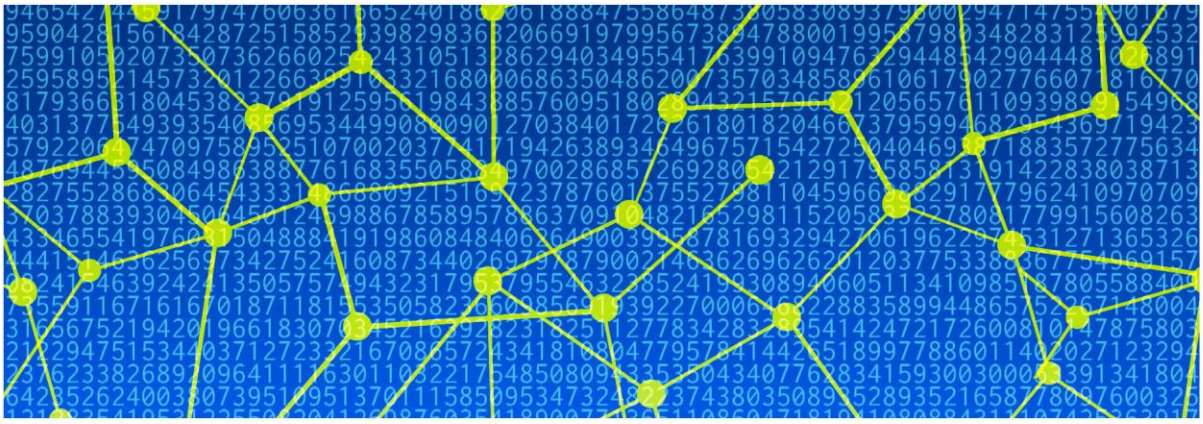

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 3/2016

Opinion on the exchange of information on third country nationals as regards the European Criminal Records Information System (ECRIS)

EDPS

13 April 2016

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking - in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. The EDPS considers that compliance with data protection requirements will be key to the success of exchanging information on the criminal records of third country nationals through ECRIS.

Executive Summary

The extension of the exchange of information regarding criminal records in the EU to third country nationals (TCN) in the ECRIS (European Criminal Records Information System) has been envisaged for a long time by the EU legislator. The Proposal to extend ECRIS to TCN was accelerated by the EU Agenda on Security, which acknowledged that ECRIS "does not work effectively for non-EU nationals convicted in the EU".

The ECRIS framework currently uses the Member State nationality of convicted persons as a central point in the exchange of information. This is why the creation of a parallel system is justified for third country nationals. The Commission chose to implement the exchange of information regarding the criminal records of third country nationals in a decentralised system, through the use of an index-filter for each participating Member State. The index-filter will be updated with specific information every time a third country national is convicted and will be sent to the other Member States.

The EDPS has carefully analysed the legislative Proposal and issues recommendations with a view to assist the legislator and to ensure that the new measures will be compliant with EU data protection law, and in particular Articles 7 and 8 of the EU Charter of Fundamental Rights.

While the EDPS welcomes the proposal of an EU decentralised system to process data related to criminal records of TCN, based on a "hit/no hit" search feature and using technical measures intended to limit interferences in the rights to respect for private life and for personal data protection, the EDPS raises three main concerns and other additional recommendations, further detailed in the Opinion.

Firstly, a corresponding regime for TCN as the one existing for EU nationals regarding processing of fingerprints should be put in place, which takes into account the specificity of the national criminal systems, meeting thus the requirements of necessity and proportionality of the processing of personal data.

Secondly, the text of the Proposal inaccurately refers to the information in the index-filter as being "anonymous". The EDPS recommends the clarification that the information processed for the purposes of ECRIS-TCN is personal data, which has undergone a process of pseudonymisation, and not anonymous data.

Thirdly, the EDPS considers that creating a different type of system to process data for EU nationals that have a third country nationality other than the one in place for EU nationals does not meet the requirements of necessity in EU data protection law and could lead to discrimination. Therefore, the EDPS recommends that the measures in the Proposal only refer to TCN and not also to EU nationals that also have a third country nationality.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty of the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular Articles 28(2), 41(2) and 46(d) thereof,

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION AND BACKGROUND

I.1 Consultation of the EDPS

1. On 19 January 2016 the European Commission published a Proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA ('the Proposal')[1]. The EDPS was consulted informally before the publication of the Proposal. However, the EDPS regrets to have not received a request for an Opinion after the publication of the Proposal.

I.2 Objective of the Proposal

2. ECRIS is an electronic system for exchanging information on previous convictions handed down against a specific person by criminal courts in the EU for the purposes of criminal proceedings against a person, and, if so permitted by national law, for other purposes. The system is based on Council Framework Decision 2009/315/JHA ('the Framework Decision') and Council Decision 2009/316-JHA[2].

[1] COM(2016) 7 final, 2016/0002 (COD), Strasbourg, 19.1.2016.

[2] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (Framework Decision), OJ L 93, 7.4.2009, p. 23, and Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, OJ L 93, 7.4.2009, p. 33.

3. According to the Explanatory Memorandum accompanying the Proposal, the underlying principle of ECRIS is that complete information on previous convictions of an EU national can be obtained from the Member State of nationality of that person, which can provide exhaustive up-to-date information on the criminal records of its nationals upon request, regardless of where in the EU convictions were handed down. This architecture makes it presently difficult for authorities to exchange information on convictions concerning third country nationals and stateless persons (hereinafter: TCN) through ECRIS, as "TCN have no Member State of nationality", and "in order to obtain a complete overview of the criminal records history of a particular individual requests must be sent to all the convicting Member State(s)"[3].

4. Therefore, the objective of the Proposal is to improve the efficiency of ECRIS with regard to the exchange of information concerning the criminal records of TCN.

5. The Explanatory Memorandum describes the system that was chosen to achieve this objective. The system will be organised in a decentralised way, meaning that there will not be a single EU database containing the relevant information, but each Member State will maintain a data file. Member States will have to extract identity data from their criminal record and feed it into a separate file - "the index-filter", whenever a TCN is convicted. The data will be converted into "locks and keys". The index-filter will be distributed to all Member States, enabling them to search independently at their own premises. The system will allow the Member States to match their own data against the file and to find out whether further entries in criminal records exist in other Member States (a "hit/no hit" system).

II. DATA PROTECTION IMPLICATIONS

6. The EDPS welcomes the reference in Recital 12 of the Proposal, to Council Framework Decision 2008/977/JHA[4] on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters and its application in the context of computerised exchange of information extracted from criminal records of Member States, providing for an adequate level of data protection when information is exchanged between Member States, whilst allowing for Member States to require higher standards of protection to national data processing. In addition, the EDPS notes that the proposed Data Protection Directive for criminal matters[5] (DPD) will be fully applicable to the processing of personal data envisaged by the Proposal, once it enters into force. **Therefore, the EDPS recommends that the Preamble of the Proposal includes a reference to the DPD, clarifying the relationship between the instruments.**

7. The measures laid down in the Proposal involve processing of personal data and, therefore, they constitute an interference with the fundamental right to private life, as enshrined in Article 7 of the Charter of Fundamental Rights of the EU ('EU Charter'), and with the fundamental right to the protection of personal data, as guaranteed by Article 8 of the EU Charter[6]. In this sense, the EDPS welcomes the reference made in the Explanatory

[3] Explanatory Memorandum of the Proposal, p. 3.
[4] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L350/60, 30.12.2008.
[5] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data, as agreed on 18 December 2015 by the Council.
[6] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, 8.4.2014, at 33 and 36.

Memorandum to the jurisprudence of the Court of Justice of the EU applying Articles 7 and 8 of the EU Charter with regard to access of authorities to personal data for law enforcement purposes, and especially to the *Digital Rights Ireland ('DRI')* case.

8. Article 52(1) of the Charter provides that any limitation on the exercise on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others[7].

9. The fight against terrorism and fight against serious crime in order to ensure public security is recognized as an objective of general interest in EU law[8]. As acknowledged in the preamble of the Proposal, "the exchange of information on criminal convictions is important in any strategy to combat crime and counter terrorism" (Recital 7). The proposed measures, therefore, meet an objective of general interest and can be justified, subject to the principle of proportionality. The analysis below focuses on several aspects regarding the proportionality of the proposed measures; it will also highlight the need to better define the material scope of the Proposal, in relation to the type of data processing (anonymisation/pseudonymisation).

II.1 Material scope of the measure proposed

A. Processing of fingerprints

10. According to the Proposal, on the one hand, Member States will have an unconditional (except for cases where prints cannot be taken for factual reasons[9]) obligation to store the fingerprints of convicted TCN, according to Article 1(4) of the Proposal. In addition, fingerprints of TCN must be stored *in the index-filter*. On the other hand, Member States only have to store fingerprints of convicted EU citizens when they are available to the central authority (Article 11(1)(c)(ii) of the Framework Decision). It is understood that the fingerprints of EU citizens thus may or may not, in accordance with national legislation, be available to the central authority.

11. The proposed compulsory collection, storage and use of fingerprints for the ECRIS-TCN system is an interference according to both Articles 7 and 8 of the Charter. In this sense, the Court of Justice of the European Union (CJEU) found in its *Schwarz* judgment that "the taking and storing of fingerprints by the national authorities (...) constitutes a threat to the rights to respect for private life and the protection of personal data"[10]. While the use and storage of fingerprints for ECRIS-TCN indeed pursues a legitimate interest, as required by Article 52(1) of the Charter, namely the fight against terrorism and fight against serious crime in order to ensure public security, it must be assessed whether the measure is necessary and proportionate.

12. As a preliminary remark, it must be noted that "the conditions under which Member States store fingerprints during criminal investigations and proceedings are not harmonised

[7] See also *Digital Rights Ireland*, at 38.
[8] CJEU, Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission* EU:C:2008:461, at 383; Cases C-539/10 P and C-550/10 P *Al-Aqsa* v *Council* EU:C:2012:711, at 130; Case C-145/09 *Tsakouridis* EU:C:2010:708, at 46 and 47.
[9] The wording used in Article 4a(1) for this exception is: "in exceptional individual cases, where this is not possible".
[10] See, to this effect, CJEU, C-291/12 *Schwartz v. Stadt Bochum*, 17.10.2013, at 30.

by EU law"[11]. In practice, this means that Member States currently have different rules for storing fingerprints for law enforcement purposes, depending on the seriousness of crimes and offences. A factor to consider when assessing the necessity of the compulsory use of fingerprints is that each Member State has its unique criminal law policy, with different thresholds of the gravity of offences which require the storage of fingerprints of convicted persons in their own judicial databases[12]. As a consequence, a situation may arise that a Member State may be obliged pursuant to the Proposal to collect and store the fingerprints of a person for a minor offence (which represents an interference in the person's right to private life), while its national law does not require the fingerprints to be stored in relation to the criminal record of that person.

13. The obligation of Member States to store the fingerprints of all convicted TCN in the index-filter is justified by the legislator through the need to "secure identification"[13], having regard to the fact that "this is the only way to be sure of the identity of the person"[14]. The added value of using fingerprints especially for the identification of TCN must be recognised, to the extent that it is conceivable there can be cases of TCN who do not have identification documents or whose names are written in alphabets which are not used by the official languages of the Union, leaving thus room for misidentification.

14. However, according to the Explanatory Memorandum, many Member States' central authorities do not currently store fingerprints in their national criminal record registers and are not connected to the national automated fingerprint identification system (AFIS)[15]. Member States also invoked "constitutional concerns"[16] raised by the obligation to store fingerprints of all convicted TCN, irrespective of the type of offence or crime committed.

15. It cannot, therefore, be considered that there is no other way to ensure identification of the persons then to use fingerprints and the necessity of the compulsory use of fingerprints for TCN in ECRIS is therefore yet to be demonstrated.

16. Having regard to all of the above, it does not seem necessary, nor proportionate to impose an obligation to all Member States to store the fingerprints of TCN, regardless of the sanction thresholds and the nature of offences in their own national systems. **The EDPS recommends the legislator to consider creating a corresponding regime for TCN as the one existing for EU nationals regarding processing of fingerprints, by extending the scope *ratione personae* of Article 11 of the current Framework Decision 2009/315/JHA to TCN. This would make storage of fingerprints optional at national level, in compliance with the constitutional systems of the Member States, but it would maintain the obligation that whenever fingerprints of TCN are stored at national level, they must be inserted in the index-filter.**

[11] Impact Assessment, p. 15.
[12] As the Commission acknowledged in one of its communications, "certainly, criminal law is a sensitive policy field, where differences amongst the national systems remain substantial, for example regarding sanction types and levels as well as the classification of certain conduct as an administrative of criminal offence" - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *"Towards an EU criminal policy: ensuring the effective implementation of EU policies through criminal law"*, COM(2011) 573 final, 20.09.2011, p. 2.
[13] Recital 10 of the Preamble.
[14] Explanatory Memorandum, p. 6.
[15] Explanatory Memorandum, p. 6.
[16] Explanatory Memorandum, p. 6.

17. The EDPS has emphasised in previous Opinions related to data-bases containing biometric data that "the inherently sensitive nature of biometric data requires specific safeguards"[17], such as a targeted impact assessment on the use of biometrics, putting an emphasis on the enrolment process (the way they will be collected), highlighting the level of accuracy and putting in place a fall-back procedure, in order to respect the dignity of persons who could have been wrongly identified and to avoid transferring onto them the burden of the system imperfections[18].

18. As for the measure at hand, the Impact Assessment of the Proposal contains dedicated sections to the analysis of the use of fingerprints, taking into account several options – centralised/decentralised storage, compulsory/voluntary use. In addition, the legislative Proposal contains specific safeguards that take into account the sensitive nature of biometric data. Both the mechanism to pseudonymise data within the index-filter and the implementation of an EU decentralised "hit/no hit" system are welcome safeguards concerning the processing of fingerprints in the data file. In addition, **the EDPS recommends that in the following implementing acts to be proposed by the Commission, further safeguards are inserted concerning the enrolment process, highlighting the level of accuracy and putting in place a fall-back procedure.**

B. Anonymisation/pseudonymisation

19. The Proposal refers to an "anonymous" index filter allowing Member States to check if other Member States hold information about a specific TCN. According to the information provided, the EDPS considers that the information provided cannot be qualified as "anonymous", because of the nature of the system, which is to allow the identification of individuals that have a criminal record issued by another Member State. In order to assess the usage of terminology in the Proposal, it is appropriate to revisit the relevant definitions:

- "Personal data" are defined in the EU legal order as meaning "any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly"[19]. The term thus also covers indirect identification, e.g. via a reference number;
- "Pseudonymisation" is defined in DPD as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person"[20]. Pseudonymised data are thus still personal data and as such within the scope of data protection law;
- "To make anonymous" is defined in Article 2(k) of the Council Framework Decision 2008/977/JHA as "to modify personal data in such a way that details of personal or material circumstances can no longer or only with disproportionate investment of time, cost and labour be attributed to an identified or identifiable natural person". The Article 29 Working Party found that "'anonymised data' would therefore be anonymous data that previously referred to an identifiable person, but where that

[17] Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II) (COM(2005) 230 final, COM(2005) 236 final and COM(2005) 237 final), OJ C 91,19.4.2006, p. 43.
[18] EDPS Opinion on SIS II, 2005, p. 44.
[19] Article 3(1) of the DPD.
[20] Article 3(4a) of the DPD.

identification is no longer possible"[21]. As they are not related to identified or identifiable natural persons, "anonymous data" are thus outside the scope of data protection law.

It is against these established definitions that the wording of the Proposal needs to be assessed.

20. The Proposal enables two different processing operations of personal data belonging to TCN, in addition to the exchange of information *per se*. The first processing operation of personal data is the "storage" by Member States of a set of 11 personal data items[22], including fingerprints of the person, "where a conviction is handed down against a third country national (...), unless, in exceptional individual cases, this is not possible"[23].

21. The second processing operation of personal data is the creation and use of the index-filter. Article 1(4) of the Proposal, inserting an *Article 4a(2)* in the ECRIS Directive, provides that "the central authority shall create an index-filter containing *anonymised information*" (our emphasis), which must contain five of the data items stored by Member States[24], including fingerprints. According to the Explanatory Memorandum, the index-filter as described above *"will not contain personal data"*[25], because the information that will be stored in the index-filter will be *"anonymised"*[26]. Moreover, the Preamble of the Proposal further states that "[t]he personal data *should be rendered anonymous* in such a way that the data subject *is not identifiable*"[27] (our emphasis).

22. Therefore, it is clear that the very purpose of the existence of the index-filter containing fingerprints is in fact the precise identification of TCN who have a criminal record in other Member States, by identifying those Member States and further requiring all available information regarding that specific TCN who is the subject of the search. As according to established definitions any information relating to an identified or identifiable natural person is personal data this includes the information which is contained by the index-filter. The Explanatory Memorandum of the Proposal itself specifies that "to secure effective *identification* of third country nationals, fingerprints should be included in the identification data to be stored in the person's criminal record and in the index-filter"[28].

---

[21] In this regard, see the conclusion of the Article 29 Working Party in Opinion No. 4/2007 on the concept of personal data, that "Anonymised data would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible" (p. 21). Also see "Additional EDPS Comments on the Data Protection Reform Package", p. 1 to 3, published on 13 March 2013.

[22] *Article 4a(1)*: (a) information on the convicted person (full name, date of birth, place of birth (town and country), gender, nationality and – if applicable – previous name(s); (b) information on the nature of the conviction (date of conviction, name of the court, date on which the decision became final); (c) information on the offence giving rise to the conviction (date of the offence underlying the conviction and name or legal classification of the offence as well as reference to the applicable legal provisions); (d) information on the contents of the conviction (notably the sentence as well as any supplementary penalties, security measures and subsequent decisions modifying the enforcement of the sentence); (e) the convicted person's parents' names; (f) the reference number of the conviction; (g) the place of the offence; (h) if applicable, disqualifications arising from the conviction; (i) the convicted person's identity number, or the type and number of the person's identification document; (j) fingerprints of the person; (k) if applicable, pseudonym and/or alias name(s).

[23] Article 1(4) of the Proposal (new Article 4a(1) of the Framework Decision).

[24] Points (a), (e), (i), (j) and (k) of the list enumerated in Footnote 22.

[25] Explanatory Memorandum of the Proposal, p. 5.

[26] Recital 11 of the Preamble of the Proposal.

[27] Recital 11 of the Preamble of the Proposal.

[28] Explanatory Memorandum, p. 9.

23. Even though the process used for feeding data in the index-filter is described as "irreversible"[29], the fact remains, beyond doubt, that the purpose of the processing data in the index-filter is the identification of specific TCN that have criminal records in other Member States by producing a "hit/no hit" result. The "hit/no hit" result, together with the identity data used to search the index filter lead to the identification of natural persons and additional information about them (i.e. whether they have a criminal record in one or more of the other Member States).

24. The data processed in the index-filter cannot, therefore, be defined as "anonymous". It appears that it is pseudonymised instead - which is personal data subjected to the process of pseudonymisation as described in paragraph 9 above.

25. While we appreciate the technique envisaged[30] to transform the data in the index-filter into "locks and keys" as an appropriate safeguard to limit the interferences to the right to private life and the right to personal data protection of the individuals concerned[31], we underline that data protection law applies to the data in the index-filter. Therefore, we recommend that, for the purposes of clarity and legal certainty, the text of the Proposal should be synchronised with the text of the DPD[32] to the extent that **references to anonymous data should be removed from the Proposal and replaced with accurate references to the process of pseudonymisation.**

C. Categories of personal data to be processed

26. Article 1(4) of the Proposal introducing a new Article 4a(1) in the ECRIS-Directive specifically lists the data to be stored by the central authority of a Member State in the case of a conviction of a TCN. A similar list is laid down in Article 11 of the current Framework Decision for the EU nationals that have been convicted. Article 11 of the Framework Decision - compared to the new Article 4a - is more limited with regard to the interference in the private life of EU nationals. It creates three different categories of data to be processed for the purposes of ECRIS: obligatory information, optional information (e.g. names of convicted person's parents) and additional information. This differentiation does not exist for the data of TCN to be processed for the purposes of ECRIS.

27. In practice, by comparing the two lists, it is apparent that the information items concerning "the convicted person's parents' names", "the reference number of the conviction" and "the place of the offence", which are optional information to be transmitted in the case of EU nationals, are compulsory information to be transmitted in the case of TCN. Having two different articles in the proposed Directive that detail the information to be exchanged, one article applicable to EU nationals, and the other applicable to TCN, does not appear to be justified. There is additional information required about TCN, which for EU nationals is just optional information. This distinction could be justified only if it is based on

[29] Explanatory Memorandum, p. 5.
[30] It appears that the European Commission already has a planned technical solution for the implementation of ECRIS-TCN and that the text of the Proposal was written so that it fits this technical solution. As a general point, the process should be to first define the requirements for a technical solution and then to procure or develop a solution fulfilling these requirements.
[31] Compared to a fully centralised index file.
[32] The DPD is in the final stage of the adoption. On 18 December 2015, the Permanent Representatives Committee (Coreper) confirmed the compromise texts agreed with the European Parliament on data protection reform. The agreement was reached between the Council, Parliament and Commission on 15 December. The formal adoption is expected in the first half of 2016.

strong and precise legal reasoning, which does not seem to be available. The EDPS recommends extending the *ratione personae* scope of application of Article 11 ("Format and other ways of organising and facilitating exchanges of information on convictions") of the Framework Decision 2009/315/JHA to TCN, instead of inserting an additional article in the Directive that specifically lists the information of TCN to be processed.

II.2 Personal scope of the measure

28. The Proposal creates two distinctions concerning the personal scope of the measure proposed: one between EU nationals and TCN, and the other one between EU nationals that only have the citizenship of an EU Member State and EU nationals that also have the citizenship of a third country. The two distinctions appear as a result of the creation of the index-filter, which will contain data of TCN, including data of EU citizens that also hold the nationality of an EU Member State. To this effect, Article 1(4) of the Proposal (new *Article 4a(4)* of the future ECRIS-Directive) specifies that the creation of the index-filter "*apply ... also regarding third country nationals who hold the nationality of a Member State*". This distinction is also made in the new Article 4b(2) on the "use of index-filters".

29. The EDPS recalls that Article 8(2) of the Charter requires that processing of personal data must be fair. In addition, as shown above, processing of personal data represents an interference with the right to the protection of personal data[33], and Article 52(1) of the Charter requires that any interference with Article 8 must be necessary and proportionate.

30. The distinction between TCN and EU nationals made with regard to different ways of processing their personal data seems to be necessary, because it is justified by objective factors related to the purpose of the measures proposed, as described in paragraph 3 of this Opinion. Particularly, the creation of the index-file for TCN is justified by the fact that TCN do not have a Member State of nationality, so that the regular ECRIS procedure for exchange of information cannot be applied to them[34].

31. With regard to the distinction between EU nationals who are only EU nationals and EU nationals who are also the citizens of a third country, the necessity of the measure is not demonstrated. If a certain processing operation, such as the processing of data in the index-filter, is not needed for EU nationals, it is not needed for EU nationals who are also TCN, either.

32. In *Huber*, the Court of Justice found that former Article 12(1) EC providing for the right to non-discrimination based on nationality within the EU (current Article 18(1) TFEU) "must be interpreted as meaning that it precludes the putting in place by a Member State, for the purpose of fighting crime, of a system for processing personal data specific to Union citizens who are not nationals of that Member State"[35]. The Court recalled that "comparable situations must not be treated differently and that different situations must be treated in the same way. *Such treatment may be justified only if it is based on objective considerations independent of the nationality of the persons concerned and is proportionate to the objective being legitimately pursued*"[36] (our emphasis).

[33] To this effect, see paragraph 7 above and the reference therein.
[34] Explanatory Memorandum, p. 3.
[35] C-524/06 *Heinz Huber v. Germany*, 16.12.2008, at 81.
[36] C-524/06 *Huber*, at 75.

33. The difference of treatment contained in the proposal does not seem to be necessary to achieve the objective pursued, considering that for EU nationals the existing procedures of ECRIS can be applied in order for authorities to share information. The Explanatory Memorandum of the proposal does not provide any explanation as to why such a distinction would be necessary. This difference of treatment may result in discrimination, which would breach Article 21(1) of the EU Charter. This Article prohibits, within the scope of application of the TEU, "any discrimination based on any ground" which cannot be justified in accordance with Article 52(1) of the Charter.

34. Ultimately, the aim of enacting data protection legislation in any area (commercial or criminal matters) is "*to ensure a high level of protection of the fundamental rights and freedoms of natural persons, (...), with respect to the processing of personal data*"[37], including the right to non-discrimination. Therefore, a situation in which the processing of personal data would breach the fundamental rights of the persons whose data are processed, such as the right to non-discrimination as enshrined in Article 21 of the EU Charter, would not be compliant with EU data protection law.

35. **The EDPS therefore recommends that the index-filter is limited only to information pertaining to TCN, without EU nationals who also hold the citizenship of a third country.**

II.3 Data quality

36. The EDPS welcomes the provision in the Proposal in Article 4a(3) of an automatic update of the personal data contained in the index-filter, following any alteration or deletion of the information, which is similar to the obligation enshrined in Article 4(3) of the current Council Framework Decision 2009/315/JHA with regard to the criminal records of EU nationals. Accuracy of information is particularly important in the exchange of information in criminal matters, where a person can be subject to decisions having legal effects or adverse effects as a consequence of the processing of data.

III. CONCLUSION

37. As already stated in the EDPS 2006 Opinion on the ECRIS Proposal, "for third country nationals, an alternative system might be needed", because "for obvious reasons, the proposed system cannot work in those cases"[38]. We therefore welcome the current Proposal and we acknowledge the importance of efficient exchange of information extracted from criminal records of convicted persons, particularly in the context of the adoption of the EU Agenda on Security[39].

[37] See Article 1(1) of the Council Framework Decision 2008/977/JHA and Article 1(1) of Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 23/11/1995, p. 0031 - 0050.

[38] Opinion of the EDPS on the Proposal for a Council Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States (COM (2005) 690 final), OJ C 313/26, 20.12.2006, paras 15 and 18.

[39] "European Agenda on Security" - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 28 April 2015, COM(2015) 185 final.

38. After carefully analysing the Proposal, the EDPS makes the following recommendations, in order to ensure compliance with EU data protection law:

1) With regard to the compulsory use of fingerprints for TCN, **a corresponding regime for TCN as the one existing for EU nationals should be created**, in line with the existing rules on collecting fingerprints at national level;

2) References to anonymous data should be removed from the Proposal and replaced with **accurate references to the process of pseudonymisation**;

3) **The data to be stored at national level regarding convicted EU nationals and convicted TCN should not be differently categorised,** by extending the same regime currently existing for EU nationals (e.g. "optional data", "additional data") to TCN as well;

4) **The use of the index-filter system should be limited only to personal data of TCN**, a category of persons that should not include EU nationals who also hold the citizenship of a third country.

39. In addition, the EDPS makes the following recommendations which would strengthen the protection of personal data processed for the purposes of ECRIS-TCN:

1) The Preamble of the Proposal should include **a reference to the DPD**, clarifying the relationship between the instruments;

2) Further safeguards should be provided for the processing of fingerprints in the Implementing Acts to be proposed by the Commission, **concerning the enrolment process, highlighting the level of accuracy and putting in place a fall-back procedure;**

Done in Brussels, 13 April 2016

Giovanni BUTTARELLI

European Data Protection Supervisor