, following a reasoned request by the competent authorities. The Court finds that neither the public prosecutor nor the competent customs officer are independent national authorities. The Law must therefore be annulled as it fails to designate the independent body that is in charge of that prior review. Pending the designation of that independent body by the legislator, the Data Protection Authority may perform that duty. The provision in question may therefore continue to apply on the basis of that interpretation.

2.1.5. The period of PNR data retention (B.71-B.75)

The applicant argues that it is exorbitant to retain the data for a period of five years.

According to the CJEU, it is justified to retain PNR data on all passengers for an initial period of six months, but not beyond that period. Beyond that period of six months, only data regarding persons presenting a terrorist or serious criminal risk related to the journey may be retained.

According to the Court, the contested provision can be interpreted in the sense that, **after six months, only the data of persons presenting a risk are retained for a period of five years, whereas other data must be deleted**. On the basis of that interpretation, the Court rejects the applicant's criticism.

2.2. The freedom of movement for persons within the European Union (B.76-B.79)

The applicant is of the opinion that the contested provisions, by extending the PNR system to intra-EU flights, indirectly reintroduce border controls that would breach the freedom of movement for persons guaranteed under European law.

As mentioned in point 2.1.2, the Court, taking the CJEU's judgment into consideration, observes that the genuine terrorist threat justifies the PNR system's application to several means of transportation within the Union's borders. For similar reasons, the Court finds that the limitation of the freedom of movement, to which the Law of 25 December 2016 would lead, is justified.

According to the CJEU, the possibility to include API data among PNR data does not alter the fact that the API Directive does not apply to intra-EU flights. The processing of API data may only concern passengers crossing the EU's external borders. The CJEU holds that PNR data, given the exhaustive nature of the purposes set out in the PNR Directive, may not be retained in a single database that may be consulted both for those as well as other purposes.

The Court concludes that, given the existence of a single database containing both PNR and API data, it is not possible to interpret the Law of 25 December 2016 on that subject in accordance with EU law. **The Court therefore annuls the provisions that authorize the processing of API data within the framework of the PNR system for intra-EU flights**, as they relate to intra-EU flights. The Court also annuls the purpose of improving checks on persons at external borders and combatting illegal immigration, which is inseparable from the annulled provisions. The legislator must organize the collection of API data in a database that is distinct from the PNR database and under conditions observing the API Directive.

3. Conclusion

The Court annuls several provisions as mentioned above. It specifies that those annulments result in the fact that data processing operations on the basis of the annulled purposes or data transmission without prior review must be regarded as illegal, but that this partial annulment does not affect other processing operations of passenger data. The Court rejects the appeal for the rest, under the reservations of interpretation mentioned above.

The CJEU's judgment implies that it is not possible to maintain the effects of the annulled provisions on a temporary basis. The Court specifies that the competent criminal court, if the occasion arises, must give a verdict on the admissibility of evidence that was gathered during the execution of the annulled provisions, in accordance with the applicable rules of criminal procedure and in light of the CJEU's explanations.

The Constitutional Court is the court that watches over the compliance with the Constitution by the various legislatures in Belgium. The Court can annul, declare unconstitutional or suspend laws, decrees or ordinances for violating a fundamental right or a rule on the division of competences.

This press release, drafted by the Court's media unit, is not binding on the Constitutional Court. The text of the judgment is available on the website of the Constitutional Court.

Press contact : Tim Souverijns | 02/500.12.21 | Thomas Leys | 02/500.12.60 | Martin Vrancken | 02/500.12.87 | Romain Vanderbeck | 02/500.13.28

Follow the Court on Twitter @ConstCourtBE