BRIEFING

Implementation Appraisal

European Parliament

Revision of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data

This briefing is one in a series of 'implementation appraisals', produced by the European Parliamentary Research Service (EPRS), on the operation of existing EU legislation in practice. Each briefing focuses on a specific EU law, which is likely to be amended or reviewed, as envisaged in the European Commission's annual work programme. 'Implementation appraisals' aim to provide a succinct overview of publicly available material on the implementation, application and effectiveness to date of an EU law, drawing on input from EU institutions and bodies, as well as external organisations. They are provided by the EPRS Ex-Post Evaluation Unit, to assist parliamentary committees in their consideration of new European Commission proposals, once tabled.

SUMMARY

The advance passenger information (API) system dates back to 2004, when the Council adopted Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data to improve border control and fight against irregular migration (the 'API Directive'). New data sharing schemes have since been developed to improve EU border control and migration management and, specifically, fight terrorism and serious crimes. Today, air carriers are required to transfer not only API but also passenger name records (PNRs) in line with Directive (EU) 2016/681 of 27 April 2016 on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (the 'PNR Directive'). PNRs comprise a larger set of data that encompass API.

To improve coherence in EU legislation and support harmonisation between Member States, the API Directive might be aligned with the PNR Directive. The European Commission's counter-terrorism agenda for the EU, adopted on 9 December 2020, announced that the proposal to revise the API Directive may consider providing for the use of these data for countering serious crime, improving the effectiveness in the use of API data and the coherence with other instruments such as the entry/exit system, the European travel information and authorisation system, and the PNR system. However, it raises questions as regards data protection and the right to privacy.

In its 2022 work programme, the Commission stated its intention to revise the API Directive. Initially planned for the second quarter of 2022, the revision was postponed to the last quarter of 2022. This implementation appraisal looks at the practical implementation of the directive in light of the expected Commission proposal for its revision.

Background

Advance passenger information (API) data is biographic information on passengers collected by air carriers during check-in for transmission to the border control authorities of the country of destination. The processing of API data enables advance checks of air travellers – the authorities' screening of passengers' data while in-flight (or shortly before) for the purposes of border control.

EPRS | European Parliamentary Research Service

Author: Marie-Astrid Huemer

Ex-Post Evaluation Unit

PE 734.699 – December 2022

EN

The transfer of passenger information data to border authorities is governed by Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (the 'API Directive'). Its main purpose is to improve an effective border control and combat illegal immigration.

API is distinct from passenger name record (PNR) data. PNR data are unverified information provided by passengers and collected by air carriers or travel agencies during the flight booking process to enable reservation and check-in processes. In addition to biographic data, PNR include travel-, itinerary-, and modes of payment-related information.[1] Initially, PNR were to facilitate the exchange of booking information between airlines for purposes other than law enforcement.[2] In 2016, after five years' negotiations between the co-legislators, Directive (EU) 2016/681 on the use of PNRs (the 'PNR Directive') was adopted for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Air carriers collect PNR data from passengers on international flights – or, in some cases, intra-EU flights[3] – and transmit them to passenger information units (PIUs), operated by national police forces, for a preliminary assessment.[4] According to Article 6(3) PNR Directive, PIUs can '(a) compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such databases; or (b) process PNR data against pre-determined criteria'. They can be kept for more thorough examination by relevant authorities if necessary.[5]

Legal framework

In the aftermath of the Madrid terrorist attack,[6] the Council adopted a declaration on combatting terrorism, in which it recommended expediting work on a series of measures; these included the proposed Council directive on the obligation of carriers to communicate passenger data. As a result, the directive was adopted without consultation of the European Parliament.[7]

The explicit aim of the API Directive is to **improve border control and combat illegal migration** (Article 1). The directive builds on Articles 62(2)(a)[8] and 63(3)(b)[9] of the Treaty establishing the European Community.[10] It lays down complementary obligations to those already imposed on carriers by Article 26[11] of the 1990 Schengen Convention implementing the Schengen agreement of 14 June 1985, and its subsequent complementary rules.[12] However, the 2004 circumstances and the explicit reference to the declaration on combatting terrorism, together with the possibility for implementing countries to use the data for law enforcement purposes (Article 6(1)) underlined a more general objective of enhancing security of EU citizens.

The directive applies to all EU Member States, including those that do not apply fully the Schengen *acquis*[13] and the Schengen-associated countries.[14] Despite initial delays to date, the directive has been transposed in all countries.

The directive sets up **minimum standards for the collection** and **processing** of passengers data. In line with Article 3(1), Member States are required to establish an obligation for air carriers to transmit, at the request of border control authorities, information concerning the passengers about to cross the EU external border. A list of mandatory information must be transferred shortly prior to take-off. Despite the carriers' obligation to transfer data on request, state authorities are not obliged to make such a request.

The air carriers' obligation is defined in sufficiently loose terms for implementing countries to enjoy **wide discretion** when deciding on their implementation law. They may specify the scope of application and the data to request; whether that data will concern only flights landing in the main airports or in all airports, only for in-bound flights or also for out-bound flights; and if data must be requested in relation to flights arriving from a third country into the Schengen area or also in relation to intra-Schengen flights or even domestic ones. Combination of flights entering or exiting the Schengen area are multiple, and the control of their passenger data is ultimately left to the implementing countries' policy choice. The same discretion is used for deciding which carriers are required to respect the obligation, for requesting more information than that listed in Article 3, and even for adopting rules that go beyond EU minimum rules.

As regards **processing of data**, the relevant authorities are required to save the data temporarily before deleting them within 24 hours after their transmission, and once the passengers have entered the country's territory. Likewise, carriers must delete data within 24 hours of the aeroplane's arrival. In line with their national law and subject to EU data protection rules,[15] border authorities are authorised to derogate from the 24-hour-retention rule only when data are needed for the exercise by border authorities of their statutory functions. By contrast, the directive does not specify conditions and safeguards for such processing when data are needed for law enforcement purposes. This use is an extension of the 'purpose limitation' principle, according to which data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'.[16] API data are not only collected to improve border control and fight against irregular migration but might, beyond that, be collected for law enforcement purposes; this has raised concerns regarding the implementation of the strict 'purpose limitation' principle.[17]

Dissuasive, effective and proportionate **sanctions** are required and must be applied against carriers that do not transfer passenger data by fault, or transfer incomplete or false data. In line with Article 4, the penalties must be within a range of between a minimum of €3 000 and a maximum that must not be less than €5 000. Again, implementing countries may go beyond that and apply additional and more severe sanctions such as immobilisation, seizure and confiscation of the means of transport, or temporary suspension or withdrawal of the operating license.

European Commission reports and consultation activities

European Commission inception impact assessment

On 5 June 2020, the Commission published an inception impact assessment (IIA), offering insight into its views on the scope of the revision, the policy options and their expected impacts. The IIA was followed by 12-week public consultation, the results of which will feed into the evidence-based analysis and complement data collection in support of the forthcoming revision. As a general objective, the revision will ensure that the collection and processing of API data is more effective and consistent with other EU instruments. This implies, in particular, that the legislation is revised taking full account of EU border and migration laws, interoperability,[18] and law enforcement and data protection rules.

The policy options will have to address the nature and scope of data to be collected and processed. The revised directive will have to propose a framework so the best technical solutions are set up with a view to improving the quality and reliability of data; similarly, the interoperability of information systems relevant for EU security and border control must be improved to the point that there are minimal or no overlaps. The IIA notes that the nature of the revision, i.e. whether it should be a regulation or a directive, will be addressed separately.

Stakeholder consultations

In the seven contributions received as feedback from public bodies, non-governmental organisations, and companies, the following issues arose:

- The scope of data needs clarification, to comply with data protection rules and pass the test of necessity and proportionality. Some stakeholders suggest including crew data and/or expanding data collection; however, they express reservations as regards extending data collection to all flights, as this might be contrary to the free movement of EU citizens. The Community of European Railway and Infrastructure Companies (CER) expresses serious doubts as to the expansion towards the railway sector (see also Court of Justice of the EU below). Moreover, some stakeholders stress the detrimental economic, social and environmental impacts on companies and passengers without clear and proportionate security improvements.
- There are concerns as regards inconsistencies with other EU rules, and the use of API under the PNR Directive for law-enforcement purposes. The harmonisation between both directives raises concerns, as well as triggering calls for clarifying the exact scope

of application of both texts. There are also questions on the impact on passenger flows and additional costs, in particular for transporters.

- Efforts are needed when using available technologies, such as the extended use of interactive API (iAPI) and/or establishing a single window whereby API and PNR data would be collected centrally and trigger a single aggregated response back.

European Commission evaluation report

In 2020, the Commission concluded its second evaluation of the API Directive and its implementation. The results of the first evaluation from 2012 served as baseline. At the time, the main challenges to a smooth implementation were deemed to be technological. Today, after 15 years' implementation, the main objective is to assess whether the directive is still fit for purpose, considering legal and technological changes. In particular, with the 2016 PNR Directive, the development of large-scale data bases and their interoperability, questions on overlap, added value and data protection requirements arise. The evaluation relies on the findings and recommendations of an externally contracted study published in February 2020, which covers the period from 2012 to 2019. There were challenges in implementing a methodology where quantitative and qualitative data ensure an evidence-based assessment; quantitative data were not available. Another weakness is the lack of both literature on the specific question and of preparatory documents, since the directive had to be completed urgently. However, other sources were used, including primary data, multiple and comprehensive consultations of stakeholders and proxy data.

Effectiveness of the directive was assessed positively in 2012 and in 2019. The analysis stressed **enhanced border control**. Border authorities are in a better position to verify and identify in advance those passengers and/or documents for which a second check is necessary, including those posing security risks. Likewise, border authorities may **combat irregular migration** more effectively by identifying irregular migrants such as those destroying their travel documents after boarding with the hopes of entering the country without immediate forced return. Passengers and migratory flows have increased, so authorities are obliged to cross check ever-increasing amounts of data. The API system (APIS) was nonetheless deemed relevant and effective in strengthening their response capacity.

However, as effective as it may be, APIS faces **obstacles**. As suggested, some are due to differences in national implementing rules, which are challenging for carriers. Technological changes such as self-check-in, whereby risks of unverified data increase, represent new obstacles. Questions also arise around the nature of data to be analysed, and the 24-hour-retention time, which could be insufficient in certain cases to ensure an effective control. The distinct use of API and PNR is said to minimise API added value while creating confusion among stakeholders. The APIS had an **impact** on carriers, national authorities and passengers. Most carriers had to bear additional costs. The reduction in border-crossing time allowed by APIS is only partial; this is, however, due to other factors.[19] It also seems that passengers do not perceive the issue of data transmission as a problem in itself.[20] National authorities, for their part, recognise that they benefit from a greater capacity for control, detection and investigation.

On **relevance**, the evaluation concluded that the directive still responds to the countries' needs – better border control and combatting irregular migration remain high on countries' political agenda. Moreover, some countries stressed the benefit of the APIS for law enforcement purposes, particularly in fighting terrorism. Relevant authorities concurred in acknowledging a further need of API data in view of the internationalisation and professionalisation of transnational criminal groups.

Table 1 – Potential benefits of the APIS

Potential benefits of the APIS according to stakeholder	
National authorities	- Advance screening of passengers facilitates identification of those posing risks or problems - Enhances authorities' enforcement capacities - Allows faster clearance and flow of low risk passengers - Enables more effective allocation and management of human and financial resources
Carriers	- Enhances carrier security - Lowers risks of having passengers without valid official travel documents - Reduces carriers' exposure to penalties in cases of passengers without valid travel documents - iAPI enables a carrier to refuse boarding and avoid assuming responsibility and associated costs for detention/return at arrival
Passengers	- Reduces waiting time on arrival at border-crossing point

Data source: Commission evaluation, 2022.

As regards **efficiency**, the assessment relies mainly on authorities' and carriers' consultation.[21] **National authorities** continue to viewed costs/benefits positively, despite significant differences between the amounts allocated to the APIS across implementing countries.[22] National authorities budgeted the setting up of the system, and continue to allocate resources for its maintenance and other staff/running costs on a yearly basis; these expenses are deemed necessary and beneficial in view of the positive impacts on border control and fight against irregular migration. Some countries reported more arrests / increased detection of irregular migrants as a direct result of implementing the APIS. **Carriers** came to the opposite conclusion, since the obligation imposed to them was costly, without having any direct and quantifiable commercial benefit. They noted that the money invested would have been used for commercial purposes had the directive not been adopted. Firstly, they had to set up or adapt their IT infrastructure for the collection and transfer of API data. Secondly, they needed to cover non-compliance costs in cases of judicial proceedings and sanctions. Current implementation of the APIS is not viewed differently, in that it still does not bring benefits to carriers; additionally, carriers pointed to the national differences that cause uncertainties and further risks of non-compliance. Stakeholders noted that costs might have been reduced if standardised requirements and other technological solutions such as centralised routing mechanisms[23] had been adopted.

Coherence is assessed at national, EU and international levels.

1 At national level, objectives of national APIS are to some extent coherent with those from the directive – their aim is to enhance border control and fight irregular migration. However, the wide discretion left to implementing countries on few key provisions resulted in multiple systems. As said before, the use of data for law enforcement purposes, and the nature and scope of data collected, vary as much as the type of technologies selected by implementing countries.

2 At EU level, EU legislation has introduced important changes that resulted in inconsistencies, including after the establishment of various databases applicable to border management (2.1) and law enforcement (2.2), all of them calling for data protection rules (2.3).

2.1. Border management

Controls used to be based on a rapid and straightforward verification of the validity of travel documents at border-crossing points. In 2017, Regulation (EU) 2017/458 on the reinforcement of checks against relevant databases at external borders (the 'Systematic Check Regulation') amended the Schengen Borders Code by extending systematic checks to all EU citizen, including a check against other EU databases.

Most countries verify documents against Interpol's stolen and lost travel documents database (SLTD) and the Schengen information system (SIS[24]). An advance check using API is reportedly less frequent, making complementary verifications almost inexistent. The use of API against the visa information system (VIS[25]) is reportedly even less systematic. Moreover, the new entry/exit system (EES[26]) and the European travel information and authorisation system (ETIAS[27]), interlinked with VIS, are about to become operational. The ETIAS/EES central systems capture personal data from travel document(s); the carrier must send a query to determine if the traveller is entitled to board. This query contains (nearly) the same data as those received under the APIS. The carrier industry calls this query an interactive API (iAPI). A question arose as to the possibility of establishing a central routing mechanism where all data[28] could be forwarded to various destinations for analytical purposes. Although this technology could facilitate data processing and interoperability, some countries stressed financial costs and existing limits in the analytical capacity of such a system. These difficulties may justify that the APISs are maintained even though many data collected are identical, giving the impression of redundant systems.

2.2. Law enforcement

The API Directive is not fully consistent with the PNR Directive. The collection of data does not relate to the exact same set of data. The PNR Directive requires air carriers to transfer API data, in addition to a longer list of data. The scope of application differs as well, and data might be collected for different types of flights under both texts. In terms of law enforcement purposes, both directives are not identical either. The terms are explicit in the PNR Directive, adopted for 'the prevention, detection, investigation, and prosecution of terrorist offences and serious crimes'; this corresponds to a strictly defined list of offences. By contrast, the API Directive does not include a definition of 'law enforcement purposes', leaving the implementing countries to define them more broadly. Finally, the PNR Directive applies only to EU Member States and not to Schengen countries.

2.3. Data protection framework

The data protection rules referred to in the API Directive are still the same as those of the 1995 Data Protection Directive, which applied until 25 May 2018, when it was replaced by the General Data Protection Regulation ('GDPR'). In line with the GDPR, collection of data is still authorised under strict conditions of necessity and proportionality to the purposes for which data are collected. The lack of a precise definition of law enforcement purposes leads to uncertainty in that regard. The 24-hour-retention time limit is deemed proportional and justified by the necessity of border control. However, possible derogations for the exercise of statutory functions, as well as the right to retain data beyond 24 hours, lack precisions. Since 2016, Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by law enforcement authorities (the 'Police Directive') also requires time limits in various situations.

3 At international level, consistency with international rules is relevant in that the establishment of national APISs became an International Civil Aviation Organization (ICAO) standard.[29] The United Nations (UN) adopted several resolutions, calling on its member states to set up and use APISs to help fighting terrorism.[30] In Europe, ministerial Council Decision 6/16 of the Organization for Security and Co-operation in Europe (OSCE) affirms OSCE participating states' commitment to establish national APIS as well. Yet, data requested under the international regulatory framework and by the international aviation community[31] are more detailed, and there could be inconsistencies. Since not all flights are covered by EU legislation, efforts to cross-check data and coordinate at international level might be affected negatively.

Regarding **EU added value**, many implementing countries established an APIS as a result of EU requirements, and would not have done so otherwise. EU-level intervention presumably allowed

economies of scale where a solely national initiative to set up an APIS may have been much more costly. Although migratory flows do not affect EU Member States equally, the improvement of border control benefited all of them, and could not have been achieved without EU level action. This is all the more true as international rules did not require such a system when the directive was transposed but came much later. However, the fact that countries were given a broad margin of appreciation of their operational, organisational and technological models has weakened the impact of the APIS more broadly.

European Parliament position / MEPs' questions

European Parliament resolutions

API data are mainly mentioned in relation to security issues. On 11 February 2015, in its resolution on anti-terrorism measures, the Parliament calls on Member States to make optimal use of existing platforms, databases and alert systems at European level, such as the SIS and the APIS. In its 17 December 2020 resolution on the EU security union strategy, the Parliament stresses that the API Directive has contributed to more efficient border controls and the identification of people posing security threats; it expects the announced revision to be accompanied by a thorough impact assessment, including fundamental rights implications. Parliament has been aware of the need for improvements. In its decision of 13 May 2020 on discharge in respect of the implementation of the eu-LISA budget,[32] it observes 'the possible development of a centralised router for the exchange of API and PNR information among Member States; notes that the use of such information for checks against large-scale IT systems has been proposed as an element of interoperability of future interest'.[33]

MEPs' questions

Written question to the Council by **Nicola Caputo (S&D, Italy), 3 March 2016**

In his question, the Member stressed the inability of surveillance to prohibit terrorist attacks in Brussels and Paris, and argued that the PNR system would not improve this incapacity. The Member therefore asked the Council if an integrated solution of API and PNR data should be preferred instead of creating another structure, which would not be in line with fundamental citizens' rights.

Written answer by the Council, **16 September 2016**

In its reply, the Council pointed out that Member States already use these PNR data. It stressed that the purpose of the API Directive was to harmonise Member States' legal provisions at EU level.

Written question to the Commission by **Josu Juaristi Abaunz (GUE/NGL, Spain), 26 November 2015**

The Member reported that the Spanish Interior Ministry is storing personal data of travellers beyond the 24-hour limit. The Member asked if the Commission is aware of that, and if an investigation has already been started, given that Article 6 of the directive prohibits this practice.

Written answer by **Mr Avramopoulos on behalf of the European Commission, 16 June 2016**

The Commission pointed out that the supervision and enforcement of data protection rules falls under the competence of the national Data Protection Supervisory Authority and courts. It stressed that Article 6(1) of the directive allows the storage of data after the 24-hour limit when needed for statutory functions of the authorities responsible for external border checks. Additionally, API data can also be used for law enforcement purposes. Both cases have to be in accordance with national law and subject to data protection provisions under the Data Protection Directive 95/46/EC.

Council of the EU

In in its 2021 conclusions on the expansion of PNR data transfers with third countries, the Council highlighted the importance of PNR data to secure public safety. From the Council's perspective, PNR data play an important role in the fight against organised crime, and can be used as an effective tool

to prevent terrorism travel and facilitate border control. It nevertheless acknowledged shortcomings of agreements, as pointed out by the Court of Justice's opinion 1/15 on the draft agreement between Canada and the EU. Thus, the **focus on the EU Charter of Fundamental Rights** remains most important.

Tendencies to widen the exchange scope of API and PNR data can be traced back to the Council conclusions of December 2019. The conclusions go beyond the extension of data use in cooperation with third countries, and focus on the collection of passenger-related data for other forms of transport at EU level. The Council emphasised again the significance of API and PNR data to combat terrorism and serious crime in effective and targeted way. Nevertheless, it noted that API and PNR data collection has to be treated as sensitive concerning fundamental rights. It therefore requested an impact assessment from the Commission to investigate possible effects of such an extension.

EU Agency for Fundamental Rights

The harmonisation of EU rules may imply **facilitated access and use of API data for law enforcement purposes**, and consistent use of border management mechanisms. The Fundamental Rights Agency (FRA) conducted several analyses that touch precisely on those matters.[34] In its 2018 report, 'Under watchful eyes – biometrics, EU IT-systems and fundamental rights', FRA analysed how such an access may put at risk fundamental rights of data protection and privacy. Interoperability between IT databases could weaken the purpose limitation principle.[35] On the one hand, the use of IT systems is optimised for combatting irregular migration, serious crimes and terrorism, and on the other, this optimisation might enable the use of data for purposes not initially envisaged, personal data stored in one system being used across all systems to ensure identification of a person.[36]

In the same year, in its opinion on interoperability and fundamental rights implications,[37] FRA underlined that 'next to the immediate fundamental rights concerns resulting from the interoperability proposals, there are also possible **longer-term implications** … [T]he European Commission indicated that decentralised EU systems – such as those operating under the … PNR – may at a later stage be included in one or more of the interoperability components, should its necessity be demonstrated. Therefore, the design of interoperability must already now take into account any possible future expansion of the set of data covered and its potential impact on fundamental rights.' If this were the case, the remark applies to API **from the moment it is aligned with the PNR**.

Court of Justice of the EU

On 21 June 2022, on a reference for preliminary ruling on transposition of the PNR and the API Directives into national law, the Grand Chamber of the Court of Justice of the EU (CJEU) clarified key points. Whereas the judgment concluded that the PNR Directive was compliant with the fundamental rights of privacy and data protection, some of its points echo concerns raised by the Council of Europe.

According to the CJEU, the PNR Directive entails undeniably **serious interferences** with Articles 7 (respect for private and family life) and 8 (protection of personal data) of the EU Charter of Fundamental Rights ('the Charter'), in so far as it seeks, inter alia, to introduce a **surveillance regime that is continuous, untargeted and systematic**,[38] including automated assessment of the personal data of everyone using air transport services.[39] Moreover, there is a large margin of error.[40] However, Articles 7 and 8 are not absolute rights.[41] After examining whether the conditions to derogate or limit the exercise of such rights are fulfilled, i.e. whether they are **legal**, strictly **necessary** to reach the objective of **public interest** pursued, and **proportionate** to the need of that objective,[42] the CJEU concludes that the interferences the PNR Directive entails do not affect the essence of those rights adversely.[43]

According to the CJEU, the **purposes** of preventing, detecting, investigating and prosecuting terrorist offences and serious crime undoubtedly constitute objectives of general interest, which may justify even those serious interferences. This is justified in the point where the CJEU, referring to existing errors,[44] concludes that 'they are not capable, however, of rendering the said system

inappropriate' for pursuing the objective of combatting terrorism and serious crime, and 'that automated processing carried out …have indeed already made it possible to identify air passengers presenting a risk'. For the CJEU, the PNR system's appropriateness essentially depends on the proper functioning of the subsequent verification over the results by non-automated means.

To determine whether the interferences are **necessary**, the CJEU concludes that the nature and scope of data are of a sufficiently clear and precise nature overall.[45] It is then for the Member States to ensure that the application of the directive is effectively limited to combatting serious crime, and does not extend to offences that amount to ordinary crime. It may also be deemed strictly necessary for Member States to apply the PNR system to all or some specific intra-EU flights, providing that conditions defined by the directive are complied with.

When it comes to **data processing**, PIU must ensure the non-discriminatory nature of automated processing operations. The CJEU underlines that, if a positive match ('hit') results from the advance assessment by automated means, 'the PIU is to carry out an individual review by non-automated means', and transfer data only if there is reasonable suspicion of involvement in terrorist offences or serious crime. The relevant authorities must 'give preference to the result of the individual review conducted by non-automated means by the PIU'. For the CJEU, national supervisory authorities and courts will supervise the implementation of such processes so that data subjects may seek legal remedies, whereas lawfulness of automated processing must be open to review by the data protection officer and the national supervisory authority.

As regards **data mining** and risks of profiling beyond what is pursued by the PNR Directive, the CJEU concludes that the rules allow the rights and obligations of the relevant authorities to be strictly applied, and that databases against which search is conducted are clearly identified.[46]

Regarding **pre-determined criteria** used in the advance assessment of PNR data, the CJEU interprets the directive as not allowing the use of artificial intelligence in their definition, insisting that those criteria must be determined in such a way as to target specifically individuals who might be reasonably suspected of involvement in terrorist offences or serious crime.[47]

Regarding the disclosure and processing of PNR data for the purposes of their subsequent assessment after six months, the CJEU deems the terms and conditions of the directive sufficient safeguards. On the question of disclosure of PNR data to intelligence services within the remit of their monitoring activities, which were said to be part of the prevention activities conducted by intelligence services, the CJEU notes that it is up to the national court to assess if intelligence services are competent to conduct such prevention activities. On a principled base, the CJEU reiterates the exhaustive nature of the purposes of the PNR Directive.[48]

As regards the **retention period**, the CJEU clarifies that 'the continued storage of the PNR data of all air passengers' after the initial period of six months (within PIU) goes beyond what is strictly necessary, although it seems permissible to store them beyond that initial period only in so far as, in specific cases, there is objective evidence that certain passengers may present a risk that relates to terrorist offences or serious crime. However, a general retention period of five years for PNR data, applicable indiscriminately to all passengers, is liable to infringe the limitation on retention period.

As regards **intra-EU flights**, the API Directive must be interpreted as not applying to intra-EU flights. The differences in objectives between the API and the PNR Directives prevent all data from being collected and processed in the same way.

Council of Europe

The Council of Europe (CoE) mainly examined questions around the use of PNR from the **personal data protection angle**. In view of considerations for aligning the API and the PNR Directives, warnings from the CoE on risks of misuse of PNR deserve special attention.

In 2015, the Consultative Committee ('the Committee') of the CoE Convention for the protection of individuals with regard to automatic processing of personal data[49] issued a report on passenger name records, data mining and data protection, calling for strong safeguards. The report analysed

the context and the mechanisms that led to an increasing use of information systems to collect and process data such as PNR for security purposes. While acknowledging the legitimacy of the objectives, the report detailed the risks of misuse associated with this collection and transfer of data between state authorities. These risks include processes of **data mining**[50] and **profiling**[51] that may lead to the identification of potential suspects through 'smart algorithms'. However, algorithms often lead to what specialists call 'false positives', meaning hypothetical suspects identified through data cross-checking that prove wrong in the end, once human verification is completed. The report insisted on the lack of data to demonstrate and quantify the number of suspects that would consequently have been identified out of legitimate concerns. It called for strong safeguards for data protection and for reducing the use of such data processing for unclarified law purposes.

On 19 August 2016, the Committee published its opinion on the implications of the processing of PNR on data protection, reiterating concerns from the 2015 report and insisting on requirements set up by a well-established case law from the European Court of Human Rights (ECHR). In view of the serious interferences with the rights to data protection and privacy that PNR measures may represent, the ECHR concluded that the legality,[52] proportionality and necessity[53] of PNR systems need to be strictly respected and demonstrated, thus implying specific measures and strong safeguards. It insisted on the principle of **purpose limitation**, underlining that 'the purposes need to be clearly and precisely predefined by law on the basis of objective criteria which limit the transmission of the data only to the competent authorities as well as the further use of such data'. This is key, in particular, when defining the scope of terrorism offences and serious crimes. Without prohibiting data mining and profiling, the ECHR expressed strong concerns, calling for 'greater transparency on the assessment of the efficacy of such systems', with a view to enabling a sound independent assessment of the necessity of the system:

> *While such transparency should be detailed, it should not defeat the legitimate purpose. For instance, objective and quantifiable information regarding results achieved, such as the number of arrested persons, terrorist threats which could be avoided, other deterrent effects, the modification of criminals' behaviours …, the likelihood of substantially increased costs and difficulty of perpetrating crimes (like terrorist attacks) would help inform an assessment as to whether a PNR system is necessary'.*

ENDNOTES

1 See Annex 1 to the PNR Directive.

2 It started in the United States, where air carriers were requested to introduce secure information data to enable passengers screening by law enforcement authorities for security purposes.

3 In line with Article 2(3), Member States may apply the PNR Directive to selected intra-EU flights.

4 This initial assessment aims to identify passengers for whom there is a suspicion of them being involved in terrorist activities or serious crimes (Article 6(2)(a) PNR Directive).

5 The Council of Europe expressed concerns regarding risks of data misuse in a context of strategic surveillance.

6 On 11 March 2004, 193 people were killed and nearly 2 000 injured when 10 bombs exploded on four trains in three Madrid-area train stations during morning rush hour.

7 See recital 5, 'The Council has exhausted all possibilities to obtain in time the opinion of the European Parliament', and recital 6, 'Under these exceptional circumstances, the Directive should be adopted without the Parliament's opinion'.

8 The Council, acting in accordance with the procedure referred to in Article 67, shall, within a period of five years after the entry into force of the Treaty of Amsterdam, adopt: […] (2) measures on the crossing of the external borders of the Member States which shall establish: (a) standards and procedures to be followed by Member States in carrying out checks on persons at such borders; […].'

9 'The Council, acting in accordance with the procedure referred to in Article 67, shall, within a period of five years after the entry into force of the Treaty of Amsterdam, adopt: […] (3) measures on immigration policy within the following areas: […] (b) illegal immigration and illegal residence, including repatriation of illegal residents; […].'

10 To date, a new API Directive can be based on the 2012 Treaty on the Functioning of the European Union; Articles 77(1)(b) and 79(2)(c), when API are collected for border and migration purposes, and Article 87(2)(a) for law enforcement purposes.

11 Article 6 provides the obligation of air, land and sea carriers to assume responsibility for aliens they transport.

12 Such as Council Directive 2001/51/EC supplementing Article 26.

13 Bulgaria, Cyprus, Croatia and Romania. In December 2021, the Council confirmed that Croatia may join the Schengen area.

14 Iceland, Norway and Switzerland. Liechtenstein is not concerned since it has no airport; it will be referred to under implementing countries rather than EU Member States in the text.

15 The 1995 Data Protection Directive, applicable when the API Directive was adopted. The new API must be aligned with the GDPR.

16 See Article 6(1)(b) of the Data Protection Directive, echoed by recital 12 of the API Directive, which stresses the legitimate use of data for the enforcement of entry and migration law.

17 Entry and migration law must be understood as the 'specified and explicit purpose' required under the purpose limitation principle. See CEPS Working Document No 320/September 2009.

18 Interoperability is the ability of information systems to exchange data and enable the sharing of information.

19 Since 2017, key changes affecting border controls include the introduction of systematic verification and authentication of travel documents against Interpol's stolen and lost travel document (SLTD) data base, and systematic border check against the Schengen information system (SIS); see the Systematic Check Regulation.

20 Either because they are not aware of the APIS or because they do not perceive data as being confidential.

21 As mentioned, quantitative data are not available systematically and do not suffice to present a detailed view.

22 For both evaluations the differences result from (a) the technological system selected (b) the nature of data to be collected (c) since data are different, the verification vary (d) the level of integration of the APIS with other national system.

23 Centralised routing mechanism is a central point of collection of data that can forward passengers data to other information systems.

24 The SIS is one of the EU's largest databases. It allows competent authorities to share and manage information regarding missing people, wanted people, illegal entrants in the Schengen area, stolen vehicles, and lost or stolen identity documents. Data include personal data, fingerprints and palm prints.

25 The VIS is used to exchange visa data between the Schengen Member States. The system is comprised of a central IT system and a communication structure that links the central system to national systems. Simply put, the VIS connects consulates abroad to all border points of the Schengen area. It stores data and information on third-country nationals who applied for, possess or were denied a visa to enter the Schengen area. Amendments to the existing VIS rules were adopted in July 2021.

26 The EES, adopted by Regulation (EU) 2017/2226, is a new scheme expected to become operational in 2023 (no fixed date yet). Its main purpose is to register entry and exit data of non-EU nationals crossing the external borders of EU Member States in order to strengthen and protect the Schengen area's external borders. It will include facial, personal and travel-related data.

27 ETIAS allows and keeps track of visitors from countries that do not need a visa to enter the Schengen area, the main goal being the identification of possible threats or risks associated with travellers. Regulation (EU) 2018/1240 establishing ETIAS was published on 19 September 2018; however, for technical reasons, ETIAS is not expected to become operational before November 2023. For more information, see the related fiche on the European Parliament's Legislative Train Schedule and the dedicated website of the Commission's Directorate-General for Migration and Home Affairs.

28 A future API instrument could re-use the data sent under the ETIAS/EES(VIS) Regulations for purposes specific to the API instrument, and thus prevent passengers, carriers and service providers from providing (nearly) identical data twice, capturing those data in a single moment for different purposes, as specified in multiple legal instruments.

29 In 2018, the Convention on International Civil Aviation required signatories to set up an APIS (Annex 9).

30 UN Security Council resolutions 2178(2014), 2309(2016) and 2396(2017).

31 The international aviation community is taken to mean the International Air Transport Association, the ICA and World Customs Organization.

32 eu-LISA is the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. It deals with the interoperability of IT systems; APISs are managed by EU Member States.

33 For more details on how carrier queries will be dealt with once the EES and ETIAS are operational, see carriers interface on the eu-LISA website.

34 In its 2011 opinion on the PNR Directive, FRA already formulated reservations on the compliance of some of its provisions – potential discriminatory effects, lack of precision of what serious crimes are – with fundamental human rights.

35 As mirrored in Article 8(2) of the Charter, and in Article 5(1)(b) GDPR and Article 4(1)(b) Police Directive.

36 See in particular opinion 10 in key recommendations.

37 This opinion aims to inform the European Parliament position on the 2017 legislative proposals on interoperability between EU IT systems. It examines implications of increased forms of interoperability, including access by law enforcement authorities and Europol to EU IT.

[38] PIUs assess systematically and by automated means, that is to say continuously and regardless of whether there is any indication of a risk that the person concerned is involved in terrorist offences or serious crime (point 103 of the judgment).

[39] See point 111 and preceding explanations in points 93 to 110.

[40] Point 106: in its opinion on the EU-Canada PNR Agreement, the Court held that, 'since automated analyses of PNR data are carried out on the basis of unverified personal data and are based on pre-determined models and criteria, they necessarily present some margin of error'. in its 2020 review of the PNR Directive, the Commission noted a fairly substantial number of false positives (i.e. positive matches from automated processing that prove to be incorrect following individual review by non-automated means) in 2018 and 2019, amounting to at least five in six individuals identified.

[41] Point 112; however, they must be considered in relation to their function in society

[42] See Article 52(1) of the Charter.

[43] Points 119 to 120: information is limited to certain aspects of a person's private life, it is prohibited explicitly to process sensitive data, and the purposes for which those data are to be processed are circumscribed; there are rules to process data and ensure security, confidentiality and integrity of those data, and to protect them against unlawful access and processing.

[44] Point 123: '…while the possibility of "false negatives" and the fairly substantial number of "false positives" resulting … from automated processing under that directive in 2018 and 2019, are liable to limit the appropriateness of that system …'.

[45] Points 125 to 140.

[46] Points 182 to 192.

[47] They must be defined in such a way as to take into consideration both 'incriminating' and 'exonerating' circumstances, and be updated, inter alia, to react to developments in the fight against terrorist offences and serious crime.

[48] Point 236: if monitoring activities within the remit of the intelligence and security services are treated 'as an integral part of the prevention, detection, investigation and prosecution of terrorist offences and serious crime, that legislation is liable to disregard the exhaustive nature of the list of the objectives pursued by the processing of PNR data under the PNR Directive, which is a matter for the referring court to verify'.

[49] The 1981 Convention was the first legally binding international instrument in the data protection field.

[50] Data mining is an automatic or semi-automatic process that extracts and analyses large amounts of scattered information to discern trends and patterns, anomalies or correlations. It makes sense of it and turns it into knowledge.

[51] Profiling means collecting and using pieces of information about individuals (or that can be linked indirectly to individuals) in order to make assumptions about them and their future behaviour (p. 23 of the CoE report).

[52] The measure must have: i) some basis in domestic law, ii) be clear and precise enough to be accessible to the person concerned (it must obviously be public), and iii) have foreseeable consequences.

[53] It must be demonstrated that such data processing is a necessary measure in a democratic society for a legitimate aim.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)