10 September 2020

Feedback from the EDRi network, Access Now, Edward Hasbrouck, epicenter.works, FiPR, IT-Pol Denmark, Statewatch on the Roadmap – Ares(2020)3918953 on the external dimension of the EU policy on Passenger Name Records

European Digital Rights (EDRi) is an umbrella organisation with 44 NGO members with representation in 19 countries that promotes and defends fundamental rights in the digital environment.

We welcome the opportunity to contribute to the roadmap on the **external dimension of the EU policy on Passenger Name Records (Ares(2020)3918953).**

The **right to privacy and the right to data protection are fundamental rights.** They are not just a social convention, but legally enforceable rights enshrined in the Treaties, laws and the Charter of Fundamental Rights. In line with the Charter of Fundamental Rights, **infringements of fundamental rights (by long-term storage and processing of such data) are only permissible if they "genuinely meet objectives of general interest"**. In our opinion, neither the PNR Directive nor the existing PNR agreements respect this principle.

On 26 July 2017, the Court of Justice of the European Union **(CJEU) confirmed that the envisaged EU/Canada agreement on the collection and sharing of air travellers' data breaches European law** <http://www.politico.eu/wp-content/uploads/2017/07/EU-Canada-PNR.pdf>. This was the third time that the European Court has ruled against arrangements for mandatory storage of personal data.

The EU PNR Directive was adopted despite **concerns raised by the Fundamental Rights Agency (FRA)[1], the European Data Protection Supervisor (EDPS)[2] and Article 29 Working Party[3]**. A study undertaken for the Council of Europe[4] explained that "no serious, verifiable evidence has been produced by the proponents of compulsory suspicionless data collection to show that data mining and profiling by means of the bulk data in general, or the compulsory addition of bulk PNR data to the data mountains already created in particular, is even suitable to the ends supposedly being pursued –let alone that it is effective".

An additional problem that requires greater scrutiny is the connection between PNR and other surveillance proposals[5] that show very close links between the industry and policy makers[6].

1 https://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_EN.pdf
2 https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2015-12-eu_pnr_en.pdf
3 https://www.statewatch.org/media/documents/news/2015/mar/eu-pnr-letter-art-29-wp-to-chair-libe.pdf
4 https://rm.coe.int/16806a601b
5 http://www.statewatch.org/marketforces/index.htm
6 https://www.euractiv.com/section/justice-home-affairs/opinion/checked-for-tuesthe-curious-tale-of-the-french-prime-minister-pnr-and-peculiar-patterns/

Finally, the "Fundamental rights review of EU data collection instruments and programmes"[7] identified the following problems with PNR systems:

- "Broad data retention mandates, either in terms of retention duration, and/or scope of data subject covered;
- Vague measures on access to retained data that often lack appropriate safeguards on data security or limitation on authorities authorised to access the data;
- Authorisation to process sensitive data, or failure to adequately prevent such processing, even though the processing of special categories of data goes beyond what is necessary for the identified aim of the instrument"

For the purpose of this feedback we have also incorporated, when required, our analysis on the two most recent documents from the Commission, namely the Commission Staff Working Document – On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (SWD(2020) 128 final, 24 July 2020) (hereby "the Staff Working Document" or "the SWD") and the European Commission Report on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime{SWD(2020)128final} (hereby "the EC Review Report").

One general remark to which we would like to bring the European Commission's attention is the appalling lack of evidence (including statistics and a diversity of sources of data and information) both documents demonstrate. They seem to rely solely on information coming from the Member States, leading to a poor critical assessment of the Directive. For example, the section related to the role of Data Protection Officers merely includes a broad evaluation made by national authorities, with no consultation of data protection officers' own opinions, nor those of individuals who filed complaints to them. Similarly, there is a crucial lack of information regarding the number of complaints issued concerning false positives or other issues, making assessment of the current safeguards provided by the Directive difficult. EDRi has repeatedly encouraged the Commission to produce evidence-based policy and not policy-driven evidence. We therefore hope the following remarks will be taken into due account and addressed.

What are the main problems of the PNR Directive and PNR agreements?

- **Unlawful Blanket Data Retention:** After the ruling of the European Court of Justice that invalidated the Data Retention Directive, and considering what the CJEU has said with regard to the envisaged EU/Canada PNR agreement, it is difficult to imagine the Court adopting a different appreciation of the PNR Directive and the

7 Fundamental rights review of EU data collection instruments and programmes, Fondaziona Brodolini, available at http://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf

existing agreements. In addition, practices in the Member States raise considerable concerns, as the SWD recognises on a number of occasions, for example when it admits that "two Member States have failed to correctly transpose the requirement that the disclosure of full data must be reasonably believed to be necessary for responding to a request according to Article 6.2(b)" and that "four Member States have failed to correctly transpose the safeguard concerning the need for ex-post review by the Data Protection Officer when the disclosure of PNR data has been approved by another competent authority."[8]

- **Excessive data retention period:** Even if the retention of data could be reduced to the point of being considered legitimate, it is not clear how the periods (even in the most reduced cases) are necessary or proportionate. In the CJEU's hearing on data retention, neither the European Commission nor the individual Member States were able to give any justification for the retention periods demanded. The SWD states that "Member States have confirmed that the five-year retention period is necessary from an operational point of view." However, no evidence is offered to support this claim, which we are supposed to accept without question.
- **Lack of concrete protections from arbitrariness and lack of harmonisation:** In most Member States "the competences of the supervisory authority to deal with complaints from data subjects, to carry out investigations, to verify the lawfulness of data processing and to provide advice to data subjects have been fully and correctly enshrined in the national legislation. Six Member States reflected most of these competencies, but failed to include all in their laws".[9] This implies that at least six Member States are in violation of the Directive. However, there is no mention of potential corrective actions. Furthermore, the SWD also admits that "[o]f particular concern is the practice of sending broad and unspecified requests to many (or even all Passenger Information Units). Such requests, even if refused as not duly reasoned, create an additional burden for the Passenger Information Unit staff" and that "[t]he lack of harmonisation of national criminal laws leads to additional complexity in this respect" because "[w]ith regard to the serious crimes listed in the PNR Directive, the terminology, classification and applicable sanctions vary across the Member States, which may result in differences in the scope of application."[10]
- **Profiling and automated matches:** It is unclear how screening to find potential suspects is being done and we fear that Member States can, in practice, use it with very limited restrictions. The Commission's review of the PNR Directive[11] mentions

8 SWD, p.19.
9 SWD, p.17
10 SWD, p. 35.
11 EC Review Report: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-305-review_en.pdf . Commission staff working document: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/

that "only the personal data of a very limited number of passengers are transferred to competent authorities for further processing". Specifically, the SWD notes on page 28 that 0.59% of passengers are identified though automated matches and that 0.11% are transmitted to competent authorities after the obligatory manual review. Statistics from Germany[12] and Austria[13], possibly using different data sources and statistical definitions, suggest that the risk of automated false-positive matches is considerably higher. The SWD claims that the obligatory manual review of automated matches eliminates the risk of false positives. This is unlikely to be the case (unless the outcome of the manual review is tautologically defined to be correct) since profiling travel behaviour may still single out innocent persons, even after a manual review. Furthermore, there may be errors in the data used for automated matches which are not necessarily corrected by the manual review. The SWD mentions that PNR data are not used to establish individual profiles of travellers, only 'abstract profiles' of travel behaviour. However, these 'abstract profiles' are used for making automated matches subject to manual verification, a data processing activity that would fit the normal definition of 'profiling'. **There are existing measures (VIS, SIS, API and ETIAS) which already provide sufficient information.** Not enough evidence has been put forward so far regarding the need for another system.

- **Lack of evidence showing that these measures are effective, necessary and proportionate in the investigation or prevention of serious crimes:** In the European Commission's own impact assessment[14] there was no concrete evidence on the actual usefulness of the collection of PNR for tackling of serious crime or terrorist offences. It is particularly worrying that the European Commission stated in its proposal that "PNR data is unverified information provided by passengers"[15] while remaining convinced – despite their questionable accuracy – it could be used in real time "to prevent a crime".

  At the very least, those interested parties arguing for mandatory data retention must, since it involves a serious interference with fundamental rights, provide evidence of its efficacy. Yet in spite of this having been called for for years (e.g. by the researchers from the Max Planck Institute that studied the issue a decade ago[16]), the Member States and their law enforcement agencies still do not collect reliable, statistical information on clear-up rates and their possible linkage to retained data.

20200724_swd-2020-128_en.pdf

12 https://www.sueddeutsche.de/digital/fluggastdaten-bka-falschtreffer-1.4419760
13 https://edri.org/why-eu-passenger-surveillance-fails-its-purpose/
14 http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2011/sec_2011_0132_en.pdf
15 http://ec.europa.eu/home-affairs/news/intro/docs/com_2011_32_en.pdf, page 3
16 https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf

- **Lack of proportionality:** The Fundamental Rights Agency (FRA), the European Data Protection Supervisor (EDPS) and Article 29 Working Party agreed on the lack of proportionality of the original Directive proposal. The EU PNR systems entail data collection and analysis for all passengers on international flights without any sort of targeting. Although it is claimed that the system is not particularly intrusive and requires minimal data processing, in effect the maximum processing of personal data seems the best way of getting results. The SWD admits that PNR data is cross-checked with all sorts of other data bases saying that "[m]ost Member States are now able to process PNR data against databases and watch lists relevant for the purposes of the Directive" – including national databases, SIS and Interpol's SLTD (p.11-12). The lack of proportionality is especially clear with respect to free-text remarks, which can contain an unlimited amount of information on an unlimited variety of subjects. No basis is provided for the claim that all of this information is truly "necessary" or even relevant. No examples are provided of any criminal convictions based on free-text remarks in PNRs. PNR data is incorrectly described as being collected from travellers, but in fact remarks in PNRs are collected from the travel industry staff, often without the knowledge of the individuals to whom the remarks pertain.
- **Excessive costs:** Implementing new PNR agreements with third countries would result in significant costs for Member States as the number of data requests will eventually rise. The high expenditure is confirmed by the European Commission's impact assessment, which evaluates the cost at hundreds of millions of euro. In times of a global pandemic characterised by a drastic reduction of flights and travels between national borders, pushing for the implementation of such pervasive measures are a waste of public resources and show lack of prioritisation from public authorities. This is reinforced by the SWD struggling to assess how useful it is for law enforcement authorities. In the same paragraph the SWD concedes that "it may be difficult to single out the exact impact that the use of PNR data has had in each specific case" but that "law enforcement authorities from across Member States have indicated that PNR data has been successfully used to organise and plan operational and monitoring activities in advance, obtain full details of persons of interest, identify previously unknown suspects, establish links between members of crime groups through the analysis of contact and payment details, and verify the assumed 'modus operandi' of serious criminals and organised crime groups". One would think that with all of those successes some sort of evidence of the impact would be available, but it is not.
- **Mixed with biometric or other sensitive data, a disaster**: Dr. Krisztina Huszti-Orbán and Prof. Fionnuala Ní Aoláin (UN Special Rapporteur on defending human rights while countering terrorism) state in the report "Use of Biometric Data to Identify

Terrorists: Best Practice or Risky Business?"[17] that "[b]oth API and PNR are frequently linked with biometric data, with watchlists and other relevant databases also commonly containing biometric information—an aspect that needs to be considered when addressing implications of these obligations separately." We have already discussed elsewhere the use of biometrics for mass surveillance[18]. The mix with other sensitive data is recognised in the SWD when it states that "[f]our Member States have failed to transpose correctly the prohibition on the use of discriminatory pre-determined criteria or criteria based on sensitive data" and that "[f[ive Member States did not transpose the obligation that decisions of competent authorities must respect the principle of non-discrimination".[19] Despite the fact that the Commission argues that technology is "designed in a way that makes the collection and processing of sensitive data technically impossible", we remain suspicious that that is actually the case without further evidence made available in the Review Report and the Staff Working Document. For example, special meal requests can indicate religious preferences of the passenger. Furthermore, we agree with the authors of the Council of Europe Report when they state that there is "misplaced focus on the use of "sensitive data" in profiling" since "discrimination can result from profiling that does not use any such data, or even any proxies for such data (such as meal preferences)" and "algorithms can reinforce much more deeply and insidiously embedded social distinctions, linked to almost any kind of matter (e.g., postcode or length of residency)".[20]

- **Data protection provisions are not fully implemented:** Currently numerous data protection provisions from the PNR Directive are implemented incorrectly or not at all, which undermines any efforts for external transfers of PNR data: The Staff Working Document recognises that "instances of non-conform transposition have been identified" but no action has been taken despite the Commission's stating that its "commitment" to "ensuring full conformity of transposition" means it "will not hesitate to pursue infringement action" after the September 2019 compliance assessment study (cited in footnote 3 of the SWD). The SWD also recognises that "[f]our Member States have adopted national measures that go beyond the purpose limitation, by specifically allowing the use of PNR for national security purposes" and that "the requirement to only use the databases relevant for serious criminal offences and terrorism is explicitly reiterated in the national PNR laws of all Member States, except two."[21] Such implementations present a clear risk that PNR data will be processed by Member States' national security services without the data

17 https://www.ohchr.org/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf
18 https://edri.org/blog-ban-biometric-mass-surveillance/
19 SWD, p.20.
20 See Council of Europe, 2015, "Passenger Name Records,data mining & data protection:the need for strong safeguards", p. 103
21 Staff Working Document, page 15.

protection safeguards of EU law. No action seems to have been taken against them, but some against countries like Spain that have not implemented the Directive yet. This gives the impression that incorrectly implementing the Directive, and in so doing failing to protect fundamental rights, is better than not implementing it at all.

- **Potential lack of independence and power of Data Protection Officers**: On page 16 of the SWD we read that "the degree of independence of the Data Protection Officer (DPO) can be expected to be greater when he or she is not a member of the Passenger Information Unit staff and is not subordinated to the head of Passenger Information Unit." This can be read as indicating that in some instances this is actually the case, which would clearly undermine the independence of a DPO. Clarifications are required from the Commission to provide a better understanding of the actual situation in Member States. Furthermore, on p.17 the SWD admits that "[f]our Member States do not explicitly recognise the competence of their Data Protection Officers to refer cases of unlawful processing to a national supervisory authority" which undermines the credibility of the DPO to perform their functions. In several Member States, it is also observed that the role of the DPO has been restricted in the national transposing legislation (e.g. not informed when PNR data is transferred to a third country, not able to carry out ex-post reviews of PNR data disclosures which are approved by another competent authority than a judicial one) – which clearly does not conform with the Directive's requirements. The SWD even notes that one Member State failed to appoint a DPO (p.9).
- **Insufficient passengers' rights**: The SWD recognises that "four Member States have failed to fully transpose other conditions provided for by the Directive relating to the purposes for which the data can be transferred or the authorities competent to receive it".[22]
- **Next stop, surveillance of all means of transportation?**: The SWD states in different parts how the flight reservations made by travel agencies and tour operators are not collected and processed by the PIU and concludes that "the extension of data collection to non-carrier economic operators will require a detailed analysis of the legal, financial and technical aspects stemming from such extension, like the lack of standardisation of data formats" which assumes that it has arrived to a conclusion of what to do next with that data collected by non-carrier economic operators. Furthermore, the SWD points to the "positive operational experiences" of PNR data in maritime, rail and road transport and we are warned of the "serious concerns" "raised by law enforcement experts with regard to the lack of collection of passengers' data from other modes of transportation", which provides a clear indication of likely future tendencies in this area.[23]

22 Staff Working Document, p.22.
23 SWD, p. 39-40.

Because of all of the above, the signatories of this document express that PNR systems:

- **are not necessary, proportionate or even effective** in the fight against terrorism and serious crime across the globe;
- **represent disproportionate use of personal data** without respecting fundamental rights;
- **bring legal uncertainty** for passengers and air carriers;
- **in relation to third countries, PNR agreements will only lead to additional mass surveillance** taking place outside of EU borders.

Conclusion and recommendations:

We recommend that the European Commission suspends the existing PNR agreements, pauses further negotiations with additional third countries and suspends the EU PNR Directive. In addition, the **EU Commission should ensure that outcomes of the negotiations at the International Civil Aviation Organisation (ICAO) for draft new PNR standards** through an expert Task Force established within the ICAO Facilitation Panel (which does not include any representatives of data protection authorities or civil society) **is in line with EU law and does not lead to new obligations being placed on the EU and its Member States**. In particular, the EU cannot adhere to standards that would contradict Opinion 1/15 of the CJEU and lower the level of data protection guaranteed in the EU – both for data stored and processed in the EU and in the context of international transfers. As several cases regarding the legality and validity of PNR measures are currently before the Court of Justice of the EU, the EU should refrain from agreeing to new obligations on PNR until the Court has providing guidance as to which measures are lawful under EU primary law.

Sources:

CJEU: The Court declares that the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data may not be concluded in its current form (26.07.2017)
http://www.politico.eu/wp-content/uploads/2017/07/EU-Canada-PNR.pdf

FAQ: Passenger Name Records (PNR)
https://edri.org/faq-pnr/

EU-Canada agreement on PNR referred to the CJEU: What's next? (03.12.2014)
https://edri.org/eu-canada-agreement-on-pnr-referred-to-the-cjeu-whats-next/

CJEU hearing on the EU Canada PNR agreement: Still shady (06.04.2016)
https://edri.org/cjeu-hearing-on-the-eu-canada-pnr-agreement-still-shady/

The curious tale of the French prime minister, PNR and peculiar patterns (04.10.2016) https://www.euractiv.com/section/justice-home-affairs/opinion/checked-for-tuesthe-curious-tale-of-the-french-prime-minister-pnr-and-peculiar-patterns/

ECJ: Data retention directive contravenes European law (09.04.2014) https://edri.org/ecj-data-retention-directive-contravenes-european-law/

European Court confirms: Strict safeguards essential for data retention (19.07.2016) https://edri.org/european-court-confirms-strict-safeguards-essential-data-retention/

Max-Planck-Institut für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten, 2nd enlarged edition, 2011, available at: https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf

Fundamental rights review of EU data collection instruments and programmes, Fondaziona Brodolini, available at_
http://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf

Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, report prepared for the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) of the Council of Europe, 2015, available at: https://rm.coe.int/16806a601b

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-305-review_en.pdf

Signatories:

European Digital Rights

Access Now

Edward Hasbrouck

epicenter.works

FiPR

IT-Pol Denmark

Statewatch

Contact person:
Diego Naranjo
Head of Policy
European Digital Rights (EDRi)
diego.naranjo@edri.org