EUROPEAN
COMMISSION

Brussels, 29.6.2017
SWD(2017) 248 final

COMMISSION STAFF WORKING DOCUMENT

Analytical Supporting Document

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council

establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless people (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) N° 1077/2011

{COM(2017) 344 final}

Table of Contents

Introduction

On 19 January 2016, the Commission adopted 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 criminal records information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA (COM/2016/07 final). Its purpose is to introduce a mechanism into the ECRIS system that would allow the efficient identification of Member States having convicted third country nationals or stateless persons (TCN). The Commission proposed the creation of a decentralised system for processing alphanumeric and fingerprint data using the Ma³tch-software[1].

However, during the legislative process, including a feasibility/cost assessment study on the use of fingerprints finished in June 2016[2], it was revealed that the implementation of the proposed decentralised solution for information exchange would face technical difficulties with regard to the exchange of pseudonymised fingerprints of convicted TCN.

In order to support the supplementary proposal, in this analytical note a different solution for creating an effective centralised ECRIS-TCN mechanism is presented and assessed.

The analysis in this note is based on the previous Impact Assessment presented as part of the January 2016 proposal (COM (2016) 7 final). The problem definition remains unchanged from the Impact Assessment which accompanied the 2016 Commission proposal. Also, the general and specific policy objectives remain the same.

1. THE PROPOSED SOLUTION: FULLY CENTRALISED SYSTEM CONTAINING ALPHANUMERIC DATA AND FINGERPRINTS

Following the adoption of the 2016 proposal and in the light of the legislative process, the Commission has ordered two additional studies to support its work on an ECRIS-TCN mechanism. The first of these was focused on different options for dealing with the exchange of fingerprint and alphanumeric information through both centralised and decentralised mechanisms. A second study was ordered to focus on the costs of establishing a centralised solution for both alphanumeric and fingerprint data.

It should also be noted that using fingerprints for the identification of TCN was considered a sub-option in the 2016 Impact Assessment, whereas in the proposed solution assessed in this analytical note fingerprints are included. This is because the discussions on the 2016 proposal have clarified that there is strong support from the legislators for including fingerprints, even if discussions on the details of the implementation have not yet been finalised.

In this solution, the Member States would not share any identity information regarding convicted TCN directly with each other. The identity information would be centralised in an EU-wide system created for the purpose of dealing with ECRIS TCN and managed by eu-LISA. A Member State wishing to identify Member State(s) holding criminal record

[1] A description of the Ma³tch-software in detail can be found in Annex 5 of the Impact Assessment accompanying the Commission proposal of January 2016.

[2] The study identified that currently there is no mature technology on the market which would provide the necessary large scale one-to-many matching of fingerprints using pseudonymised or hashed templates. The Ma³tch-technology – which the Commission's original proposal relied on - works well for pseudonymised alphanumeric data, but is not suitable for fingerprints, as it would not produce equally accurate and timely results as for alphanumeric data.

information on a particular TCN can do so by performing a remote “hit/no hit” search in the central TCN system.

The solution has the following key characteristics:

- A central ECRIS TCN system is put in place under management of eu-LISA.
- Alphanumeric identity information of TCN convicted at national level is stored in the central ECRIS TCN system.
- Fingerprints of TCN convicted at national level are stored in the central ECRIS TCN system.
- Both alphanumeric and fingerprint data are used for enabling a centralised "hit/not" search.
- A Member State seeking to find the past criminal history of a particular TCN performs a “hit/no hit” search in the central ECRIS TCN system for identifying which other Member State(s) can be queried for information about these past convictions.

When a TCN is convicted in a Member State, the Central Authority of the Member State enters the alphanumeric identity information and fingerprints of the TCN into the local ECRIS TCN system. The local ECRIS TCN system transmits the fingerprints along with the alphanumeric identity information to the central ECRIS TCN system for storage.

If a Member State performs a hit/no hit search in the central ECRIS TCN, the central ECRIS TCN system performs two tasks:

- It triggers a one-to-many matching using its internal AFIS. The AFIS responds internally to the central ECRIS TCN system with a list of hits, including a unique technical reference provided by the convicting Member State for the fingerprints that caused the hit(s).
- It performs a search with alphanumeric identity information received from the requesting Member State to find corresponding matches in the database of alphanumeric information. This also results in a list of Member States with possible hits.

The central ECRIS TCN system then consolidates both lists of Member States where hits were found and provides this list as a response to the national ECRIS TCN system of the requesting Member State. In cases where a hit was found using fingerprints, any corresponding alphanumeric data could be provided as well, for the purpose of conclusive identification of the TCN concerned. The requesting ECRIS TCN system could then automatically generate draft ECRIS requests for the complete conviction information targeting the Member State(s) that were identified.

1.1. Variants A and B

For this solution two variants were considered and costed: variants A and B. They differ only in the way fingerprints are kept and processed at national level for the purposes of ECRIS TCN. In variant A, fingerprints of convicted TCN are stored at the national ECRIS TCN system. In variant B, the national ECRIS TCN system is linked to an existing external

national automated fingerprint database (AFIS)[3], that is then reused for the purposes of ECRIS TCN.

Member States may individually choose variant A or variant B. Whilst these variants influence the implementation costs at Member State level, they have no effect on the costs at EU level.

1.2. Direct access for Eurojust, Europol and the European Public Prosecutor's Office

The creation of a centralised system would make it possible to extend access to the database to other actors with a legitimate need to identify the Member State(s) holding conviction information on TCN. Whilst such direct access was not considered necessary for national law enforcement authorities, since they could obtain this information through their national criminal records authorities, direct access at the EU level for Eurojust, Europol and the European Public Prosecutor's Office (once established) was considered to be necessary, and in line with their mandates. Once they would have identified the Member State(s) possibly holding conviction information, they could make use of their exchange channels with national authorities to obtain the actual conviction information, without having to make use of the ECRIS system. Such direct access would also assist in the creation of a contact point at EU level for third States interested in obtaining criminal record information on TCN.

Cost estimates could not be established in the study as the main obstacle for estimating these cost impacts is the lack of detailed information on how many searches would be issued by Eurojust, Europol and the European Public Prosecutor's Office. It is therefore assumed that these costs will be borne by the budget of the respective organisations.

1.3. Creating a contact point at EU level for third States

Creating a contact point at EU level for third States requiring information on previous convictions would have the advantage that these States would no longer have to address multiple Member States with requests for such information, as is currently the case. Member State's ECRIS experts recognised the advantages of this approach. Nevertheless, it was stressed that this approach should not lead to the situation that the EU central contact point would give out any information on previous convictions, not even an indication as to whether or not such convictions may possibly exist. The European contact point would only inform the Member State(s) where a possible conviction had been identified through the use of the central ECRIS-TCN mechanism of the interest of the third State concerned. The Member State's authorities would then have full liberty in deciding whether or not information on previous convictions of TCN could be provided to the third State in question, in line with their national legislation. The implementation of this option would thus not create any change in the existing legal possibilities to exchange criminal record information with third States – it would merely ensure that requests from third States would need to be handled only by the Member State(s) concerned, in line with their national law. Eurojust was identified as the most suitable organisation to function as EU level contact point for this purpose.

1.4. Inclusion of conviction data in a fully centralised database

In the impact assessment accompanying the Commission's 2016 proposal, the option of creating a fully centralised database containing the identity information of the convicted persons, as well as the complete conviction information, was briefly discussed, but quickly discarded.

[3] National fingerprint databases containing fingerprints taken in the course of investigations and criminal proceedings in the Member States.

In the last years security issues have become much more prominent following the horrific terrorist attacks on European territory, in particular in Paris and Brussels. As a consequence, the political appreciation of issues surrounding data sharing and security has changed.

The inclusion of the actual conviction data in a centralised ECRIS-TCN database would avoid a "two-step-approach" where after a "hit" in the ECRIS-TCN mechanism, Member States must send a normal request for conviction information to the identified Member State(s) through the established ECRIS. If conviction data would be immediately and automatically available with a "hit" in the ECRIS-TCN database, response times which are currently 10 working days after receipt of the request, would be much shorter. Also, this could make the ECRIS-TCN mechanism more suitable for interoperability with other systems.

However, this approach was not supported by the Member States. Although the possible benefits where acknowledged, concerns on data control and data ownership prevailed. Most Member States want to maintain full control over their conviction data, as well as over the decision whether or not to provide that data in response to an individual request. This was also related to the fact that currently there is an obligation for Member States to reply to ECRIS requests only if the information is needed for the purposes of criminal proceedings. Requests for other purposes, such as border control, can be replied to or not, according to the national law of the requested Member State. This approach would be hard to maintain if all conviction information would be directly available through a centralised database.

In addition, this approach would not be in line with the principle of data minimisation, since the actual conviction data would be duplicated in both national criminal records registers and the central database at eu-LISA.

On the basis of these arguments, this variant was discarded without further analysis.

1.5. Inclusion of identity data of EU nationals in the centralised database

Another option discussed with the ECRIS experts in January 2017 concerned a centralised mechanism not only to identify Member State(s) holding conviction data on TCN, but also on EU nationals. This approach would offer the following advantages: the administrative burden for criminal records authorities would be lowered, as complete conviction data would not anymore need to be sent to the Member State(s) of nationality. Problems occurring from the convicted persons changing nationality would be avoided.

Member States are, however, reluctant to change the well-functioning ECRIS system for EU-nationals at this moment, even if the advantages of this alternative solution were recognised as well. Member States indicated that in their opinion now is not the right time for changing the whole system, but that this might be reconsidered in the near future. Member States therefore indicated their support for a review clause, so that the issue would be looked at again, after experience with the centralised ECRIS-TCN mechanism would have been gathered.

Such an approach would probably necessitate a total recast of the ECRIS Framework Decision, also touching on a number of other issues not yet considered. It could therefore have considerable impacts on the timing of the new proposal, possibly leading to unpredictable delays, and further effects on the technical implementation and on costs. This would not fit well with the high political priority and the inclusion of ECRIS TCN as a deliverable on the European Agenda on Security, as emphasised by the Member States and as confirmed by the Joint Declaration on the EU's legislative priorities for 2017.[4]

[4] https://ec.europa.eu/commission/publications/joint-declaration-eus-legislative-priorities-2017_en

On the basis of these considerations, this variant was not further analysed in detail.

2. STAKEHOLDER VIEWS

An extensive consultation strategy was developed to ensure a wide participation regarding the Commission's 2016 proposal. Consultations included included bilateral contacts, stakeholder- and experts meetings, and written contributions, providing the Commission with knowledgeable and representative opinions. The Commission has sought a wide and balanced range of views on this issue by giving the opportunity to all relevant parties (Member States, national authorities, lawyers and academics, fundamental right stakeholder, data protection stakeholders) to express their opinions, in particular the European Union Agency for Fundamental Rights (FRA), the European Data Protection Supervisor (EDPS) and the Art.29 Working Party, composed of Member States' data protection supervisory authorities. Further consultation with the EDPS and the Member States has also taken place in the preparation of the suplementary proposal. In addition, the issue was discussed in the Commission's Criminal Law Expert Group, consisting of academics and practitioners in the field of criminal law, on 23 March 2017.

The views of fundamental rights stakeholders, which were consulted prior to the Commission's proposal of January 2016, continue to remain valid. They acknowledged in general the positive effects of a future ECRIS-TCN mechanism from an overall justice perspective through its contribution to appropriate sentencing and protecting children from abuse, as well as the positive effects as regards legal certainty for persons with a clean criminal record. They advocated in principle for a decentralised system that would, in their opinion, entail less interference with the right to the protection of personal data in comparison with a central system at EU level.[5]

These stakeholders have also pointed out that introducing a TCN-specific system that would treat TCN differently from EU nationals is possible from the point of view of the principle of equality, to the extent that it respects the essence of this principle and is objectively justified as necessary and proportional. TCN-specific factors need to be taken into account here, as creating a centralised system entails some risk of adverse impacts on the fundamental rights of TCN, which should be mitigated. The stakeholders drew attention to the safeguards needed to address the specific situation of TCN in the context of migration, aspects related to the creation of an index and the use of fingerprints, the rights of the child, as well as the rights of data subjects and effective remedies.

In its Opinion 3/2016 on the Commission’s proposal of 19 January 2016, the EDPS appreciated pseudonymisation as an appropriate safeguard to limit the interferences to the right to private life and the right to personal data protection on the individuals concerned. He also appreciated the decentralised approach chosen by the Commission in its proposal of 19 January 2016, without excluding a centralised option.

In the Expert meeting of 10-11 January 2017, the Member States supported a central system containing only the identity data of convicted TCN, but rejected further centralisation of data, such as identity data of EU nationals, and the inclusion of conviction data in the centralised database (see also sections 2.4. and 2.5. above).

During the same Expert meeting the Commission also consulted the Member States on the possible repercussions of the work of the High Level Expert Group on Information Systems

[5] Fundamental Rights (FRA) Opinion 1/2015, Opinion EDPS 3/2016.

and Interoperability on the legislation underway. According to the Member States the emphasis should lie on quickly creating the ECRIS-TCN system. Whilst the other concepts were interesting, and the system should be designed to take possible future interconnections into consideration, the Member States confirmed that, in their opinion, the one element which should be implemented right from the start would be the use of the shared biometric matching service. In addition, Member States indicated that the possibility to store facial images should be created from the start, so that at a later stage facial recognition software could be deployed for even more effective identification.

3. ASSESSMENT OF THE PROPOSED SOLUTION

The proposed solution is discussed and assessed hereunder against the following criteria:

- *Effectiveness*: measured against the general and specific objectives.
- *Costs (set–up and ongoing)*: the total costs incurred for the European and for the Member States are estimated for the preferred solution. Some of the one-off costs may be compensated by EU funding under the form of co-financing and through a corresponding increase in EU costs. The Commission could co-finance up to 80% of the costs of proposals submitted by Member States fulfilling the Commission prerequisites required for co-financing. An overview of the costs is presented in the following sections.
- *Administrative costs*: these are the costs incurred by the Member States for the required day to day administrative business activities when performing the exchanges.
- *Impact on fundamental rights*: in particular on non-discrimination and data protection.
- *Information control and security*
- *Proportionality*

3.1. Effectiveness

As was the case for the options assessed in the Impact Assessment accompanying the Commission's 2016 proposal, the proposed solution is efficient in addressing the general and specific objectives, as argued below.[6]

- Specific objective: to replace costly blanket requests by a more efficient system to identify Member States holding criminal record information on TCN; thus, to encourage more systematic use of ECRIS for TCN.

The proposed solution would provide for a hit/no-hit search mechanism against both alphanumeric and fingerprint data of convicted TCN in order to identify the Member State(s) holding criminal record information. Inefficient 'blanket' requests and their costs can thus be avoided in all options. Since convicting Member States can be identified easily, the use of ECRIS with regard to TCN can be expected to significantly increase from the current 5%.

- General objective: to reduce and combat crime

The easy identification of the Member State(s) holding conviction information will ensure that ECRIS can be used equally effectively for both TCN and EU nationals. Using ECRIS to its full potential will put EU nationals and TCN on the same footing and contribute to

[6] See section 6.3. of that Impact Assessment.

reducing crime and fostering crime prevention. This aspect is therefore not assessed separately. See also section 3 of the 2016 Impact Assessment for more details.

3.2. Costs

3.2.1. Implementation costs (set-up and on-going)

Variant A

The one-off costs incurred by the EU for the establishment of a central system processing both alphanumeric data and fingerprints are higher than for a central system processing only fingerprints. However, the costs for the Member States would be significantly lower, leading to an overall more cost effective result.

Estimated costs (in €)	**One-off costs**	**Ongoing costs per year**
Variant A		
For the EU	13.002.000	2.133.000
For 28 MS	4.356.000	1.487.000
Total	**17.358.000**	**3.620.000**

Table 1 Total costs to set up (one-off) and yearly maintenance of Variant A

Variant B

The costs of processing of fingerprints might be higher for the Member States should they consider extending their national AFIS for ECRIS, instead of using a simple storage capacity as under Variant A.

Estimated costs (in €)	**One-off costs**	**Ongoing costs per year**
Variant B		
For the EU	13.002.000	2.133.000
For all MS	13.344.000	1.487.000
Total	**26.346.000**	**3.620.000**

Table 2 Total costs to set up (one-off) and yearly maintenance of Variant B

3.2.2. Administrative costs

Administrative costs for the Member States are calculated on the basis of the average cost of the required administrative activity. The administrative costs of the different options are not significantly different from when they were assessed in the 2016 Impact Assessment.

The administrative costs for the preferred approach are estimated at approximately €4 600 000 when the exchanges start and approximately €13 900 000 when the exchanges will reach their maximum capacity in normal operation.

The administrative costs for Variant A is slightly higher - respectively €4 700 000 at start and €15 900 000 at maximum - due to the fact that the verification of fingerprints upon the receipt of an ECRIS request is performed manually in Variant A, while in Variant B the verification is performed with the support of an AFIS.

3.2.3. Costs and technical complexity

Overall this centralised solution is better compared to decentralised solutions. Following further studies since the 2016 Impact Assessment, a centralised solution is less complex to implement compared to the decentralised solutions, in particular for the Member States. Costs at EU level will be higher due to the need to create and maintain a centralised database containing both fingerprint and alphanumeric data.

In evaluating the complexity, the main consideration was that the implementation of a central ECRIS TCN system could benefit from the experience of eu-LISA with proven technologies and successful implementation of already existing fully automated centralised systems such as EURODAC and the VIS. Decentralised solutions are considered feasible for the implementation of ECRIS TCN exchanges, however at higher complexity than the centralised options. In particular, these options would be more complex to implement for the Member States, requiring more elaborate changes to their national systems than centralised options. For the Member States the proposed solution is the least complex to implement, since they would only need to connect their national systems to the central system at eu-LISA for both alphanumeric and fingerprint data.

3.3. Fundamental rights/non-discrimination

Compared to the Commission's 2016 proposal, both fingerprints and identity data of TCN are processed at EU-level, whereas the identity data of EU-nationals is stored and processed at national level only. Such difference in treatment can be justified, if there are objective reasons for it. Although decentralised approaches based on other technical solutions are possible, they are costly and technically complex. The overall effect on the convicted TCN of the different options is the same, and the different technical approach would thus not lead to different results, provided that the central processing is safeguarded with appropriate data protection and data security measures.

Nevertheless, it can be argued that all options considered create a difference in the way conviction information of TCN and EU nationals are treated, since a separate mechanism is created to deal with TCN conviction information. However, these differences only relate to technical issues. This difference in technical treatment of the data is proportionate considering that the practical effect will be that under the new system conviction data of TCN and EU nationals can be obtained equally efficiently for the intended purposes of combating and preventing crime. The use of the identification data stored locally to confirm the identity of the TCN concerned serves to minimise false positive "hits" so that requests for conviction information are sent only to the Member State(s) which could hold conviction information.

In addition, the storage of data at the central level will have no discernible direct impact on the position of the TCN concerned. For them the effects are the same, irrespective of whether their data is stored at EU level or by the national authorities, since the usage of the data is in both cases limited to the identification of the Member State which holds actual conviction information.

The EDPS and the Fundamental Rights Agency (FRA) consulted in the context of the Commission's proposal dated 19 January 2016 and as set out in the Impact Assessment accompanying that proposal, expressed a preference for a decentralised system, as initially proposed by the Commission.

The preference of both the FRA and the EDPS for a decentralised system with a view to the right to privacy does not imply that in a centralised system privacy could not be equally well protected. Strong data protection- and privacy rules should apply both to centralised and decentralised processing of data. Equally, such rules exist and apply whether the personal data is stored in the Member States or at EU-level. The data protection rules require special safeguards for biometric data independent of whether they are stored decentrally or centrally. The data and the right to privacy can therefore be equally well protected both in the decentralised and centralised options.

3.4. Data protection

The proposed solution is characterised by the processing of personal data at both national and EU level. Therefore, the existing data protection rules for the current ECRIS decentralised system at Member State level have to be complemented with specific rules for the processing at EU level, in as far as these are necessary to complement the rules applicable under Regulation 45/2001. An additional data protection regime – similar to the one used for other already existing centralised information exchange systems at EU level – would therefore have to be put in place, which must complement Regulation (EC) 45/2001 with specific rules applicable only to the centralised database. The processing of personal data at eu-LISA is already covered by Regulation 45/2001, and will be governed by the successor to that Regulation, once agreed by the legislators.

In this fully centralised scenario, where identity information is shared directly only between the convicting Member States and eu-LISA, pseudonymisation as an additional safeguard is not necessary. It must be noted that the data protection rules do not require pseudonymisation, but pseudonymisation is mentioned as an example of how data protection principles can be safeguarded.[7]

Only Member States criminal records authorities and designated EU agencies will have direct access to their own data, which remain limited to identity data only. In case of a 'hit', the system will only provide indications as to which Member State(s) may hold criminal records information on the person concerned. The actual identity information can also be provided to Member States on their request, in as far as they need such data to conclusively confirm the identity of the persons concerned, so that they can avoid false positives and only send requests for conviction information to the Member State(s) must likely to actual hold such information. This would not be possible if only reference data would be provided together with the 'hit'. The identity data may not be used for any other purposes than verification of identity and preparing requests for conviction information.

As data duplication and data flows are minimised compared to the decentralised approach taken in the draft Directive proposed in January 2016, the safeguards which currently apply to the ECRIS (such as limitation of access rights and purposes, logs, secure communication infrastructure, storage limitations according to national law) and which are in line with data protection requirement are sufficient and proportionate.

---

[7] See Article 25 (1) of Regulation 2016/679 (General Data Protection Regulation), Art 20 (1) of Directive 2016/680 (Police Directive).

Also when considering data protection aspects, the main differences occur between the decentralised and the centralised approaches. Both approaches have both positive and negative data protection aspects associated with them. Whereas decentralised options can rely on a purely national data protection regime, centralised options require the creation of a specific regime to deal with the processing of personal data at the central level, which would supplement the applicable provisions from Regulation 45/2001. Whilst it could be argued that this creates an additional layer of complexity, there is no doubt that effective data protection regimes can be created at the central level. This is demonstrated for a large number of EU level information systems, including the SIS, the VIS, and Eurodac, which are all currently managed by eu-LISA. In addition, a centralised system would benefit from EU level control by the European Data Protection Supervisor. Furthermore, the proposed solution scores best on data security and data minimisation, since only central storage of identity data is foreseen, with no distribution to other Member States except in case of a hit, and at the request of the Member State querying the system.

A major downside of decentralised solutions is that personal data are distributed much more widely through these options than in a centralised solution, leading to less control by the Member States over their data, and increasing security risks. Although these risks can be mitigated through the use of pseudonymisation techniques, this would lead to more duplication of data, which is not in line with the principle of data minimisation. As discussed above, in the centralised preferred approach pseudonymisation is not required due to the strict access controls, and would be disadvantageous to trustworthy identification of the person concerned by the querying Member State before it sends its requests for conviction information. Pseudonymisation would not bring any additional benefits to the TCN concerned, since the actual conviction information will in all cases be provided in accordance with the applicable EU and national legislation.

All in all, the differences between the different options in terms of data protection are not such that they should be a decisive factor in the choice for the preferred solution.

3.5. Information control and security

As already indicated in the 2016 Impact Assessment, it would be necessary to agree rules on access rights, as well as rights to input, update, amend, rectify or delete data in the central system, as part of the additional data protection regime described in the previous point.

In particular, access to ECRIS TCN data must be limited to authorised staff in the performance of their tasks, both on central and national level. It must be ensured that the use of ECRIS TCN data is limited to that what is necessary, appropriate and proportionate for carrying out the respective tasks.

Data is kept in the ECRIS TCN system for the duration of the national retention periods related to the crimes committed. Convicting Member States will delete without delay data kept in the central system, when the corresponding data in the national criminal records systems are deleted according to national law. Every data subject can have the accuracy of his personal data checked and can require that inaccurate data about him/her is corrected and unlawfully recorded data is deleted by the convicting Member State. In order to exercise their rights, the persons concerned can address the central authority of any Member State..

The role of eu-LISA would be limited to technical operations, in particular maintaining the operation and the security of the system. It is the Member States that will be authorised to input, update, correct and delete data in the central system.

Security and logging measures must be agreed, put into place and maintained in order to enable monitoring that the principles above are respected and in accordance with the general principles of Regulation 45/2001 (or its successor regulation).

Each EU State must require a national supervisory authority to monitor the lawfulness of the processing of personal data by that country. The EDPS will monitor the activities at European level.

It should be noted that the information and security measures taken mirror the ones taken for other EU-information exchange system in the area of security and border control. These systems are equally hosted at eu-LISA and face similar challenges with regard to the protection of centrally stored sensitive/biometric data. The table below gives an overview of the types of identity data stored and used for the purposes of these large scale EU-data bases which are either already operational or in preparation (EES and ETIAS). Prüm is the only example of a decentralised database that also processes biometric data.

	Decentralised/ Centralised	Fingerprints	Facial Images	DNA
VIS (Visa Information System)	Centralised (eu-LISA)	+	+	
SIS (Schengen Information System)	Centralised (eu-LISA)	+	+	
EURODAC (EU asylum fingerprint database)	Centralised (eu-LISA)	+	+ (proposal)	
EES (Entry Exit System)	Centralised (eu-LISA)	+	+	
ETIAS (European Travel Information and Authorisation System)	Centralised (eu-LISA)			
PRÜM	Decentralised	+		+

3.6. Proportionality

The proportionality of this preferred approach is different with respect to the central processing of personal data. In this particular case, the duplication and centralisation of TCN personal data at EU level can be considered necessary, since it is now demonstrated that the objectives of the initiative could not be achieved equally well at national level.

4. CONCLUSION

The proposed solution scores best on all evaluation criteria, as discussed in detail in the study mentioned above. Member States can still choose independently of each other which of the variants A or B they would prefer.

Decentralised solutions are far more costly and more technically complex as well. Although there are some differences between the centralised and decentralised solutions, these

differences are not so important that they would justify spending a lot more resources at the EU and national level on the creation of decentralised solutions. It would therefore not be justified and proportionate to implement a decentralised solution bringing about higher costs and complexity without any significant substantive advantage for the processing of data on convicted TCN.

It should be noted that the total costs of the decentralised solution chosen as preferred option in the Impact Assessment accompanying the Commission proposal in January 2016 were considerably higher than the costs of the centralised approach taken now. As set out in the Impact Assessment, it is especially the integration of fingerprints into the decentralised TCN system that would generate high costs in the decentralised scenario. These costs would have to be borne by the Member States.

Estimated costs (in €)	**One-off costs**	**Maintenance costs per year**
Decentralised option with fingerprints		
For the EU	5 000 000	1 000 000
For all MS	37 500 000	11 500 000
Total	**42 500 000**	**12 500 000**

Table: 3 Total costs to set up (one off) and yearly maintenance of the preferred option, as resulted from the Impact Assessment accompanying the Commission's proposal in January 2016

If compared to the tables 1 and 2 presented under 4.2.2., it is clear that depending on the variant chosen by the Member States one-off costs would be at least three times higher for the Member States than in the centralised option chosen here. Total one-off costs would be at least 50% higher than in the centralised scenario. With regard to yearly maintenance costs, total costs would be almost four times higher than in the centralised solution, with the bulk of the costs to be borne by Member States.

In addition, creating a centralised system offers the additional advantages of creating the possibility of using a shared biometric matching service and common identity repository, facilitating direct access for Eurojust, Europol and the European Public Prosecutor's Office, (once established), and creating a central contact point for third States requiring information on convicted TCN. It also makes it possible to create a system which can be future-proofed for further interoperability with other EU level systems, if so decided by the legislators. Centralised systems are easier to interconnect than decentralised solutions.

Regarding data protection and security, there are no significant differences between the solutions considered, even if a central solution necessitate clear rules and a delineation of tasks between the Member States and the EU-level. EU level data protection rules offer the same protection as national regimes for national databases. Proven technology for security measures exists and is already in place for a number of large scale EU databases such as the SIS, the VIS and Eurodac.

With regard to non-discrimination between EU-nationals and TCN, the proposed solution centralises at EU-level identity data of TCN, whereas data of EU-nationals are kept and processed at Member State level. This is justified and proportionate, as demonstrated above, because the difference in processing their data does not lead to any substantial disadvantages for TCN. Any decentralised solution would be more costly and technically complex without completely eliminating different treatment, as also in decentralised solutions a mechanism built on identity data of TCN would be created that does not exist for EU-nationals. After all, all solutions aim at remedying the substantive inequalities that currently exist, as ECRIS is not equally efficient for TCN as for EU-nationals.