EUROPEAN
COMMISSION

Strasbourg, 19.1.2016
SWD(2016) 4 final

COMMISSION STAFF WORKING DOCUMENT

Impact Assessment

Accompanying the 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

{COM(2016) 7 final}
{SWD(2016) 5 final}

EN   **EN**

1. BACKGROUND AND POLICY CONTEXT

Efficient cooperation between Member States and exchange of information extracted from criminal records of convicted persons is a necessary cornerstone of a properly functioning common area of justice and security.

The European Council and the Justice and Home Affairs Council of Ministers have stated on several occasions that the exchange of information on criminal convictions is important in any strategy to combat crime and counter terrorism[1]. The improvement of the existing **European Criminal Records Information System** (ECRIS) is part of the European Agenda on Security[2].

ECRIS is an electronic system for exchanging information on previous convictions[3] handed down against a specific person by criminal courts in the EU for the purposes of new criminal proceedings against the same person and, if so permitted by national law, for other purposes. The system is based on Council Framework Decision 2009/315/JHA and Council Decision 2009/316/JHA[4].

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. Convicting Member States must send information and updates related to convictions handed down against a national of another Member State to the Member State of nationality. The Member State of nationality must store this information and can thus provide exhaustive, up-to-date information[5] on its nationals' criminal records upon request, regardless of where in the EU convictions were handed down.

> Example 1:
> A German national residing in Belgium was convicted of a criminal offence in France in 2013 and is now being prosecuted for a new criminal offence in Bulgaria. Bulgaria can receive complete criminal record information from Germany, i.e. the Member State of nationality.

---

[1] Riga Statement of the European ministers of Justice and Home Affairs of 29 January 2015; Conclusions of the Council of the EU on Counter-Terrorism of 20 November 2015, doc 14406/15; Conclusions of the Council of the EU on enhancing the criminal justice response to radicalisation leading to terrorism and violent extremism, of 20 November 2015, doc 14419/15; Council Conclusions adopted by the European Council at its meeting on 18 December 2015.

[2] '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.

[3] The annex of Council Decision 2009/316/JHA contains a list of criminal offences ranging from terrorism to other forms of crime

[4] 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. 23-32, 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. 33-48.

[5] Comprising information on the nature of the offence, the conviction and related sanctions or other measures.

Standardised electronic formats[6] allow for efficient and immediately understandable communication in all EU languages and within short deadlines[7]. Designated 'central authorities' in every Member State are the contact points in the ECRIS network, dealing with all tasks such as notifying, storing, requesting and providing criminal record information.

ECRIS became operational in April 2012. Member States have received financial support from the EU to implement the system. The Commission provides general support and technical assistance to the Member States and is responsible for the establishment and maintenance of the IT communication infrastructure. Today, 25 Member States[8] are interconnected. They exchange around 35 000 notifications and 25 000 requests per month, and these numbers are likely to increase (see graph in Annex 4).

The operation of ECRIS in Member States has been constantly monitored by the Commission in co-operation with Member States since April 2012, i.e. the implementation deadline for Member States in the 2009 Framework Decision. This has included the gathering and consolidation of statistical data (such as for example the volume of notifications and requests, the number of interconnections) of collected information from Member States, including information exchange related to third country nationals.

These findings on how ECRIS functions have been taken into account in drafting the Impact Assessment. The statistical data presented in Annex 4 of the report are the result of a monthly monitoring of the ECRIS 'workflow' in the Member States.

A Commission report on the implementation of Council Framework Decision 2009/315/JHA that will be presented at the same time as the Directive amending ECRIS, examines the way how Member States apply the rules of the Framework Decision, including the fact that ECRIS is not in use in all Member States.

2. PROBLEM DEFINITION

2.1. The problem

The current ECRIS legal framework does not sufficiently cover the particularities of requests concerning third country nationals and stateless persons (hereinafter: TCN)[9]. Although it is possible to exchange information on TCN through ECRIS today, there is no procedure or mechanism in place to do so efficiently. As TCN have no Member State of nationality, a complete overview of the criminal history of a particular individual must be requested directly from the convicting Member State(s). Generally, requesting Member States do not know in which Member State(s) a TCN has previously been convicted.

---

[6]   When exchanging criminal record information via ECRIS, Member States refer to codes as laid down in tables of offences and sanctions, including the parameters relating to the degree of completion and level of participation and, where applicable, the existence of total or partial exemption from criminal liability. The tables of offences (annexed to Council Decision concern all types of crime ranging from serious crime like terrorism or organised crime to driving without a licence or other offences

[7]   According to Framework Decision 2009/315/JHA replies to requests for the purposes of criminal proceedings shall be transmitted immediately and in any event within ten working days. For details, see Article 8 of Framework Decision 2009/315/JHA.

[8]   Malta, Portugal and Slovenia are currently not participating in ECRIS.

[9]   The JHA Council of 14 April 2005 decided to have separate strategies for exchanges of information concerning EU nationals and those concerning TCN.

- If one Member State wants to have this information, it has to send requests to all Member States ('blanket requests'). This creates an administrative burden in all Member States, including in (the majority of) countries not holding the requested information. The administrative burden of 'blanket requests' would amount to an estimated € 78 million per year if Member States were to request information each time a TCN faced conviction[10].

  The costs of replying to 'blanket' requests are not compensated by an equivalent benefit and are, in fact, lost because the majority of the replies will not return results. This is especially detrimental to smaller Member States required to respond to all requests without being necessarily well equipped to do so[11].

- A flood of unnecessary requests undermines confidence in the reliability and functioning of the ECRIS network as a whole, as users may conclude that the inefficiency of ECRIS-TCN is indicative of the inefficiency of ECRIS as a whole.

- In practice, Member States avoid sending 'blanket' requests and often rely only on information stored in their own national criminal record registers. This means that complete information on the criminal history of TCN is often not available to the responsible authorities in the Member States. In fact, although in 2014 558 000 TCN were convicted in 19 Member States[12], only 23 000 requests (from 25 Member States participating in ECRIS today) related to TCN convictions were made in ECRIS. If ECRIS had been systematically[13] used for TCN, the number of requests should have at least equalled the number of convictions. It follows from this that today, with regard to TCN, ECRIS does not even reach 5% of its potential.

2.2. The problem drivers

ECRIS is based on the principle that the Member State of nationality is the central point of contact for obtaining full criminal record information. With regard to TCN, Article 7(4) of Framework Decision 2009/315/JHA obliges Member States to transmit information contained in their criminal record registers to the same extent as provided for in Article 13 of the European Convention on Mutual Assistance in Criminal Matters (MLA Convention)[14].

---

[10] Out of the € 78 million, the largest economic cost element is the cost of responses to blanket requests which goes up to € 73 million per year. More details on these costs can be found in Table 4 of Annex 8 – Administrative cost calculation.

[11] Bigger Member States which generally have more convicted TCN would produce many more requests than Member States with smaller populations, if ECRIS was used systematically for TCN. If each Member State was to send unnecessary requests to all other Member States, the smaller Member States in particular would suffer, as they have to allocate a disproportionately high amount of their resources, designed for their own relatively moderate needs, to answering inefficient 'blanket' requests from other Member States.

[12] Number of convictions in 2014 as provided by 19 Member States (AT, BE, CY, CZ, DE, ES, FI, FR, GR, HU, HR, IT, LT, LU, LV, NL, PL, PT and RO).

[13] Council Framework Decision 2008/675/JHA stipulates that Member States judicial authorities take into account during criminal proceedings previous convictions handed down against the same person in other Member States. This implies that for every convicted TCN an ECRIS-request should have been made.

[14] Art. 13 of the MLA Convention reads:
1. A requested Party shall communicate extracts from and information relating to judicial records, requested from it by the judicial authorities of a Contracting Party and needed in a criminal matter, to the same extent that these may be made available to its own judicial authorities in like case.

This means:

- Framework Decision 2009/315/JHA does not define a Member State of reference as a single point of contact to which relevant criminal record information has to be transmitted. The Council Decision 2009/316/JHA also does not contain any storage obligations regarding convictions in respect of TCN.

- Criminal record information on TCN must therefore be requested directly from the convicting Member State(s). However, Framework Decision 2009/315/JHA does not provide for a mechanism to identify Member State(s) having convicted a particular TCN.

- With regard to TCN, Framework Decision 2009/315/JHA[15] refers to Article 13 of the MLA Convention. The provisions in the MLA Convention do not address the deficiencies of ECRIS regarding TCN listed above, as they also do not provide a mechanism to identify Member States holding relevant criminal record information. Moreover, the MLA Convention does not provide for electronic, speedy and standardised information exchange with certain strict time limits (as ECRIS).

2.3. The effects of the problem

- **Criminal proceedings**

   Council Framework Decision 2008/675/JHA[16] stipulates that Member States judicial authorities should, during criminal proceedings, take into account previous convictions handed down against the same person for different facts in other Member States, irrespective of the nationality of the person concerned. This concerns decisions taken at the pre-trial stage, the trial itself and at the time of execution of the conviction. Previous convictions have to be considered when deciding on provisional detention, the offence committed, the type and level of sentence and the rules governing the execution of the decision.

   Example 2:
   A national of Turkey is accused of having committed a crime in Poland. He has been previously convicted for a similar criminal offence in Sweden, where the execution of the penalty was suspended. As the judge of the criminal court in Poland is not aware of the previous conviction, he hands down a penalty which is again suspended. If the judge in Poland had known about the earlier conviction, he would have been obliged to take that into consideration.

   Member States cannot fully implement Framework Decision 2008/675/JHA with regard to TCN if previous convictions in the EU are not available to national judicial authorities.

   Example 3:
   An American national residing in Belgium was convicted in France in 2013 and is now being put on trial for a new criminal offence in Bulgaria. The Bulgarian court is

---

2. In any case other than that provided for in paragraph 1 of this article the request shall be complied with in accordance with the conditions provides for by the law, regulations or practice of the requested Party.

[15]   Article 7(4) of Framework Decision 2009/315/JHA
[16]   Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings, OJ L 220, 15.8.2008, p. 32.

> *only in a position to take account of the recidivist nature of the new criminal offence and adapt any sanction accordingly if complete criminal record information is available.*

- **Investigation and prosecution phase**

  Previous convictions are a source of important background information on suspects and perpetrators, including instigators and accomplices.

  If previous convictions are unknown, the context of an offence might be overlooked and links to organised crime, terrorist crime or other serious forms of crime may not be detected. This may have an impact on the choice of investigative tools (e.g. phone tapping, undercover agents), urgent decisions (e.g. to arrest or detain a person), the deployment of staff, the priority of the prosecution as well as the scope of investigation (e.g. extension to possible accomplices).

  > *Example 4:*
  > *Pre-trial detention decisions depend (among other criteria) on previous convictions of the suspect. Imagine a case where a Bulgarian national and a Serbian national are both suspected of having committed a crime in Austria. Both have previously been convicted for a similar offence in France. The investigative judge only has information through ECRIS on the conviction concerning the Bulgarian national. He therefore decides to detain only the Bulgarian national. The Serbian national – under the same circumstances – is not detained.*

  Only complete information puts the competent law-enforcement and judicial authorities (police, magistrates and prosecutors) in a position to react adequately, to apply the right measures and to combat such crimes.

- **Crime prevention**

  Full information on a person's previous convictions is important to prevent the same type of crime being committed again by the same person.

  Prevention of sexual crimes involving children

> *Example 5:*
> *One of the most prominent examples in this context is a case of child abuse detected in the Netherlands in 2010. A child minder confessed that he had sexually abused between 40 and 50 toddlers in two day-care centres in Amsterdam. The man, of Latvian origin, had previously lived and worked in Germany and was convicted for the possession of pornographic images of children. He moved to the Netherlands, where he acquired Dutch nationality. He was recruited as a child minder in Amsterdam after having presented the mandatory 'Declaration of Good Conduct', based on a clean Dutch criminal record.*

The importance of protecting children against sexual abuse and exploitation led to the adoption of Directive 2011/93/EU[17]. The Directive obliges Member States to transmit information on convictions concerning sexual crimes against children through ECRIS if so requested for the purposes of pre-employment checks on persons seeking to be recruited for an activity involving direct and regular contact with children. Directive 2011/93/EU cannot be fully be implemented, as ECRIS is deficient with regard to the exchange of criminal record information on TCN.

Protection of vulnerable persons and security-sensitive areas

Complete criminal records also allow effective pre-employment screening with a view to protecting vulnerable groups, such as elderly, sick or otherwise helpless people. Screenings are likewise important for employers recruiting security personnel or personnel having access to sensitive areas or information.

Administrative decisions

A number of administrative decisions may, according to national law, require previous checking of a person's criminal history. Such administrative decisions cover a broad range and can be related to licences for firearms or other hazardous materials, residence permits, visas and naturalisation, the adoption of children or the choice of foster care parents.

- **Cost of crime**

  Inactivity with regard to crime prevention is very costly to society as a whole, in both economic and social terms. Economic costs are born largely by victims (direct economic losses suffered by crime victims, including medical care costs, lost earnings, and lost or damaged property), criminal justice systems (local, state, and federal government funds spent on police protection, legal and adjudication services, and correctional programmes, including imprisonment), and society as a whole (opportunity cost associated with a criminal's choice to engage in illegal rather than legal and productive activities). Social costs might be intangible (indirect losses suffered by crime victims, including pain and suffering, decreased quality of life, and psychological distress), loss of citizens confidence in security, the functioning of their public authorities and social cohesion.

---

[17] Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 13 December 2011, OJ L 335, 17.12.2011, p. 1.

The total cost of crime committed by TCN in the EU is unknown. Various organisations, authorities and universities have carried out studies on the costs of crime at Member State level and for different areas of crime and groups of offences, but those are not comprehensive and often not up to date. There is no comprehensive data available on the cost of crime at European level.

- **Unequal treatment of EU nationals and TCN**

Uneven levels of information with regard to previous convictions in another Member State lead to unequal treatment of TCN and EU nationals in all areas where information on previous convictions influences decision-making (during criminal investigations, at the pre-trial stage, at the trial itself and at the time of execution, in employment procedures, in naturalisation and permanent residence permit procedures, etc.).

2.4. Problem Tree

The problem, main drivers and effects as described above are illustrated in Figure 1 below.
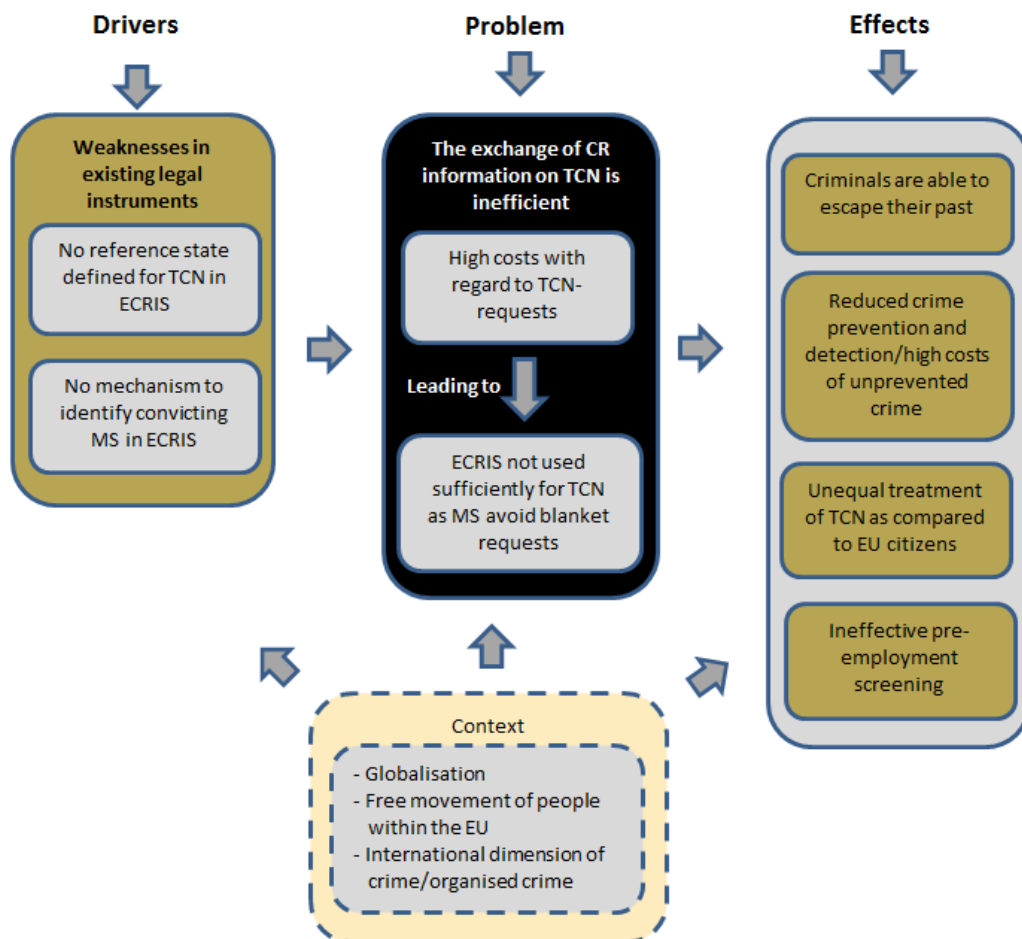

**Figure 1: Problem Tree for ECRIS TCN**

2.5. The size of the problem / Baseline scenario

According to Eurostat information, TCN residing legally in the EU on 1 January 2014 accounted for around 4% of the total EU population, which brings the total number of TCN

legally residing in the EU to around 20 million persons[18]. The number of TCN residing in the EU is expected to increase in the future.

Graph 1 below illustrates over a five-year period the number of convictions of TCN in the EU, based on the data received from 19 Member States[19]. As not all Member States have provided information, the total number of TCN convictions would most likely be higher[20].
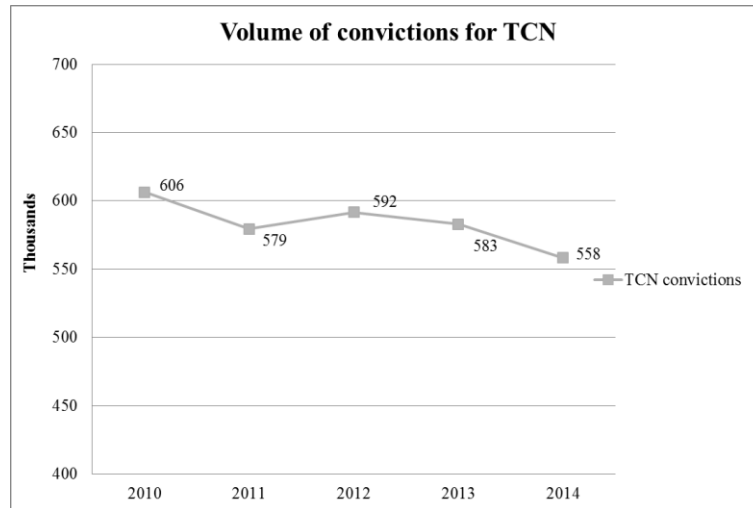
Graph 1: The number of convictions of TCN per year in the EU (for 19 Member States)

In 2014, 23 000 requests were made through ECRIS concerning TCN. That means that 95% of the convictions of TCN (654 000 convictions) were handed down without use of ECRIS regarding possible previous convictions of individuals in another Member State. By the end of 2015, 28 000 requests concerning TCN through ECRIS are anticipated. The number of TCN in the EU is expected to increase considerably in the future[21].

Greater efficiency in dealing with ECRIS requests regarding TCN may come from technical improvements such as further automation of criminal record registers at national level. As a consequence, exchange of information regarding TCN could be facilitated and increased. However, such improvements would depend on voluntary activity by Member States and would be driven by domestic needs. It cannot be expected that uncoordinated action at Member State level would produce sufficient effects of scale to improve the overall use of the system.

Other EU-measures envisaged in the context of information change and cooperation with regard to combating and preventing crime do not solve or alleviate the problem of deficient criminal record information exchange regarding convicted TCN. The improvement of

---

[18]   Source: Eurostat, Migration and population statistics.
[19]   Number of convictions per year as provided by 19 MS (AT, BE, CY, CZ, DE, ES, FI, FR, GR, HU, HR, IT, LT, LU, LV, NL, PL, PT and RO). More details on the volume of convictions can be found in Annex 11.
[20]   Member States not having submitted information have stated that the requested figures are not recorded in their national systems or are unreliable.
[21]   As regards asylum applications and illegal immigration, see European Migration Network: Annual report on Immigration and Asylum 2014; as regards immigration of skilled people, see European Agenda on Migration, COM (2015) 240 final, page 14.

information exchange regarding criminal convictions cannot be replaced by any other EU instruments of information exchange such as SIS II, the "Prüm" information exchange mechanism and EURODAC[22], as these are designed to serve different purposes. In particular, the SIS does not contain systematic information on convictions and is designed for temporary storage, until its purpose is fulfilled; the Prüm exchange mechanism concerns fingerprints, DNA and vehicle information only, and EURODAC only contains data on asylum seekers. The Prüm system, EURODAC and the VIS do not hold information on convictions, i.e. a hit would not identify a Member State holding criminal record information as it might relate to an individual without a criminal record.

3. EU RIGHT TO ACT

A legal instrument establishing an ECRIS TCN supplementing the ECRIS system would be in the form of a Directive based on Article 82(1)(d) of the TFEU.

Legal basis

Article 82(1)(d) is the legal basis for the Union's right to act in the field of judicial cooperation in criminal matters to facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions. Legislative action would amend the existing EU legislation in this area.

Subsidiarity

Improvement of an existing system to exchange criminal record information on convicted TCN cannot be done at Member State level. A common mechanism aiming at a standardised, rapid, coordinated and efficient information exchange between Member States requires concerted action. This can neither be achieved unilaterally at Member State level nor bilaterally between Member States but is by its nature a task to be undertaken at EU level.

4. POLICY OBJECTIVES

General objective	To improve the functioning of a common area of security and justice by improving information exchange in criminal matters.
	To reduce crime and foster crime prevention (including terrorism).
	To ensure equal treatment of TCN and EU nationals with regard to an efficient exchange of criminal record information.

Specific objectives	To reduce the number of unnecessary requests for TCN-related criminal record information and the resulting costs.
	To increase criminal record information exchange through ECRIS with regard to TCN.

---

[22] For an overview on the existing systems to exchange data in the field of police and judicial cooperation see Annex 10.

5. **POLICY OPTIONS**

5.1. **Option 1: Maintaining the status quo**

See section 2.5. – The size of the problem/Baseline scenario.

5.2. **Option 2: Non-regulatory option – EU co-financing of a Member State voluntary project**

The Commission could co-finance a voluntary Member State project for a more efficient mechanism to exchange criminal record information on TCN.

Before the entry into force of the ECRIS Framework Decision, a group of Member States created the 'Network of Judicial Registers' (NJR)[23] for the purpose of exchanging criminal record information. This project started with two Member States and, before being transformed into ECRIS, had 16 members and seven observers. The development and achievements of this project, in particular the IT architecture and the standardised exchange formats, were the basic inspiration for the current ECRIS system.

Through the Justice programme, the Commission could co-finance costs incurred in implementing, running, using and maintaining a tool allowing the exchange of criminal record information on TCN (necessary software, training). In addition, it could co-finance adjustments needed at national level (in the framework of the Justice programme or the Connecting Europe Facility.

5.3. **Regulatory options**

A regulatory option involves amendment of the existing ECRIS legal framework to overcome the identified deficiencies in searching for criminal convictions of TCN, and should be built on and integrated into the existing legal framework as far as possible. It must be noted that a regulatory option would improve the current ECRIS legal framework but not broaden its scope. It would in particular not aim at regulating criminal record information exchange with third countries.

An index-based hit/no hit search mechanism

To improve ECRIS with regard to TCN, it would be necessary to identify successfully the Member State(s) holding criminal record information on a particular TCN.

As far as ECRIS is concerned, Member States would have to extract identity data of convicted TCN from their national criminal record registers and feed them into a separate index-filter. Identity data contained in national criminal record registers may comprise for example the name, date and place of birth or the address of a person.

This index could be electronically searched by other Member States by means of a hit/no hit search mechanism. Those Member States introduce into the searching engine identity data for a TCN they need information about. The search engine would search the connected index-filter(s) of other Member State(s) for matching information. A 'hit' would indicate available information on a TCN whose identity data match, as well as showing the Member State which can provide the information. The identified Member State(s) would then be requested to provide complete information through the established ECRIS. 'Blanket' requests would no

---

[23]   Prior to ECRIS' entry into force, several Members States were exchanging information on criminal records electronically, within the framework of the pilot project 'Network of Judicial Registers' (NJR). The achievements reached by this project were the basic inspiration for the ECRIS system.

longer be necessary. It is only the national index-filters that can be searched by other Member States, not the national criminal record registers as such.

> *Example 6:*
> *In the case of an American national residing in Belgium who committed an offence in France in 2013 and is now being prosecuted for a new offence in Bulgaria, Bulgaria could check in the index-filter to see which other Member State holds information on the American national. Bulgaria would receive a 'hit', telling them that France has information. Bulgaria would send a request only to France for more detailed criminal record information.*

Member States would have to update the index-filter regularly. This should ideally happen through a fully automated process together with the entry of new data/deletion of data in the national criminal record register.

Experience gathered from operational information exchange systems shows that index-filter-based searches produce good results[24]. Intelligent search mechanisms can overcome differences in the spelling of names. Multiple 'hits' can be reduced by adding more information on the person concerned.

Different existing IT solutions such as for example the direct access to criminal record registers were considered. Most of them were discarded for different reasons. For example the exposure of databases was assessed unacceptable for Member States[25].

Two potentially realistic IT solutions were short-listed: 1) the IT solution "Ma3tch" used by FIU.net which is described in more detail in Annex 5, 2) and the IT solution used for the European Police Record Information System (EPRIS).

1) The FIU.net is a decentralised network aiming at identifying suspicious financial transactions in the EU. Data exchanged in the FIU network consists mainly of bank account identification information such as first names, last names, date of birth, and if necessary other relevant information such as account number, amount of transfer, etc. From 2012, as more and more Member States joined the FIU network, the FIU bureaus were facing a growing number of requests whereas their means remain limited. That is why specific software - the Ma³tch[26] hit/no hit software - was developed in order to efficiently detect if specific information was available in other Member States. Ma³tch software has already been used since 2012 to convert FIU data into anonymised information which is safely shared with other FIUs.

2) Under the EPRIS initiative, a prototype project[27] is currently assessing the feasibility of exchanging information in a semi-centralised architecture using anonymisation techniques for

---

[24] The **Prüm Decision** introduced procedures for fast and efficient data exchange in specific areas. The core of the Prüm framework lays down provisions under which EU Member States allow each other searches in the DNA analysis files, fingerprint identification systems and vehicle registration data bases. DNA and fingerprint searches are based on a 'hit/no hit' approach, which means that DNA or fingerprint profiles can be compared with profiles held in the databases of other EU Member States.
FIU.net, located in the Netherlands, is a platform connecting Financial Intelligence Units from the Member States. Its purpose is to detect and disrupt terrorist finance and money laundering activities.

[25] Outcome of a meeting held with ECRIS Experts on 17 September 2014.

[26] Ma³tch stands for Autonomous Anonymous Analysis.

[27] The prototype project – called Automation of the data exchange process (ADEP) - is led by Germany and France. Finland, Hungary, Spain and Europol are also participating to the project.

hit-no/hit searches. The prototype project could lead to a pilot in 2016. While this IT solution could potentially be an alternative to the FIU.net solution, it would not come in time.

Apart from the EPRIS and the FIU.net solutions, no other existing proven technology is used so far. From an in-depth assessment of these IT solutions, it emerged that the IT solution "Ma3tch" already used by the FIU.net would meet the needs of the ECRIS TCN system. This choice was assessed favourably by the ECRIS experts[28]. More details of the specific FIU.net technology described in this option can be found in Annex 5.

There are two possible ways to operate an index-filter-based hit/no-hit search mechanism: the index-filter could be stored and searched either at Member State level (decentralised) or at European level (centralised).

5.3.1. Option 3 - decentralised option

In the decentralised option, Member States extract identity information on TCN from their national criminal record registers and feed them into a separate file. This would happen automatically or manually depending on the level of automation at Member State level. The identity data contained in the file would have to be anonymised meaning that personal data of convicted TCN would be irreversibly transformed into locks (filters) that would not allow the transformed data to be changed back to data on individual persons. The anonymised list of convicted TCN thus becomes the 'index-filter'. Each Member State would distribute its national index-filter to all other Member States through the established secure communication infrastructure "s-TESTA" (as is the case in the existing ECRIS where information exchange is done via this IT infrastructure operated by the Commission) and regularly[29] send updates.

Example 7:
Member State A includes for a TCN identity data in its criminal record information system, e.g. Anna Miller. The identification data undergoes an anonymisation process using specific software that replaces the personal data (Anna Miller) by a code such as for example '001110'. This code is distributed to all other Member States enabling them to search at their own premises. When Member State B searches for Anna Miller, the search software will convert this personal data into a code using the same anonymisation rules. If both codes match (e.g. 001110), a hit is returned and Member State B knows that Anna Miller has a criminal record in Member State A.
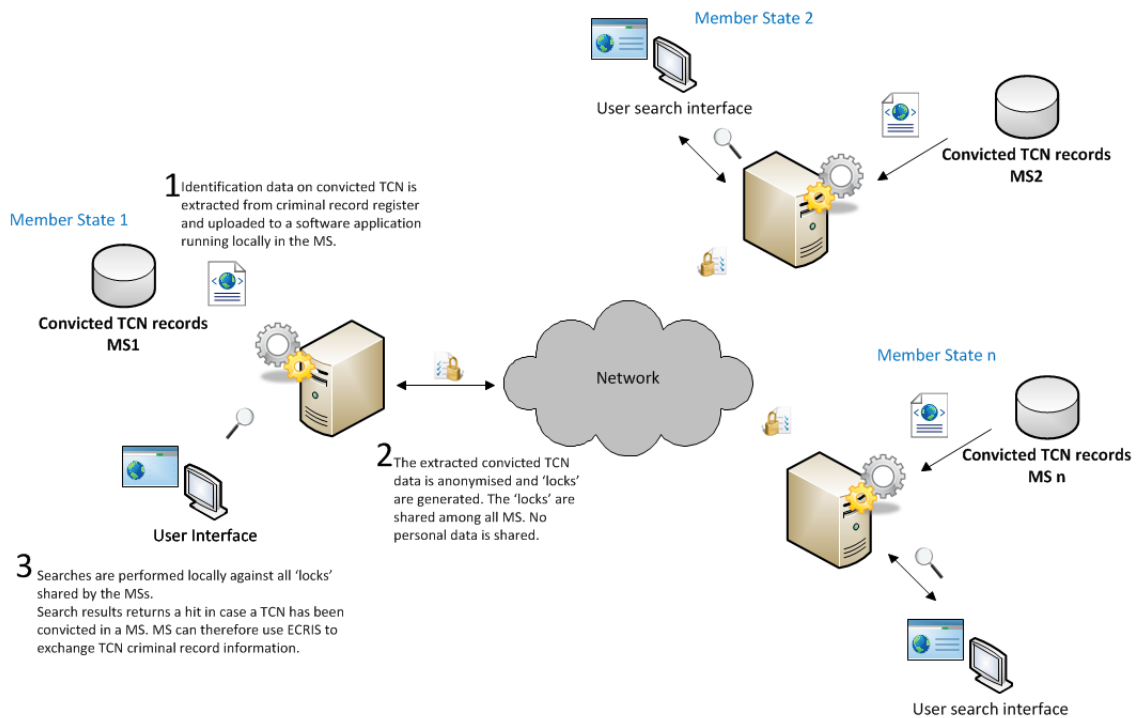
Option 3 differs from the current ECRIS and also from option 4 in that the data would be anonymised. The reason is that in option 3 Member States would have to distribute their national index-filters to all other Member States and not only transmit data to one single contact point. Option 3 therefore multiplies data flows. Anonymisation of the distributed data is a necessary prerequisite for ensuring that these data flows are justified and proportionate from the point of view of data protection.

As a consequence, all Member States would be in a position to search anonymised, up-to-date index-filters of other Member States at their own premises. There would be no exchange of personal data at that stage. The convicting Member States maintain full ownership of the identity data of TCN convicted by their national courts.

---

[28]   Outcome of a meeting held with ECRIS Experts on 18 September 2015.
[29]   The frequency of the updates would have to be determined at a technical level.

The decentralised option

Member State 1
Convicted TCN records MS1
User Interface

1 Identification data on convicted TCN is extracted from criminal record register and uploaded to a software application running locally in the MS.

Member State 2
User search interface
Convicted TCN records MS2

Network

2 The extracted convicted TCN data is anonymised and 'locks' are generated. The 'locks' are shared among all MS. No personal data is shared.

Member State n
Convicted TCN records MS n
User search interface

3 Searches are performed locally against all 'locks' shared by the MSs.
Search results returns a hit in case a TCN has been convicted in a MS. MS can therefore use ECRIS to exchange TCN criminal record information.

### 5.3.2. Option 4 - centralised option

This option would be based on a central index-filter and a hit/no-hit mechanism to be set up at EU level. As with the decentralised solution, Member States would extract identity data of convicted TCN from their national criminal record registers. Member States would have to transmit this data to a central point of storage at EU level. Searches would be done online in the centralised common index.

Unlike in the decentralised option, the index would not be anonymised[30]. The communication infrastructure s-TESTA would ensure the security of the data transmitted. In option 3, identity data of convicted TCN is distributed to all other Member States, but in option 4 the identity data is only sent to one contact point at EU level. There is therefore less need to anonymise the exchanged data.

A central index of this kind could be managed by an existing EU agency such as EU-LISA or Eurojust, or by the Commission.

---

[30] Option 4 combined with an anonymised index (hybrid solution) is discussed under section 7 as a discarded option. See for further explanation under 7.3.

The centralised option
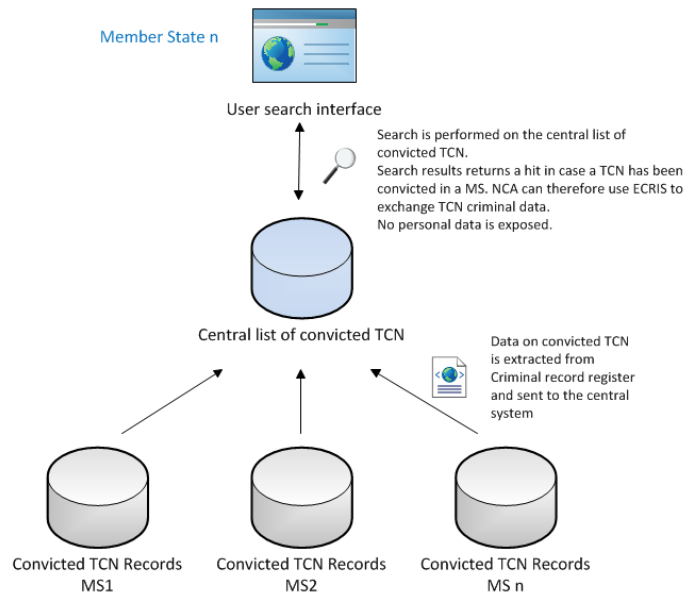
5.3.3. Sub-options to options 3 and 4: Fingerprints

A reliable system for the exchange of information on TCN convictions requires a sufficient degree of certainty regarding the data identifying a specific person. Identity criteria used by Member States in their criminal record systems tend to vary considerably. Some Member States rely on names (of the person concerned, the father's name, the mother's name, or both), date and place of birth, nationality, country of birth and sex to identify a person's identity. Others require a registration number. Yet other countries have organised identification of persons based on fingerprints. Despite the differences, Member States have reached an agreement on compulsory and optional information to be exchanged through ECRIS regarding requests on convicted nationals.

However, spelling mistakes or errors e.g. in dates of birth are not uncommon, due partly to different alphabets and languages within the EU and worldwide. Generally, the use of aliases and of false identities is common practice among members of cross-border organised crime groups seeking to escape identification.

Establishing the identity of TCN is often particularly difficult, if not impossible, because of the use of different alphabets, languages, widely used common surnames[31] or because reliable identity documents do not exist or are missing. Against this background, the introduction into ECRIS of a fingerprint exchange and matching system would be desirable. Fingerprints can contribute considerably to the certainty of identifying convicted persons and also improve certainty of verification that a particular person has not been convicted.

With regard to EU nationals, ECRIS provides for the use of fingerprints as a voluntary tool in addition to alphanumeric identification. At present, with regard to EU nationals, the Member

---

[31] For example, the top 10 surnames in mainland China account for about 40% of Chinese people in the world, with the most common surname Li, romanised as Lee, Li or Le, being used by 95 000 000 people (example from Unisys study, page 39).

State of nationality may store transmitted fingerprints (according to national law). Member States' central authorities are obliged to transmit fingerprints which have been taken from convicted persons to the Member State of nationality, where fingerprints are available according to national law[32].

There is no equivalent provision regarding TCN in the ECRIS legal framework.

5.3.3.1. Sub-option 1: *mandatory fingerprint exchange*

The legislative text could contain a provision whereby all Member States would have to store/use fingerprints (in addition to alphanumerical data) for identification of TCN through ECRIS, and to include fingerprint information in the index-filter (in the decentralised option), or in the central database (in the centralised option) Requesting Member States (through their central authorities) could then directly search using fingerprint identifiers. It must be noted that the conditions under which Member States store fingerprints during criminal investigations and proceedings are not harmonised by European law.

There would be several possibilities for putting this into practice.

(1) mandatory usage of fingerprints for ECRIS-TCN

Mechanisms allowing for the extraction of fingerprints of convicted TCN from existing national fingerprint identification systems and their storage as an additional identifier could be developed. The data would be sent either to all other Member States in anonymised form (option 3) or to a central body at EU level (option 4). As with all other information, this would need to be updated regularly (and automatically).

(2) obligation to use existing databases storing fingerprints

Member States could be obliged to use existing data exchange systems based on fingerprints to conclusively identify TCN before using ECRIS to request conviction information. At a European level, existing large-scale information exchange systems based on fingerprints include EURODAC[33], the VIS[34] and the Prüm mechanism. The most suitable system in the

---

[32]   Art. 11(1)(c)(ii) of Framework Decision 2009/315/JHA. Today the following eight Member States exchange fingerprints in ECRIS: EE, ES, FI, UK, LT, LV, RO and SE, and only a few include fingerprints in their criminal records (UK, PT, LV) or have a link between their criminal records and their fingerprint database(s) (LT, HU, RO).

[33]   The EURODAC system enables the Member States as well as countries that apply the Dublin Regulation on the basis of international agreements (Iceland, Norway and Switzerland) to help identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the European Union. By comparing fingerprints, Member States can determine whether an asylum applicant or a foreign national found to be illegally present within an EU country has previously claimed asylum in another EU country or whether an asylum applicant entered the Union territory unlawfully. In addition, national police forces and Europol are allowed to compare fingerprints linked to criminal investigations with those contained in EURODAC. This will take place under strictly controlled circumstances and only for the purposes of prevention, detection and investigation of serious crimes and terrorism. Eurodac consists of a Central Unit within the Commission, equipped with a computerised central database for comparing fingerprints, and a system for electronic data transmission between EU countries and the database. See also http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/identification-of-applicants/index_en.htm.

[34]   The Visa Information System (VIS) allows Schengen States to exchange visa data. It consists of a central IT system and a communication infrastructure that links this central system to national systems. The VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for

context of ECRIS would be the Prüm mechanism[35], a system connecting Member States' national fingerprint identification systems (AFIS) by means of a 'hit/no hit' search tool, which allows for fingerprints to be compared between Member States. The Prüm mechanism aims at data exchange in order to combat and prevent crime. Searches with fingerprint identifiers using the Prüm mechanism are permitted for the prevention and investigation of criminal offences. For the purposes of ECRIS, central authorities could be obliged to ask their national Prüm contact points to identify a person and the Member State holding information on the person. Then ECRIS could be used to obtain conviction information if available in the identified Member State.

However, the Prüm mechanism does not currently offer the capacity needed to respond to a steep increase in the number of requests produced, if it was to be systematically used for convicted TCN. Capacity is a problem and the number of requests per day and per Member State is restricted. Moreover, to date only 18 Member States participate in the Prüm exchanges.

Anonymisation of fingerprints (as would be required under option 3) is technically possible. Anonymised fingerprint matching technology exists and is already in use in, for example, election processes[36]. Nevertheless, a technological solution would need to be developed and implemented to allow for the matching of anonymised fingerprints within the context of cross-border exchanges between EU Member States.

5.3.3.2 Sub-option 2: *Voluntary use of fingerprints for ECRIS-TCN*

In this sub-option, the current legal situation for ECRIS would be extended to TCN. Fingerprints could be allowed as an additional and voluntary tool for Member States according to their national law. This would pave the way for exchange of fingerprint information as is currently the case for EU nationals, for the purpose of confirming alphanumerical identity information. It would not allow for automatic comparison of fingerprints for identification purposes. A request based on fingerprints would be successful if both the requesting and the convicting Member State allow for the use of fingerprints.

5.4. Stakeholders' views on the problem and the options

All Member States acknowledge the need to improve the exchange of criminal records information on TCN.

---

identification and verification purposes. See also http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm.

The Prüm Decision (Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L210, 6.8.2008, p. 1) introduced procedures for fast and efficient data exchange in specific areas. The core of the Prüm framework lays down provisions under which EU Member States allow each other searches in their DNA analysis files, fingerprint identification systems and vehicle registration databases. DNA and fingerprint searches involve a 'hit/no hit' approach, which means that DNA or fingerprint profiles can be compared with profiles held in the databases of other EU Member States. The automated reply gives information on whether this profile exists in the requested Member State. Additional personal information needs to be requested separately. The Prüm Decision should have been implemented fully by Member States by August 2011. So far 18 Member States have implemented the fingerprint data category. DK, EL, HR, IE, IT, PT, BE, PL, SE and UK are currently not participants in Prüm. However, UK, PL, BE and SE are expected to join soon.

[36] Example of a fingerprint-based system for obtaining an accurate and credible voter list, http://www.genkey.com/en/markets/elections

All Member States support a regulatory option and an index-filter-based hit/no-hit mechanism. A large majority of Member States could support the decentralised option on condition that the implementation software can be installed, integrated and maintained smoothly at Member State level and that financial support (grants) would be available. Some Member States favour the centralised solution, as they consider that it would demand less implementation effort at Member State level, would be less costly for Member States and would better secure a common approach of the Member States. A few Member States are undecided.

While the practical advantages with regard to secure identification of a person are acknowledged by many of them, a number of Member States have expressed constitutional concerns and drawn attention to problems regarding the practical implementation of mandatory fingerprints in ECRIS. Many Member States do currently not use fingerprints in their national criminal record registers or are connected to their national AFIS. Likewise, some Member States are concerned about possible double standards for EU nationals on the one hand and TCN on the other hand and the fact that not all convicted persons contained in the national criminal record registers have had fingerprints taken, as national rules differ according to categories of offences and between Member States.

Fundamental rights stakeholders acknowledge in general the positive effects of a future ECRIS-TCN system from an overall justice perspective by contributing to appropriate sentencing and protecting children from abuse, as well as the positive effects on TCN as regards legal certainty for persons with a clean criminal record. They also advocate the decentralised system accompanied by adequate anonymisation techniques (option 3) that would, in their opinion, entail less interference with the right to the protection of personal data in comparison with an index-filter centrally established at EU level.

They have 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. The TCN-specific factors need to be taken into account here as such a system entails some risk of adverse impacts on 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-filter and use of fingerprints, rights of the child, as well as the rights of data subjects and effective remedies. For more details see Annex 2 on Stakeholder consultations.

6. ANALYSIS OF IMPACTS OF POLICY OPTIONS

The options are discussed and measured against the following criteria:

- *Effectiveness*: the extent to which the measure fulfils the objectives of the proposal

- *Costs*

- *Administrative costs*: workflow, day-to-day business

- *Impact on fundamental rights*: in particular on equal treatment and data protection

- *Information control and security:* with regard to the information to be fed into the index-filter

- *Proportionality*

6.1. Option 1: Maintaining the status quo

See section 2 – problem definition

6.2. Option 2: Non regulatory option – EU co-financing of a Member States' voluntary project

One advantage of a Member States' project is that it might be put in place quickly (or quicker than a regulatory option). Information control and security standards could be determined by the participating Member States. The impact on data protection would be similar to a regulatory option (see 6.3.1 and 6.3.2. below). The impact on fundamental rights as regards non-discrimination would be less positive than the regulatory options (see 6.3.1 and 6.3.2 below), because a project limited to interested Member States could only partially remove unjustified differences in the treatment of convicted TCN and convicted EU nationals; it remains uncertain whether a homogeneous approach for all Member States could be achieved.

A Member States' project would not be guaranteed effective with regard to the general and specific objectives, because it would depend on countries' voluntary participation. It might therefore not cover all Member States that would have to participate in a regulatory option, and it could not be enforced. This could mean that a requesting Member State may not receive complete criminal record information on a convicted TCN, thus maintaining the status quo. For the same reasons, the NJR (Network of Judicial Registers - see under 5.2.) was finally incorporated into ECRIS.

The overall costs would be similar to a regulatory option (depending on the solution chosen, see below). However, the cost per Member State would be higher, because the costs borne by the EU in the other options would most probably need to be shared amongst a smaller number of Member States. In addition, the proportionate cost to be borne by the Member States in case of co-financing by the Commission (at least 20%), which would apply to the overall costs, might discourage Member State participation and thus reduce the territorial scope of the project.

6.3. Regulatory options

6.3.1. Option 3 – decentralised option

- *Effectiveness*

Specific objectives: Provision of a mechanism to identify Member State(s) holding criminal record information on a particular TCN. Thus, inefficient and costly 'blanket'-requests, which have discouraged systematic use of ECRIS for TCN so far, could be avoided. All Member States would only receive and would have to reply to requests on TCN they actually hold information on. All Member States, but especially smaller countries with relatively small numbers of convicted TCN in their criminal records would benefit from option 3. The identification of Member States holding relevant information (searching the index-filter) would entail only a search that can be performed on data/index-filters stored within the requesting Member State; the search in the index-filters as such would thus not affect other Member States.

The increased efficiency of ECRIS with regard to TCN will promote its use for this purpose. It will help the implementation of Council Framework Decision 2008/675/JHA[37] obliging Member States' judicial authorities to take previous convictions handed down against the same person for different facts in other Member States into account during criminal proceedings. Given that currently between 500 000 and 600 000 convictions concerning TCN

---

[37] Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings, OJ L 220, 15.8.2008, p. 32.

are handed down every year by criminal courts in the EU, the use of ECRIS with regard to TCN should increase from 23 000 requests (in 2014) to at least the number of annual convictions.

General objectives: Systematic use of ECRIS with regard to TCN will also deliver ECRIS' full potential with regard to the general objectives.

Giving competent Member State authorities easy and efficient access to complete criminal record information contributes to crime prevention and thus improves the functioning of a common area of justice and security. In particular, an efficient ECRIS can contribute to preventing and detecting recidivism, i.e. crime that is committed repeatedly by the same person.

It is, however, difficult to gauge the extent to which crime can be reduced. The reason is that full availability of criminal record information is only part of a successful crime prevention strategy. The many factors that play a role can vary from case to case. It can, however, be said that access to full information on the criminal history of a person is an important element in every crime prevention strategy.

Increased efficiency of ECRIS with regard to TCN will put TCN and EU nationals on the same footing when it comes to administrative or judicial decision-making that can be influenced by the criminal record of the person concerned. Unequal treatment stemming from deficiencies of ECRIS with regard to TCN-related requests, affecting important and often sensitive decisions in the area of criminal law but also important administrative decisions (licenses, employment, etc.) will therefore be significantly diminished.

As a result, option 3 would be effective with regard to the general and specific objectives.

- *Costs[38]*

The compliance costs consist of the one-off cost and recurring cost.

The following Table 1 shows the total costs of setting up (one-off) and yearly maintenance of the decentralised option:

Estimated costs (in €)	One-off costs	Maintenance costs per year
Decentralised option without mandatory fingerprints		
For the EU	1 089 000	502 000
For 28 MS	768 000	204 000
Total	**1 857 000**	**706 000**

Table 1 Total costs to set up (one-off) and maintain yearly the decentralised option

The cost at EU level for the decentralised solution amounts € 1 089 000 as one-off cost and € 502 000 as maintenance costs.

The one-off and maintenance costs incurred per Member State for the decentralised option are shown in Graph 2 below.

---

[38]   Study on Assessment of ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for third country nationals and stateless people (TCN) dated 4 December 2015 ('Kurt Salmon study', to be published).

Decentralised option
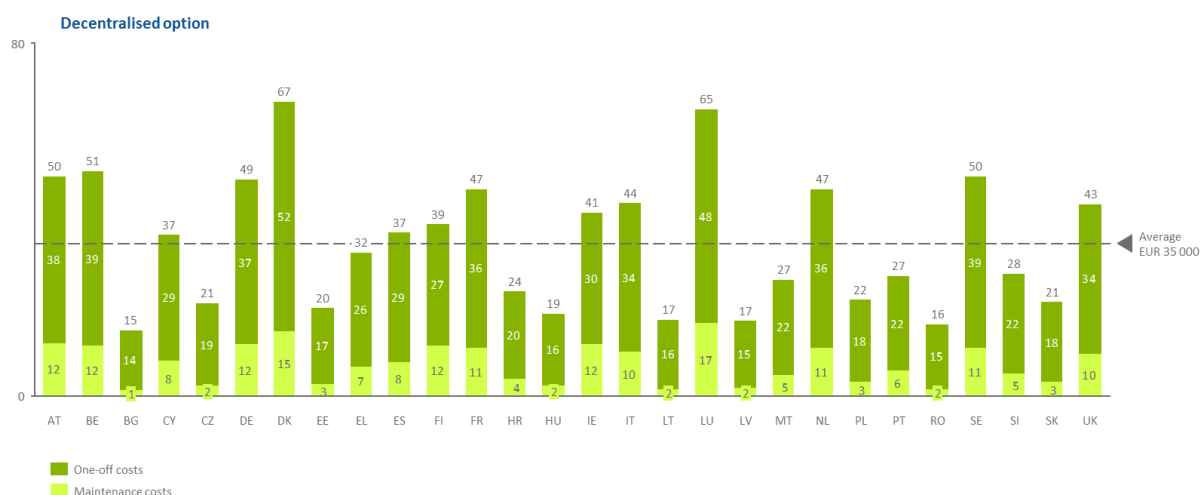
Graph 2 One-off and maintenance costs incurred per Member State for the decentralised option

On average, the total costs for the decentralised option amount to € 35 000 (€ 27 000 one–off plus € 8 000 yearly maintenance) per Member State. Costs in the Member States vary due to differences in labour costs[39]. This leads to a maximum one-off cost of € 65 000 in Luxemburg and a minimum one-off cost of € 15 000 in Bulgaria.

Set-up cost elements:

The following cost elements were considered:

At Member State level[40]:

  o Development of the software application (routine/script) that automatically and regularly extracts data from the national criminal record and loads it into the application software that anonymises the data and distributes it to Member States (Total: € 254 000).

  o Infrastructure: acquisition and set-up of hardware (server), software and network connections (Total: € 514 000).

At EU level:

  o Customisation, installation and configuration of application software (e.g. FIU.net's Ma^{3}tch software application). This includes the development of specific search software. (Total: € 693 000).

  o Follow-up of project implementation in the Member State (this cost element includes management of the implementation of the ECRIS TCN system including: planning, business requirements analysis, functional requirements analysis, coordination activities, testing and roll-out), coordination (Total: € 396 000).

Cost elements for maintenance:

---

[39] The labour rates are based on the latest available comparable data from Eurostat's structural earnings' survey of 2010 for occupation group ISCO 3 (technicians and associate professionals).

[40] Some of these costs may be compensated by EU funding through a corresponding increase in EU costs. Member States costs may be compensated by EU funding under the form of co-financing. The Commission could co-finance up to 80% of the costs of proposals submitted by Member State fulfilling the Commission prerequisites required for co-financing.

At Member State level:

- o Maintenance (patches, bug fixing and associated software releases) of the software application (routine/script) that automatically and regularly extracts data from the national criminal record and loads it into the application software that anonymises and distributes the data to Member States (Total: € 152 000).
- o Infrastructure: maintenance and support of hardware (server), software and network connections (Total: € 52 000).

At EU level:

- o Maintenance of the application software (e.g. FIU.net's Ma^{3}tch software application) (Total: € 502 000).

Basis for cost calculation:

The costs were calculated on the basis of data received from the stakeholders[41] consulted in the course of a study carried out by an external contractor. More details on the set-up costs can be found in Annex 7 - Detailed cost analysis and estimates.

Administrative costs (workflow):

The costs are assessed on the basis of changes as compared to the baseline scenario (option 1). Subsequently, administrative costs[42] are calculated on the basis of average costs of the required administrative activity multiplied by the total number of tasks (frequency) performed per year. The costs are estimated by multiplying a tariff (based on average labour cost per hour in each Member State) and the duration needed for each activity. In Table 2 below the administrative steps and costs for each step of option 3 are contrasted against the baseline scenario (option 1).

No	Administrative step (Activity)	Option 1 (Baseline scenario) Activity description	Decentralised option 3 Activity description
1	**Storing or updating information on convictions** in the national criminal record system.	Storing criminal record information in the criminal record register, including TCN convictions	Same activity as in option 1, but different frequency[43].
2	**Extracting information on convictions from** national criminal record system.	Extraction of criminal record data from central criminal record register and copying of the data into a separate file.	Extraction of convicted TCN personal data from central criminal record register and copying of the data into a separate file (index-filter).

---

[41] The following stakeholders were consulted: 28 MS, the FIU.net bureau in The Hague, representatives of the eu-LISA agency and Eurojust.

[42] More details on the Standard Cost Model to apply are to be found here: http://ec.europa.eu/smart-regulation/refit/admin_burden/scm_en.htm.

[43] The baseline scenario (option 1) is the 'as-is-situation'. To date there are 25 MS exchanging criminal record information. Three MS (PT, MT and SI) out of 28 are not yet exchanging criminal record information. In both options (centralised or decentralised) it is assumed that the mechanism to exchange criminal records for TCN will be implemented by 28 MS.

No	Administrative step (Activity)	Option 1 (Baseline scenario) Activity description	Decentralised option 3 Activity description
3	**Anonymisation of TCN conviction data.**	This activity is not performed in the current workflow in ECRIS.	Transfer of the file (extracted TCN data) to a separate server where the data is anonymised using specific software (anonymised index-filter).
4	**Sending the data.**	Transfer of the file (extracted criminal record data) to a separate server (located in the MS) where the data is formatted for notification or request purposes using specific software.	Transfer of the anonymised file (extracted TCN data in the index-filter) to all other MS through the EU network (s-TESTA).
5	**Searching for a convicted TCN.**	This activity is not performed in the current workflow in ECRIS.	Search against the locally stored anonymised files (index-filters) in each MS. Specific search software is used to overcome spelling mistakes or mismatches, the return of several hits is likely. The accuracy of the search could be influenced by adding or removing search criteria.
6	**Sending a request**	Formatting of the extracted criminal record information into a notification or a request using specific software (ECRIS Reference Implementation software or ECRIS national implementation).	Following a hit, formatting the returned information into a request using specific software (ECRIS Reference Implementation software or ECRIS national implementation).
7	**Replying to a request** (also in case of a hit through ECRIS TCN).	Formatting of the extracted criminal record information into a request response using specific software (ECRIS Reference Implementation software or ECRIS national implementation).	Same activity as in option 1, but different frequency.

Table 2: List of activities option 1 vs option 3

If the new ECRIS TCN legal instrument is fully implemented, each criminal procedure against a TCN will trigger a search for previous convictions. However, experience regarding ECRIS statistics indicates that in practice, the searches for previous convictions have increased over the years. Assuming a similar approach for TCN, it is reasonable to consider that the number of searches will gradually increase. Consequently it is anticipated that the associated administrative cost will also rise.

The administrative costs incurred in option 1, which represents the current situation (20.000 requests issued for TCN), are estimated at approximately € 1 465 000[44], which amounts on average to € 59 000 per year per Member State. And for the EU, the administrative cost is

---

estimated at € 166 000 (this is project support cost, including training and coordination for the Member States).

The administrative costs incurred in the decentralised option 3 are expected to gradually increase over the years, starting at approximately € 5 100 000 and growing to maximum € 12 600 000.

The administrative costs depend on different factors: the level of automation per Member State which will have an impact on the duration of some activities such as the handling of requests, the duration of a search, the number of requests per year, and the labour costs per Member State. The administrative costs presented above take into account the different conditions in the Member States. More details about the calculations can be found in Annex 8 - Administrative cost calculation.

To the cost referred to above, the mandatory usage of fingerprints would imply additional costs. The following Table shows the total costs of setting up (one-off) and yearly maintenance of including compulsory fingerprint usage in the decentralised option:

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 maintain yearly the fingerprint matching functionality in the decentralised option

Set-up cost elements:

The following cost elements were considered:

At Member State level:

o Implementation of a decentralised fingerprint matching functionality (including infrastructure) and linking to ECRIS. (Total: € 37 500 000).

At EU level:

o Adaptation of the ECRIS common Reference Implementation software to include the fingerprint matching functionality (Total: € 5 000 000).

Cost elements for maintenance:

At Member State level:

o Maintenance of the ECRIS AFIS (Total: € 11 500 000).

At EU level:

o Maintenance of the common Reference Implementation software including the fingerprint matching feature (Total: € 1 000 000).

• *Fundamental rights/non-discrimination*

According to the national constitutional law of all Member States as well as the Treaty on the Functioning of the European Union (TFEU) and the European Charter of Fundamental

Rights, different procedures depending on a person's nationality run counter to the non-discrimination principle, unless such different procedures are justified and proportionate.

As TCN do not have a Member State of nationality, a system different from the one applying to EU nationals needs to be introduced. The data contained in the index-filter is only an extract of data already contained in the existing databases of criminal records in the Member States. The index-filter does not serve any other purpose than the criminal record database from which it was extracted. It does not lead to a situation where searching for TCN conviction information is more efficient than a search for such information regarding EU nationals. On the contrary, the effect will be that searches for criminal record information regarding TCN and EU nationals will be equally efficient. An index-filter-based search mechanism for TCN thus removes unjustified differences in the treatment of convicted TCN and convicted EU nationals through the current ECRIS (see above under 2.3). It is therefore justified and proportionate.

- *Data protection*

Whatever the option, it must be fully compliant with both national and EU-level data protection principles and applicable provisions. Under current data protection standards, data relating to criminal convictions are considered to be special categories of personal data, requiring specific protective measures[45]. The processing of personal data by European Union institutions and bodies is covered by Regulation 45/2001, whereas the exchange of personal data between the law enforcement and judicial authorities of the Member States should be compatible with Framework Decision 2008/977.

In the decentralised option, the anonymised index-filter shared between Member States and the hit/no hit search mechanism will not lead to the exchange of personal data. Member States only share and compare irreversibly anonymised data (locks or filters)[46]. Therefore, option 3 would not require new data protection rules.

- *Information control and security*

In the decentralised option, Member States keep full control of the personal data contained in their national criminal record systems. It is only the anonymous filters that Member States share with each other. It can therefore be concluded that additional security measures at Member State level are not necessary.

- *Proportionality*

The efficient exchange of criminal record information is crucial in combating cross-border crime and contributes considerably to putting into practice the principle of mutual recognition of judgments and judicial decisions in a common area of justice and security, where people move freely. Action at EU level is therefore proportionate to the objectives of the initiative.

6.3.2. Option 4 – centralised option

- *Effectiveness*

This option is as effective as option 3 (See above under 6.3.1. Option 3).

---

[45]   See for instance Council of Europe Convention 108, Article 6, as well as Directive 95/46, Article 8(5); Regulation 45/2001, Article 10(5).

[46]   Recital 25 of Directive 95/46/EC states: "The principle of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."

- *Costs[47]*

For the cost of the central solution, different existing IT solutions (such as for example the VIS system and EURODAC) handling similar information but for different purposes (visa request for TCN for the VIS and asylum seekers identification in EURODAC) were considered. The reuse of existing software solutions was discarded for different reasons. For the VIS, the solution goes far beyond the basic ECRIS requirements as it handles the entire visa application workflow, including an AFIS. The EURODAC software solution only compares fingerprints from different sources and does not address the ECRIS requirements regarding alphanumerical identification information.

Only one potentially realistic solution was retained: the development of new software.

Table 4 shows the total costs of setting up (one-off) and maintaining the centralised option using new software:

Estimated costs (in €)	One-off costs	Maintenance costs per year
Centralised option without mandatory fingerprints		
For the EU	5 274 000	1 285 000
For 28 MS	856 000	227 000
Total	**6 130 000**	**1 512 000**

Table 4: Total costs for setting up (one-off) and yearly maintenance of the centralised option

Compared to the decentralised solution where the existing software is considered fit-for-purpose, the cost for developing the centralised solution (loading data, search and monitoring) is higher. The one-off and maintenance costs incurred per Member State for the centralised option are shown in Graph 4 below.
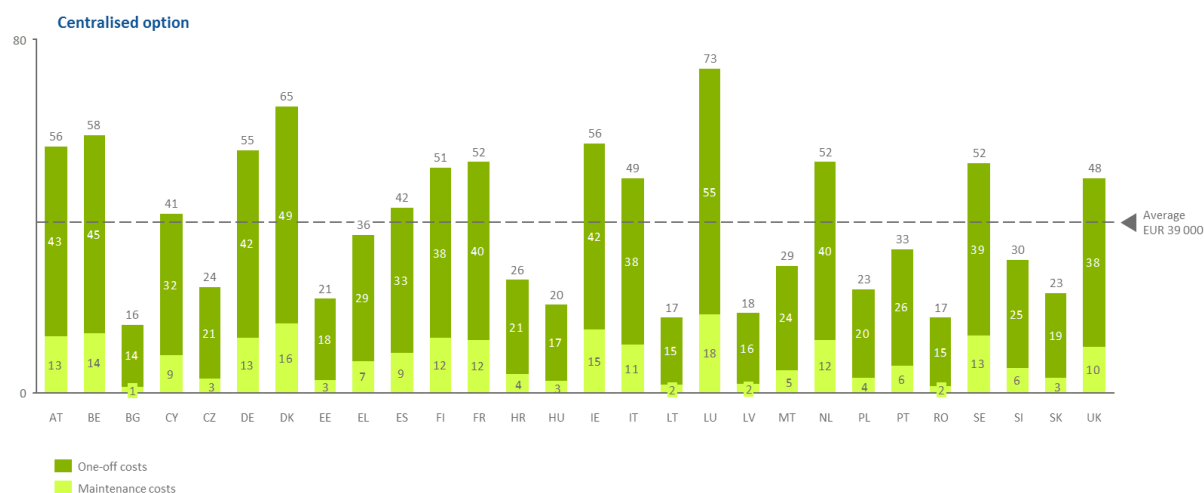
Graph 4: One-off and maintenance costs incurred per Member State for the centralised option

---

[47]   Study on Assessment of ICT impact dated 04 December 2015 ('Kurt Salmon study', to be published). The costs for the set up and development of the central solution system were provided by EU-LISA. They were based on comparable set-up costs incurred for the establishment of VIS and EURODAC.

The costs in the Member States vary due to big differences in labour costs[48]. For the centralised option, the average total costs per Member State amount to € 39 000 (€ 31 000 one–off + € 8 000 yearly maintenance), varying from € 16 000 in Bulgaria to € 73 000 in Luxemburg.

Cost of setting up:

For the centralised option the following cost elements were considered:

<u>At Member State level[49]:</u>

- o Development of a software application (routine/script) that automatically and regularly extracts data from the national criminal records and transmits it to the central index-filter (Total: € 342 000).

- o Infrastructure: acquisition and set-up of hardware (server), software and network connections (Total: € 514 000).

<u>At EU level:</u>

- o Infrastructure: acquisition of hardware, software (COTS), installation, configuration and connection, maintenance and support (Total: € 2 702 000).

- o Development of a software application that loads the data received from Member States into the central index-filter (Total: € 1 000 000).

- o Development of a graphical user interface for the search mechanism (Total: € 400 000).

- o Development of specific search software (Total: € 250 000).

- o Development of a software application that would monitor the provision of data files by Member States and enable statistical information on end-user queries to be obtained (Total: € 150 000).[50]

- o Project implementation: includes the activities carried out by central EU staff (the project implementation cost element includes management of the ECRIS TCN system including: planning, business requirements analysis, functional requirements analysis, coordination activities, testing and roll-out) as well as coordination and follow-up activities with the Member States performed by Commission staff (DG Justice and Consumers) (Total: € 772 000).

Cost of maintenance:

<u>At Member State level:</u>

- o Maintenance (patches, bug fixing and associated software releases) of the software application (routine/script) that automatically and regularly extracts data from the national criminal record and loads it into the central system (Total: € 152 000).

---

[48]   The labour rates are based on the latest available Eurostat structural earnings' survey of 2010 for occupation group ISCO 3 (technicians and associate professionals).

[49]   Some of these costs may be compensated by EU funding entailing a corresponding increase of EU costs. Member States costs may be compensated by EU funding under the form of co-financing. The Commission would co-finance up to 80% of the costs of proposals submitted by Member States fulfilling the Commission prerequisites required for co-financing.

[50]   In the decentralised option, this element is contained in the costs for "Customisation of the application software".

o Infrastructure: maintenance and support of hardware (server), software and network connections (Total: € 75 000)[51].

At EU level:

o Infrastructure: maintenance and support of hardware, software (COTS) (Total: € 905 000).

o Maintenance of a software application that loads the data received from Member States into the central index-filter. (Total: € 200 000).

o Maintenance of a graphical user interface for the search mechanism (Total: € 100 000).

o Maintenance of specific search software and monitoring (Total: € 50 000).

o Maintenance of a software application that would monitor the provision of data files by Member States and enable statistical information on end-user queries to be obtained (Total: € 30 000).

Basis for cost calculation:

The costs were calculated on the basis of data received from the stakeholders consulted in the course of a study carried out by an external contractor. More details on the set-up costs can be found in Annex 7 - Detailed cost analysis and estimates.

Administrative costs (workflow):

The table below shows the administrative steps necessary to operate option 4 as compared to the baseline scenario (option 1).

No	Administrative step (Activity)	Option 1 (baseline scenario) Activity description	Centralised option 4 Activity description
1	**Storing or updating information on convictions** in the national criminal record system.	Storing criminal record information in the criminal record register, including TCN convictions.	Same as option 1.
2	**Extracting information on convictions from** national criminal record system.	Extraction of criminal record data from central criminal record register and copying of the data into a separate file.	Extraction of criminal record data from central criminal record register and copying of the data into a separate file.
3	**Anonymisation of TCN conviction data.**	This activity is not performed in the current workflow in ECRIS.	This activity is not performed in the centralised workflow scenario.
4	**Sending the data.**	Transfer of the file (extracted criminal record data) to a separate server (located in the MS) where the data is formatted for notification or request purposes using specific software.	Transfer of the file (extracted TCN data) to the central system through the EU network (s-TESTA).

---

[51] The cost related to this element is sensibly higher than in the decentralised solution because there is not yet a central entity established. Additional costs are anticipated due to the activities related to the interconnection to a central index via the secure EU network (s-TESTA). Maintenance costs are anticipated to represent according to standard IT development practices 20% of the development costs.

No	Administrative step (Activity)	Option 1 (baseline scenario) Activity description	Centralised option 4 Activity description
5	**Searching for a convicted TCN.**	This activity is not performed in the current workflow in ECRIS.	Search against the files stored in the central system. Specific search software is used to rectify spelling mistakes or mismatches, the return of several hits is likely. The accuracy of the search could be influenced by adding or removing search criteria.
6	**Sending a request.**	Formatting of the extracted criminal record information into a notification or a request using specific software (ECRIS Reference Implementation software or ECRIS national implementation).	Same as option 1.
7	**Replying to a request** (also in case of a hit through ECRIS TCN).	Formatting of the extracted criminal record information into a request response using specific software (ECRIS Reference Implementation software or ECRIS national implementation).	Same as option 1.

Table 5: List of activities option 1 vs option 4

Compared to the decentralised option 3, the only different activity is the anonymisation of data, which is not necessary for option 4. Given that this activity is fully automated and therefore does not produce any workflow-related costs, the administrative costs incurred in option 4 are the same as for option 3. Administrative costs per Member State are thus the same as in option 3 (see Table 9 Administrative costs associated with the options in Annex 8). For the EU, the administrative cost is the same as in option 3. Under the centralised scenario it's assumed that the data cleaning and handling of duplicate is fully automated so as to reduce to a minimum the cost incurred for the EU.

In addition to the cost referred to above, the mandatory usage of fingerprints would imply additional costs. The following Table shows the total costs of setting up (one-off) and yearly maintenance of the centralised option:

Estimated costs (in €)	One-off costs	Maintenance costs per year
Decentralised option with fingerprints		
For the EU	1 970 00	450 000
For 28 MS	37 500 000	11 250 000
Total	**39 470 000**	**11 700 000**

Table 6 Total costs to set up (one-off) and maintain yearly the fingerprint matching functionality in the centralised option

Cost of setting up:

For the centralised option the following cost elements were considered:

<u>At Member State level:</u>

    o Adaptation of the existing AFIS to include the fingerprint capacity for ECRIS (Total: € 37 500 000).

<u>At EU level:</u>

o   Implementation of the central fingerprint matching functionality (Total: € 1 970 000).

Cost of maintenance:
<u>At Member State level:</u>
o   Maintenance of the existing AFIS (Total: € 11 250 000).
<u>At EU level:</u>
o   Maintenance of the central fingerprint matching functionality (Total: € 450 000).

- *Fundamental rights/non-discrimination*

The general explanations outlined above for the decentralised option are also valid for option 4.

However, in option 4 the index-filter would be operated at EU level. This introduces a new element to ECRIS. Moreover, option 4 would centralise personal data of TCN contained in 28 national criminal registers. In contrast, personal data of EU nationals are only kept decentralised at the respective national level.

- *Data protection*

The general considerations outlined above for the decentralised option are also valid here, but there are nevertheless significant differences between the two options in terms of data protection. The centralised option is characterised by the storage of data both at national and at EU level – thus leading to the duplication of personal data in a central database. Therefore, the existing data protection rules of the current ECRIS decentralised system at Member State level are not sufficient. For option 4 an additional data protection regime – similar to the one used for other already existing centralised information exchange systems at EU level – would have to be put in place.

- *Information control and security*

In option 4 personal data of convicted TCN are stored not only at Member State level but also centrally at EU level. 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 index-filter. In addition, security and logging measures must be agreed, put into place and maintained.

The role of the EU agency storing the data would be limited to technical operations, in particular maintaining the operation and the security of the system. In this scenario, only Member States would be authorised (and responsible) to input, update and delete data in the index-filter. Thus, responsibilities in option 3 are similar to those in option 4, but need more complex rules and safeguards.

- *Proportionality*

Efficient exchange of criminal record information is instrumental in combating cross-border crime and contributes considerably to putting into practice the principle of mutual recognition of judgments and judicial decisions in a common area of justice and security where people move freely. Action at EU level is therefore proportionate to the objectives of the initiative.

However, option 4 entails centralisation of personal data of convicted TCN at EU level. In this particular case, duplication and centralisation of TCN personal data at EU level could be considered unnecessary, since the objectives of the initiative can be achieved equally well at national level (option 3).

7. DISCARDED OPTIONS – DETAILS IN ANNEX 6

7.1. Centralised fully fledged system

Convicting Member States would be obliged to send full criminal record information to a central database at EU level. The central database would include the identity data of convicted TCN and all the details of their convictions.

This would mean creating a common criminal register on TCN at EU level. It risks violating the principle of subsidiarity and the non-discrimination principle with regard to TCN and EU nationals, as the storage of full criminal record information at central level and only for TCN (for EU nationals full criminal record information is only stored at Member State level) is not necessary to reach the objectives (see options 3 and 4).

7.2. Decentralised system with a reference Member State for each convicted TCN

Convicting Member States would have to notify all criminal record information concerning convicted TCN to a reference Member State. This reference Member State would take on the role of the Member State of nationality in the established ECRIS. Member States of reference could be appointed on the basis of:

– Long-term residency status within a Member State (e.g. migrants, refugees, etc.).

– Short-term permission to enter/stay within a Member State (e.g. tourist visa, visa exemption, asylum application).

– A short-term visa.

However, there is a risk that TCN would seek to 'hide' the reference Member State. It would also not solve the problem of TCN, who are not legally admitted to the territory of any Member State.

7.3. Centralised system with an index-filter with anonymised information (combining elements of option 3 and option 4)

A centralised index-filter could in theory be combined with anonymisation software as in the decentralised solution. In the decentralised option the Member States distribute their national index-filters to all other Member States. It is more acceptable for Member States to do so, if these index-filters would be anonymised.

In the centralised option, Member States share their national index-filters only with the central contact point at EU level. It could be conceived to anonymise this data as well to avoid duplicating data protection regimes and data security measures at EU level. However, there would be little added value (as compared to the decentralised option) to do so, as such a scenario would be (i) more costly as it combines the costs for the set-up of a centralised system and the costs of anonymisation and (ii) it would not be proportionate, as Member States could send the anonymised index-filter as easily to the other Member States as to the central level.

8. COMPARISON OF THE OPTIONS

In the following table the results of the assessment as described above under 7 are compared, with option 1 representing the status quo set at '0'.

Objectives / impacts	Option 1 status quo	Option 2 non-legislative	Option 3 decentralised	Option 4 centralised	Comments

Efficiency regarding the general and specific objectives	0	0	++	++	a) Option 1 is the baseline scenario. The baseline scenario is deemed to be not efficient with regard to specific and general objectives.
					b) Options 3 and 4 are equally efficient in addressing the general and specific objectives.
					   o <u>Specific objective: to replace costly blanket requests by a more efficient system to identify Member States holding criminal record information; thus, to encourage more systematic use of ECRIS for TCN.</u>
					     Both options provide for an index-filter-based hit/no-hit search mechanism, to identify Member States holding criminal record information. Thus, inefficient 'blanket' requests and their costs can be avoided. As 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%
					   o <u>General objective: to reduce and combat crime</u>
					     This 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 reducing crime and fostering crime prevention.
					c) Option 2 depends on voluntary Member State action and is therefore less efficient with regard to the objectives.

Cost-efficiency	0	+	++	+	<u>Set-up (one-off) costs</u> Option 4 total set-up costs (€ 613 000) are almost three times greater than in option 3 (€ 1 857 000). The difference between option 3 (€ 768 000) and option 4 (€ 856 000) in terms of set-up costs to be borne by the Member States is less than € 100 000, which is marginal. Option 1 would not entail any set-up-costs, as the status quo would remain unchanged. However, the economic and social costs of unprevented crime (see section 2.3, in particular bullet point 'costs of crime') outweigh by far the economic costs necessary to set up and maintain a system (as in options 3 and 4) aimed at crime prevention. Option 2 is comparable to option 3, but less cost-efficient for Member States, as project costs have to be shared by fewer Member States (it is likely that not all Member States will participate). <u>Maintenance costs</u> The maintenance costs are two times more expensive in option 4 (€ 1 512 000) than in option 3 (€ 706 000). For the Member States the difference in maintenance costs between option 3 (€ 204 000) and option 4 (€227000) is marginal.
	0	++	++	++	<u>Administrative costs</u> The annual administrative costs for option 1 amount to € 1 465 000 - on average, € 59 000 per year per Member State. Although the costs are much lower than in the other options, this does not reflect cost-efficiency of option 1. Rather the contrary, the lower costs must be attributed to the inefficiency of the current mechanism in relation to TCN and its consequent underuse. In fact, there would be a substantial reduction in costs compared to the status quo. In option 1 an individual 'blanket' request is estimated at € 106 while in option 2, 3 or 4, the individual cost of a request is reduced to €10. The high costs for individual blanket requests are not reflected in the total administrative costs of the status quo, because Member States avoid such requests and tend not to ask for information on TCN at all.

					Option 3 adds an anonymisation process and the search function to the workflow. Given that this activity is fully automated, costs would not be incurred. Therefore, the administrative costs incurred in option 4 (that does not include the anonymisation process) are the same as for option 3. The administrative costs incurred in options 3 and 4 are expected to gradually increase over the years, starting at approximately € 5 100 000 and growing to a maximum € 12 600 000. In option 4 the central level is the single point of failure, interrupting all information exchange in case of defect. For this reason it is regarded as less advantageous than option 3 and is evaluated only with a single +. Option 2 is comparable to option 3.
Fundamental rights/non-discrimination	0	++	++	+	Option 4 centralises data on convicted TCN at EU level. Option 4 is therefore less proportionate, as option 3 is equally efficient without creating unnecessary differences in the treatment of the personal data of EU nationals and TCN. Option 2 is comparable to option 3. With regard to the outcome of the stakeholder consultation regarding fundamental rights, see section 5.4.
Data protection	0	++	++	+	As option 4 entails storage of personal data at EU level, a specific set of data protection rules at EU level would be needed. Option 3 does not involve the exchange of personal data. Option 2 is comparable to option 3.
Information control and security	0	++	++	+	In Option 4 a definition and delineation of responsibilities between the Member States on the one hand and the EU level on the other hand would be necessary. This calls for more complex rules and security measures than in option 3. Option 2 is comparable to option 3.
Proportionality	0	++	++	+	See above under 'cost-efficiency' and under 'fundamental rights /non-discrimination'.

In addition to the costs referred to above, the mandatory usage of fingerprints would imply additional costs for the Member States and for the EU. In option 3, the set-up costs incurred by EU is € 5 000 000 while in option 4, the set-up costs incurred for the EU is less (€ 1 970 000) as there is no anonymisation of fingerprints foreseen. The set-up costs (€ 37 500 000) and maintenance costs (€ 11 500 000) for the MS are the same in both options 3 and 4 as in both cases the national AFIS's need to be adapted accordingly for the handling and storage of fingerprints for ECRIS purposes.

9. PREFERRED OPTION

Based on the analysis of the impacts of the different options the preferred option is: Option 3 - decentralised hit/no hit index-filter system combined with suboption 5.3.3.2 (voluntary use of fingerprints for identification of TCN.)

Operational objective	The preferred option
To add a mechanism to ECRIS that identifies Member States holding criminal record information on a particular TCN	Option 3 would introduce a decentralised hit/no hit search mechanism based on anonymised national index-filters containing identity data of convicted TCN.

- Option 3 satisfactory fulfils the general and specific objectives, as it introduces a mechanism into the ECRIS framework to identify Member States holding criminal record information. This avoids costly and inefficient blanket requests and will thus eliminate the reason why Member States currently refrain from using ECRIS for TCN. ECRIS will thus be used more systematically. An improved ECRIS with regard to TCN will more fully contribute to reducing crime, fostering crime prevention and enhancing a European area of justice and security. As option 3 would place a legal obligation on all Member States, it will guarantee a common approach and therefore the efficiency of the mechanism in all Member States.
- Option 3 is more cost-efficient than option 4, as there are no costs for setting up of an EU-level database and -infrastructure. It is expected that there will be no costs for the software needed at Member State level, as a non-exclusive licence was obtained by the Commission. With regard to administrative costs, option 3 will be more costly than option 1. However, lower administrative costs in option 1 are not the result of its efficiency, but reflect the problem (no usage of ECRIS for TCN) remedied by option 3. The administrative costs incurred in option 3 are necessary to prevent and combat crime and to reduce the costs related to crime.
- Option 3 does not require an additional layer at EU level not existant for EU nationals. It therefore complies better with the principle of non-discrimination. Option 3 also does not require additional data protection and security at EU level as no personal data is exchanged (anonymised index-filter). The reasons why anonymisation in option 4 does not add value as compared to option 3 are detailed above under 7.3.

The following obligations and rights, which are not contained in the current legal text or currently only apply to convictions of EU nationals would have to be in a regulatory option:

- the obligation of the central authorities of the Member States to store information on convictions against third country nationals and to update it; it would be construed in a similar way as the current obligation to store information on convictions against EU nationals;
- the obligation of the central authorities to create an index-filter of identification data on convicted third country nationals and transmit it to the other Member States in an anonymised way;
- the right of the central authorities to search the index-filters transmitted to them, i.e. to match own information with the information in the index-filters;

- the obligation of the central authorities to reply to request for criminal record information on third country nationals; it would be construed in a similar way as the current obligation as regards information on EU nationals and replace the reference to the Convention on Mutual Assistance in Criminal Matters;
- the obligation to do the necessary that a criminal record extract requested by a third country national is completed by information from other Member States; such an obligation exists already today for criminal record extracts for EU-citizens;
- the obligation to carry out the technical alterations in application of state-of-art-technologies necessary to make the information exchange system function (use of a standardised format and the index-filter mechanism).

10. MONITORING AND EVALUATION

Two years after the adoption of the legislative instrument, the Commission will conduct an evaluation of the extent to which it has been implemented in the Member States, and of the effectiveness of the measures that Member States have taken to achieve the objectives set out in section 4 above. On the basis of this evaluation, the Commission will decide the appropriate follow-up.

The implementation of the legislative instrument in the Member States would be constantly monitored through the existing ECRIS expert group. This group will also provide a forum for establishing best practices on exchange of information on criminal records at EU level.

The Commission will subsequently define monitoring indicators such as the level of exchanges of TCN criminal records as compared to the number of convictions involving TCN as well as others relevant ones.

The provisional timetable of the implementation of the exchange of criminal record information extracted from the criminal record registers for Third Country Nationals (TCN) can be found in Annex 9.

Lead DG: Directorate General Justice and Consumers

Agenda Planning

Reference AP No	Short title	Foreseen adoption
2012/JUST/014	ECRIS TCN proposal	19/01/2016

The improvement of the existing European Criminal Records Information System (ECRIS) is part of the European Agenda on Security[52] adopted in April 2015. The Commission decided that key instruments of information exchange like ECRIS should be kept under review and any gaps in coverage should be filled, pointing at the fact that ECRIS does not work effectively for non-EU nationals convicted in the EU.

As part of the European Agenda on Security, it belongs to the Commission's Work Programme 2016[53].

Organisation and timing

An Inter-Service Steering Group (ISSG) was set up in August 2015. The ISSG is chaired by the Directorate General Justice (JUST), and the following Services and Directorates General have been invited to participate: Secretariat-General (SG), Legal Service (LS), Budget (BUDG), Communication networks, content and Technology (CNECT), Informatics (DIGIT), European External Action Service (EAS), Neighbourhood and Enlargement Negotiations (NEAR), Migration and Home Affairs (HOME).

The ISSG met twice until the submission of the Impact Assessment to the Regulatory Scrutiny Board in December 2015. The ISSG approved the Inception Impact Assessment that was published on 15 July 2015 and the Impact Assessment Report.

Consultation of the Regulatory Scrutiny Board

The Impact Assessment Report was examined by the Regulatory Scrutiny in a written procedure from 7 December 2015 until 7 January 2016. The Board recommends that the IA report is improved, giving special attention to the following aspects:

---

[52] '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, page 8.

[53] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme 2016, 'No time for business as usual', COM(2015) 610 final of 27 October, p. 5, Section 'An Area of Justice and Fundamental Rights Based on Mutual Trust', item No 17.

Board's Recommendations	Implementation of the recommendations into the revised IA Report
1. The current framework, the overall context and all of the different aspects of the problem should be developed in more depth in the problem section.	1. The Impact Assessment has been completed with comprehensive information on existing EU systems to exchange data and why these systems do not address the identified problem. The argumentation why the absence of an EU-wide mechanism on TCN leads to problems has been deepened and the report explains what action has been undertaken to evaluate the existing ECRIS.
2. The figures and assumptions of the cost assessment should be transparently explained.	2. The report has been amended so as to address more transparently the figures and assumptions related to the cost assessment. In more detail: • The assumption on the spread of TCN convictions and requests for TCN per Member States has been revised together with its impact on the administrative cost (see for example section 2.2 and 2.5 in Annex 8). • Uncertainties were factored by thorough evaluation of the cost, extrapolation technique, averages and/or ranges. For example, the uncertainties on some assumptions factors (such as the number of request) the administrative costs were factored by ranges and an average (see Table 3, Table 6 and section 2.5 in Annex 8).
3. The different options should be assessed in a more consistent way (against the baseline). In particular, the report should better explain the estimated higher cost for Member States of a centralised solution, including the proposed choice of a specific IT tool, as well as the rationale for discarding the use of fingerprints. It should also clarify the need for legislative changes under the preferred option, developing the reasons why the existing mechanisms cannot be further automated.	3. The differences between the costs of a centralised and a decentralised solution have been further elaborated, such as for example the higher maintenance costs incurred for Member States in a centralised scenario compared to a decentralised scenario (see section 6.3.2). The choice for the IT tool has been further explained in section 5.3. The report addresses the different IT solutions available such as FIU, EPRIS, and other discarded solutions. The report highlights in section 9 that the objective of the preferred solution cannot be achieved without modification of the current legal framework. The detailed obligations and rights which are not contained in the current legal text or currently only apply to convictions of EU-nationals are described in more details. The report has been revised to better explain that this initiative aims at allowing Member States to

Board's Recommendations	Implementation of the recommendations into the revised IA Report
	receive accurate information on past convictions of a certain person in other Member States. Reliable information is one of the underlying means in order to enable an efficient exchange of information, irrespective of the mechanism and should be the main task of Member States at national level using existing identification methods (see section 4).

Evidence used

The initiative was built upon a large set of data from the following sources. The quality of the results of the referred studies was assessed.

Statistics

The following statistics were used to define the size of the problem: Eurostat, Migration and population statistics, May 2015.

Studies

A feasibility study on the Establishment of a European Index of Convicted Third Country Nationals provided a better understanding of future mechanism for exchanges on convicted third country nationals and evaluated their impacts from a technical, legal and organisational point of view[54]. A study on the Assessment of ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for third country nationals and stateless people (TCN) provided an overview of the cost incurred by the EU and the Member States for the implementation of the options[55].

External expertise

The Commission set up an Expert Group on the exchange of information on criminal record (ECRIS). The work of this group fed also into the preparation of the Impact Assessment.

The Commission services held in-depth interviews with the FIU.net[56], in particular as regards the Ma³tch, a way of intelligent information and knowledge sharing introduced by the FIU.net.

The Commission services have consulted, orally and in writing, the Fundamental Rights Agency (FRA), Vienna, and the Art.29-Working Party, i.e. Member States Data Protection Control Authorities.

---

[54] Project Final Report 'Feasibility Study: Establishment of a European Index of Convicted Third Country Nationals' dated 11 June 2010 ('Unisys study').
[55] Study on Assessment of ICT impact dated 04 December 2015 ('Kurt Salmon study', to be published).
[56] FIU.net, located in the Netherlands, is a platform connecting Financial Intelligence Units (FIUs) from the Member States. The purpose of the FIUs is to detect and disrupt terrorist finance and money laundering activities.

ANNEX 2: STAKEHOLDERS CONSULTATION

Brief summary of the consultation strategy/process

In line with the Commission's minimum standards regarding participation and openness to stakeholders' views presented in the Better Regulation Guidelines[57], an extensive consultation strategy has been developed to ensure a wide participation throughout the policy cycle of this initiative. This strategy was based on a mix of targeted consultations (bilateral contacts, stakeholder- and experts meetings, written consultations), providing the Commission with knowledgeable and representative options through bilateral contacts, stakeholder- and experts meetings. 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.

As the proposed initiative is of a technical nature on how to improve the exchange of information through an already existing information exchange system, the main choice to be made concerned the technical mechanism and the related costs. The proposed initiative does not extend its current scope beyond principle decisions already laid down in the existing ECRIS framework. It was therefore decided that due to the nature of this file a public consultation would not bring added value to the targeted stakeholder consultation.

The consultations aimed at gathering information on:

- o preferences of the Member States for one of the two main technical options: decentralised or centralised hit/no hit –search mechanism;
- o preferences of the Member States for the use of identifiers (fingerprints, alphanumerical data);
- o impact of the options on effectiveness of an improved ECRIS with regard to TCN, impact of the options on fundamental right, data protection requirements of the different options, administrative burden to implement each option for the Member States.

The Commission organised the following consultations throughout the impact assessment process:

I. Member States and national authorities:

a. Experts meeting with Member States representatives:

- to consult on a variety of possible option: 17 September 2014;

- to consult on financial and technical aspects on 18 September 2015.

b. July-October 2015: Member States survey done by an external contractor on the current technical and administrative circumstances in the Member States' central authorities.

c. September – November 2015: following the experts meeting on 18 September 2015, written consultations of all Member States, bilateral meeting with Member State representatives, other bilateral contacts with Member States authorities

All Member States supported a regulatory option. All Member States supported an index-filter based hit/no hit mechanism. A large majority of the Member States could support the decentralised option under the condition that the implementation software can be installed,

[57] SWD(2015) 111.

integrated and maintained smoothly at Member State level and that financial support (grants) would be available. Some Member States favour the centralised solution, as they consider that the central option would demand less implementation effort at Member State level, would be less costly for Member States and would better secure a common approach of the Member States. Few Member States were undecided.

With regard to fingerprints, there is no majority of the Member States supporting mandatory use of fingerprints in ECRIS. While the practical advantages with regard to secure identification of a person were acknowledged by many of them, a number of Member States expressed constitutional concerns and drew the attention to problems regarding the practical implementation of mandatory fingerprints in ECRIS: many Member States do currently not use fingerprints in their national criminal record registers, or there are no connections between their national AFIS and their criminal records authority. The mandatory use of fingerprints would therefore present a large scale exercise which cannot sufficiently rely on previous experience. Likewise, some Member States expressed concerns regarding possible double standards for EU nationals on the one hand and TCN on the other hand and regarding the fact, that not from all convicted persons contained in the national criminal record registers fingerprints have been taken, as national rules differ according to categories of offences and between Member States.

II. Target Stakeholder Consultation

a) With regard to data protection the Commission consulted:

aa) The Article 29 Data Protection Working Party

The working party was set up under the 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. It has advisory status and acts independently. The Article 29 Data Protection Working Party is composed of: a representative of the supervisory authority(ies) designated by each EU country; a representative of the authority(ies) established for the EU institutions and bodies; a representative of the European Commission.

The Commission presented the centralised and the decentralised option in the meeting of the working party on 23 September 2015, followed by a written consultation.

bb) The EDPS (European Data Protection Supervisor): the centralised and the decentralised option were presented to the EDPS in a meeting on 6 October 2015.

b) With regard to fundamental rights the stakeholders the Commission consulted:

aa) the European Union Agency for Fundamental Rights and

bb) NGOs representing on a European level academics, defence lawyers, rights of the child, migrants and refugees: Fairtrials (http://www.fairtrials.org/); OpenSocietyJusticeInitiative (part of Open Society Foundations- https://www.opensocietyfoundations.org/); CEPS (Centre for European Policy Studies- https://www.ceps.eu/); European Criminal Bar Association (ECBA -http://www.ecba.org/content/); JUSTICE (http://justice.org.uk/).

Meetings took place on 12 and 26 November 2015. The European Union Agency for Fundamental Rights delivered a written opinion on 4 December 2015.

Fundamental rights stakeholders acknowledged in general the positive effects of future ECRIS-TCN system from an overall justice perspective by contributing to appropriate sentencing, protecting children from abuse, as well as the positive effects on TCN as regards the legal certainty for persons with clean criminal record. They also advocated for the decentralised system accompanied by adequate anonymisation techniques (option 3) that would, in their opinion, entail less interference with the right to the protection of personal data in comparison to an index centrally established at EU level.

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

1. The improvement of ECRIS with regard to TCN could have the effect that in the future a significant part of the requests will be made for migration purposes. That is, we might face a function creep – ECRIS might become an instrument applied to a limited group of the EU population for purposes which only relate to their specific situation. It therefore would require specific safeguards set from the beginning.

2. The criminal record information made available through ECRIS-TCN, may entail more serious effects for the TCN in the context of migration, than criminal record information may in general entail for EU nationals. In particular, full information on criminal record information on TCN may influence a decision whether or not to return a TCN to his home-country outside the EU, to withdraw or to refuse the issuance or extension of a residence permit, etc. FRA recommended that the EU legislator would need to clearly define the system's purpose in a manner that limits EU Member States' discretion.

The Commission confirms that the future ECRIS-TCN is not meant to be a tool for the migration law purposes. It does not change any existing provisions and guarantees in this area. The recitals of the proposed legal instrument would explicitly acknowledge respect for the EU asylum and migration guarantees, which are to be upheld in the context of the future system.

3. Certain crimes, such as irregular entry or stay, or travelling with false visas or travel documents are specific to TCN and the future ECRIS-TCN should not result in disproportionate impact on the rights of TCN convicted for such offences. FRA suggested in this respect that convictions relating to irregular entry and stay should not be processed under ECRIS-TCN for purposes other than criminal proceedings.

4. Anonymisation of the ECRIS-TCN should not increase the risk of false matches and that there should be techniques to narrow down the amount of potential hits. A concern was expressed whether a dialogue between the Member States to establish the identity unequivocally will not prolong excessively the reply deadlines.

The Commission confirms that fuzzy logic techniques will be applied to determine only the most relevant hits.

5. The stakeholders acknowledged the possibility that an efficient identification of TCN might require use of fingerprints, as they pose more problems with identification than EU nationals.

However, according to FRA to assess the necessity and proportionality of using fingerprints for the index-filter, the alternatives of using passports and/or residence permits, as well as the possibilities offered by already existing EU and national databases, need to be taken into account. These need to be considered in comparison to the inclusion of fingerprints of all or certain categories of third-country nationals. If fingerprints are used, only templates should be stored.

6. Also TCN children may be particularly exposed to risks stemming from exchange of information on their convictions. Undergoing various forms of exploitation, for example by traffickers, they might be involved in criminalised activities leading to convictions. FRA suggested that in light of the vulnerability of children, consideration should be given to either excluding children from the scope of ECRIS altogether or from the index-filter, or to limiting exchanges to very serious crimes committed by children. At the same time, stakeholders would like to ensure that ECRIS-TCN should make it possible for employers to verify in an effective manner the existence of any disqualification from exercising activities involving direct and regular contacts with children arising from past criminal convictions.

The Commission explained that ECRIS is a decentralised tool for exchanging criminal records information gathered in the Member States' databases. It is up to the national law of the Member States to decide which minor and children's convictions enter the criminal records and are subject to exchanges at European level.

7. TCN themselves might have an interest in doing the bona fide requests for information about their own criminal record, which is particularly valid in case of convictions in absentia. It is vital to grant them such a possibility in order to ensure the legal certainty for persons with clean criminal record.

8. An effective right to access data and have it rectified, and the right to information for third-country nationals should be ensured in ECRIS-TCN. This needs to take into account issues such as the absence of an EU Member State of nationality, possible language barriers and, if fingerprints are involved, potential errors in the utilised technology. In the decentralised option – the guarantees of the new data protection legislation would apply to access of an individual to his criminal record; in the centralised option – some regulation at EU level would need to be ensured to give access for affected individuals to the central index-filter. Since inaccurate criminal records may be more common in cases involving TCN, safeguards would need to be built into ECRIS-TCN to ensure that only accurate data are exchanged and used, particularly for records pre-dating the establishment of the system.

ANNEX 3: WHO IS AFFECTED BY THE INITIATIVE AND HOW

The initiative will improve the functioning of a common area of security and justice by improving information exchange in criminal matters with regard to third country nationals and stateless people (TCN).

PRACTICAL IMPLICATIONS OF THE INITIATIVE FOR BUSINESSES

The initiative does not contain regulatory obligations for businesses and, thus, does not create additional costs related thereto.

PRACTICAL IMPLICATIONS OF THE INITIATIVE FOR PUBLIC ADMINISTRATIONS, COURTS AND CITIZENS

Apart from the obligation to transpose the Directive into national law and enforce it, the impacts on public administrations with regard to the set-up and the operation of ECRIS-TCN including costs are set out in Section 6.3.1 of the impact assessment and its annexes 7 and 8.

Courts are affected, as an improved ECRIS with regard to TCN will provide easy access to information on previous convictions of a TCN. Courts can fully implement Framework Decision 2008/675/JHA on taking account of previous convictions in new criminal proceedings concerning the same person (see under section 2.3.).

Administrative Member States authorities and national law enforcement authorities will be affected, as improved access to criminal record information will put them in the position to make better informed decisions better adapted to the individual requirements and circumstances. The variety of decisions that can be influenced by previous convictions (or the absence of previous convictions) are detailed under section 2.3.

Employers recruiting personnel for sensitive posts or for posts involving close contact with vulnerable persons will be affected, as they will be in a position to take account of previous convictions of a TCN (or the absence of previous convictions) when making a recruitment decision (see more detailed under section 2.3.)

Convicted TCN will be affected, as they will be put on the same footing with EU nationals: information on their criminal past will be available to decision makers regarding decisions where previous convictions may influence a decision (see the explanations above). The unconvicted majority of TCN, will be in a position to document a clean criminal record, when needed. This will facilitate their recruitment to sensitive posts and positively influence a number of administrative decisions where the absence of a criminal record is important (a.o. naturalisation, licenses to carry firearms, see section 2.3.) EU society will be affected, as sharing information on previous convictions handed down in the EU will contribute to reducing crime and crime-related costs, both tangible and intangible. It will strengthen trust in a common area of justice and security.

PRACTICAL IMPLICATIONS OF THE INITIATIVE FOR CONSUMERS

The initiative will not create any obligations for consumers.

ANNEX 4: VOLUME OF MESSAGES EXCHANGED IN ECRIS

The volume of exchanges in ECRIS is around 35 000 notifications and 25 000 requests messages per month, and these numbers show a tendency to increase.
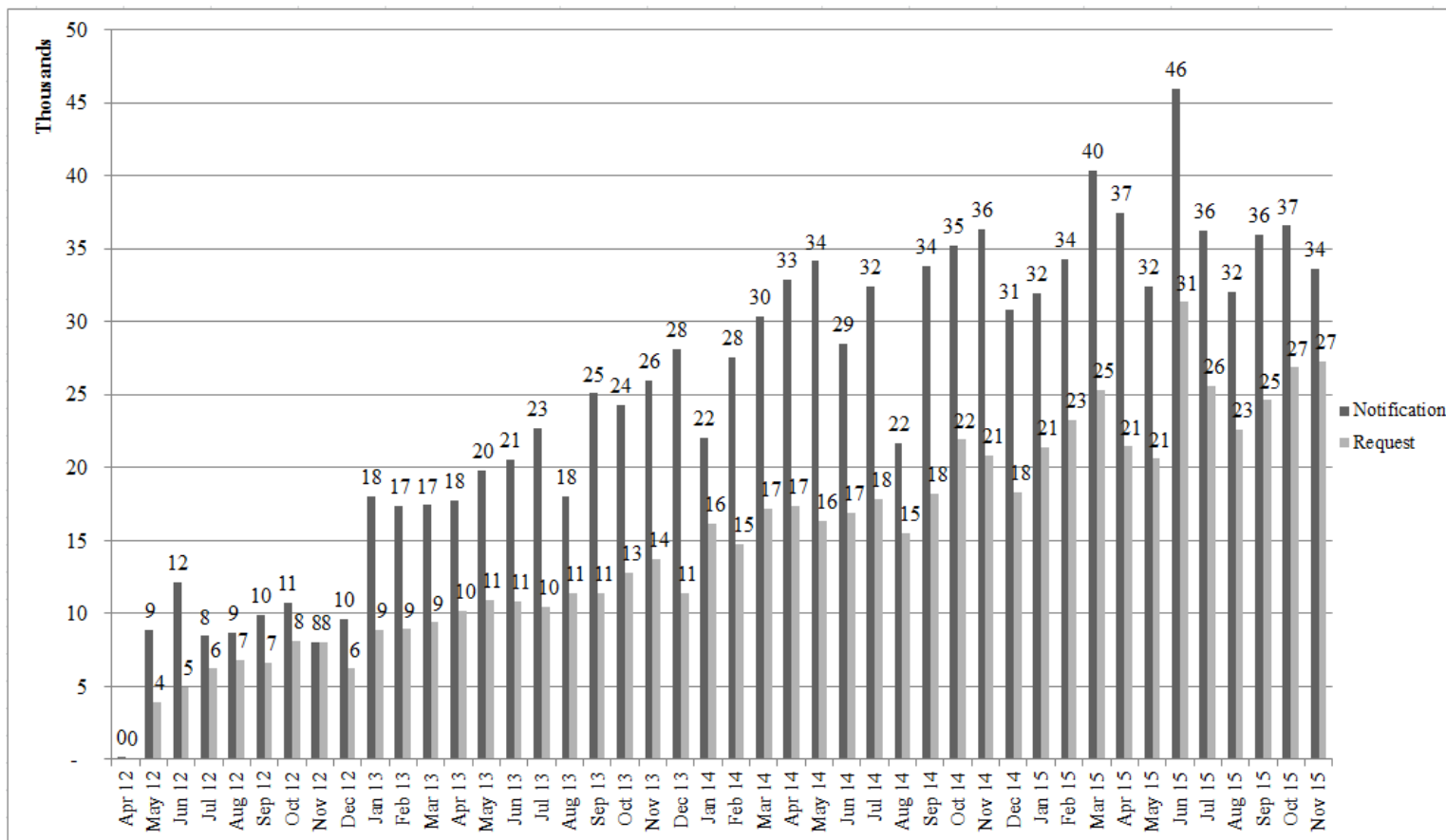
ANNEX 5: MA³TCH – AN EXAMPLE OF AN INDEX-FILTER BASED SEARCH MECHANISM AND ANONYMISATION TECHNOLOGY

The index-filter search mechanism is based on existing concepts and technology already used for the disclosure and sharing of sensitive information.

The growth of technology has brought new challenges to the protection of privacy. While technology has the ability to diminish privacy, its support can also be enlisted to protect privacy through the use of **Privacy Enhancing Technologies**. These technologies are predicated on the *Privacy by Design* philosophy embedding privacy into the design of specifications.

A new way of intelligent information and knowledge sharing – also known as Ma³tch (Autonomous Anonymous Analysis) - has been recently introduced in the FIU[58] network.

Ma³tch is based on a technology which aims at improving the exchange of sensitive information by excluding unnecessary requests, improving timeliness and enhancing privacy.

It thus provides a solution that can serve both aims by way of autonomous and anonymous data analysis: guaranteeing the interest to collect information and protecting privacy of personal data.

Ma³tch allows matching data with that of connected entities in order to check whether other entities have information in their databases. This is achieved through the creation of anonymous list that can be used to determine approximation matches without the need to share or expose personal data beyond its own premises.

The matching is performed in the following steps: 1) conversion of personal data into a uniform way; 2) then the anonymisation of the data is achieved through a combination of **anonymisation algorithms, space efficient probabilistic data structures**, **hashing, fuzzy logic** and **approximation technologies**; 3) the locks (anonymous information) are shared with one or more entities via a **decentralised network** and 4) compared with local information sources.
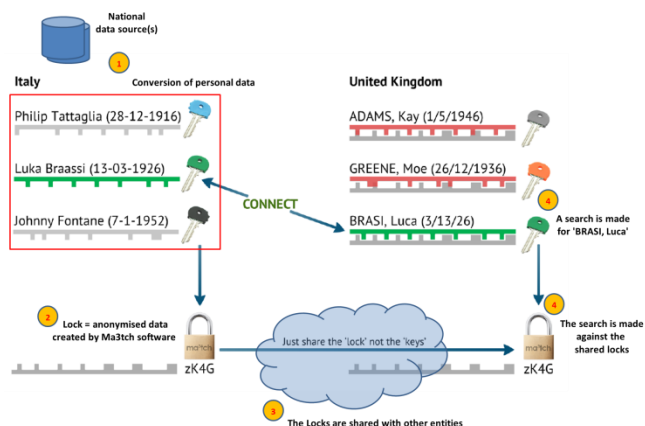
For example, if Ma³tch is applied to a list of three records containing personal details, the result is a **lock** like 'zK4G'. This is not an encryption and it is more than just **hashing**. Encrypted text can be decrypted. **Hashed text is irreversible**, but can potentially be traced back by means of 'rainbow tables'. 'Hashing' a hashed text is irreversible and it cannot be traced back to for example individuals. Once the lock (e.g., 'zK4G') is created there is no possibility of tracing back the original content of the lock.

---

[58]   Financial Intelligence Units (FIUs) are EU central, national intelligence agencies responsible for receiving, analysing and disseminating disclosures of financial information to the competent authorities (e.g., law enforcement or prosecutorial authorities) in order to combat money laundering and terrorism financing.

The algorithm used in FIU.NET was initially designed in the context of the Intersect project[59] for real time concept extraction and text analysis. It allows fast anonymous distributed cross matching: **a million records easily fit in a 1 MB anonymous data** structure and can be **matched in less than 0.3 milliseconds on a single 3 MHz processor** core, making it possible to check hundreds of distributed information resources in real time.

Currently Ma³tch does not handle fingerprints yet. The biometric matching technology exists and is already in use in for example election processes[60] where anonymised fingerprints are compared. However, to date no sufficiently mature matching technology for anonymised fingerprints offering sufficient capacity has been tested in large-scale information exchange systems. More research is required to assess the efficient application of *Privacy by Design* approach to biometrics such as fingerprints. The Commission could support financially such research.

Robustness of anonymisation techniques

Anonymisation can be performed using different techniques, namely randomisation, generalisation, noise addition, permutation, differential privacy, aggregation, k-anonymity, l-diversity, t-closeness, etc. Each anonymisation technique ensures a different level of 'robustness' – meaning a level of protection of the data privacy. The following opinion[61] expressed by the Article 29 Data Protection Working Party has been elaborated on the robustness of several techniques.

"*The Opinion concludes that **anonymisation techniques can provide privacy guarantees** and may be used to generate efficient anonymisation processes, processes, but **only if their application is engineered appropriately**.*

*The **optimal solution** should be decided on a **case-by-case basis**, possibly by using a combination of different techniques, while taking into account the practical recommendations developed in this Opinion.*"

Anonymisation market survey

Notwithstanding the ever increasing amounts of personal information in the public domain, the Privacy Enhancing Technologies is a niche market. To our best knowledge apart of the company which developed the Ma³tch software, it seems that there are very few solution providers operating in such specialised market. Recently the authorisation[62] was received to re-use the Ma3tch software.

Further reading and sources:

- "Anonymisation: Managing Data Protection Risk Code of Practice" published by the UK Information Commissioner's Office, https://ico.org.uk/media/1061/anonymisation-code.pdf

---

[59] 'Intersect Project', Internet: http://intersect.crowndesign.nl/.
[60] Example of a fingerprints based system to obtain an accurate and credible voter list, http://www.genkey.com/en/markets/elections
[61] Article 29 Data Protection Working Party - Opinion 05/2014 on Anonymisation Techniques adopted on 10/04/14,http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[62] Letter from Ministry of Justice and Security from the Netherlands dated 6 January 2016 concerning the non-exclusive license to use ma3tch software.

- "Privacy by Design: From Rhetoric to Reality"' published by the Information and Privacy Commissioner of Ontario, Canada, https://www.ipc.on.ca/images/Resources/PbDBook-From-Rhetoric-to-Reality.pdf
- "Privacy by Design and Anonymisation Techniques in Action: Case Study of Ma^{3}tch Technology" published by the European Privacy Association (EPA), February 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466990
- "Ma^{3}tch: Privacy AND Knowledge" published the 2013 IEEE International Conference on Big Data, October 2013.

1. Centralised fully fledged system

This option foresees the establishment of the central database for TCN at Union level that would contain the identity data of convicted TCN, together with all information on convictions entered in the criminal records of the Member States, such as the offence, the sanction, date of the decision, etc. Convicting Member States would be obliged to send full criminal record information to this central database.

Such a system could be highly effective in ensuring that timely and accurate criminal record information is exchanged. The added value for judicial and other authorities would be that the relevance of an individual's criminal history for a specified purpose would be immediately easily determined (i.e. whether the criminal history is relevant to a sentencing procedure - a minor driving offence might not be) and would therefore remove the need for further bilateral exchange of criminal record information helping to speed up relevant judicial processes, enhancing the provisions of ECRIS. Member State authorities would benefit from a lower workload related to the processing of requests.

The move towards a fully-fledged centralised ECRIS-TCN is however likely to be not accepted by the Member States as too invasive from the point of view of the protection of personal data. The presence of more than just identification information in a central system is considered by them to be a step too far towards a European Criminal Record System. Resistance to this option is therefore expected to be high and it seems politically infeasible in some Member States.

A fully centralised EU system would also raise governance issues. It would require a central management body that would be responsible for data protection and management issues arising from data contained in the central database. This option could raise data protection concerns and management inconsistencies with ECRIS and national law which would see TCN potentially being treated differently to EU citizens. Equally, national law may also be a barrier to different identification data being stored in the same system.

Finally, the establishment of a central database would impact negatively on the equal treatment of TCN and EU citizens as different systems will be used for exchanging information on previous convictions. This far reaching differentiation appears unproportioned from the fundamental rights point of view.

2. Decentralised system with a reference Member State for each convicted TCN

This option foresees the establishment of a decentralised ECRIS TCN and introducing obligations to: nominate the reference Member State for each TCN, to store criminal records of TCN, and to exchange information on TCN criminal records with other Member States. Convicting Member States would have to notify the country of references of any convictions taken on 'their' TCN. This reference Member State would take on the functions of the Member State of nationality in the established ECRIS. Member States of reference could be appointed based on:

– long-term residency status within a Member State (e.g. migrants, refugees, etc.); and

– short-term permission to enter / stay within a Member State (e.g. tourist visa, visa exemption, asylum application).

The 'responsibility' for TCN could be allocated to a particular Member State on the basis of the following criteria:

– where the TCN is legally residing;

– where the TCN applied for asylum;

– where the TCN was provided with a short-term visa / was allowed but did not require a visa.

Rules would be established in order to avoid cases of conflicts between Member States who might be appointed as reference countries for the TCN (for example, in cases where several Visa are issued by different Member States). Systems such as VIS and EURODAC might be used to support the choice of reference Member States as they include relevant data. All Central Authorities have access to EURODAC; only Schengen States have access to the VIS.

However, Member States may encounter difficulties in appointing reference countries for TCN. As shown by the consultation, the information on the category of TCN is not directly accessible through the criminal record and delays could be encountered when trying to access information on the status of the TCN. All the Member States consulted stated that the national criminal records do not include information on the residence status of the TCN, which is kept in a different register. Therefore, when consulting the criminal records, it is impossible to make a distinction between the different 'categories' of TCN and information on the status of a TCN can only be accessed on a case by case basis.

This option also presents the risk of TCN seeking to 'hide' the reference Member State by not disclosing their country of stay. TCN would need to present residence permit/visa when caught in a different country in order to know to whom to turn for information, and they have interest to hide this information. This might lead to problems in the identification of the reference Member State.

More significantly, this option would not resolve the problem for irregular TCN, who are not legally admitted to the territory of a Member State. This group would be left out of the system as no reference Member States can be appointed for such TCN. This might lead to reluctance from the Member States who indicated that it is important to access criminal records information for all categories of TCN without distinction.

3.   **A centralised solution with an anonymised index-filter (combining elements of option 3 and option 4)**

This option foresees combining the centralised index-filter with anonymisation software as in the decentralised solution. This would require Member States to install anonymisation software and run the anonymisation process before sending the index-filter to the central database.

It would however remove the advantage of the centralised option from a Member State view point, i.e. to offer a technically simple solution which would not require the integration, maintenance and updating of the anonymisation software at Member State level. This disadvantage is not outweighed by the advantages a centralised and anonymised solution might have over a decentralised solution. It is true, that the anonymisation of personal data would reduce the complexity of the centralised option requiring double layers of data protection and security measures. However, the costs for installing the centralised option remain high and will even rise if combined with the integration, maintaining and updating of the anonymisation software on Member State level. The advantages of the anonymised index-filter can be achieved more cost-efficient in the decentralised option.

4. **An exchange of information only for specific offences**

An option establishing a proportionate exchange of information on TCN only for specific offences based on their severity (e.g. terrorism) was not considered, as for EU nationals such limitation does not exist. The proposal does not intend to change the existing ECRIS but aims at making ECRIS as efficient for TCN as it is today for EU Nationals.

An external Contractor was mandated by the European Commission Directorate-General for Justice and Consumers (DG JUST) to assess the ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for TCN.

The objective of this study was to evaluate in terms of costs the two most realistic options identified.

The methodology applied is described in more detail in the Contractor's final report[63].

1. Cost elements

Table 1 describes in more detail the cost elements considered and the assumptions used for calculating the costs of the centralised and decentralised option.

---

[63]   Study on Assessment of ICT impact dated 04 December 2015 ('Kurt Salmon study', to be published), section 1.

Stake-holder Group	Cost element for the decentralised option	Cost elements for the centralised option
Costs for the EU	**Application software** •Description: the Application software cost element includes cost related to the customisation, installation and configuration of the software application based on FIU.net's Ma3tch. Maintenance and overall support (support fee) are included. •Assumptions: the software will be integrated with the existing ECRIS Reference Implementation software. Even though this is an existing product, some development (such as the customisation of the search, the integration of the GUI with the ECRIS RI, the production of monitoring and statistical reports, etc.) costs are considered, but they are assumed less substantial than if a completely new software application would have to be developed. •Common fingerprint matching software •Description: the common matching software cost element includes cost related to the development, customisation, installation and configuration of the fingerprint matching software application possibly based on existing technologies. Maintenance and overall support (support fee) are included. •Assumptions: the software will be integrated with the existing ECRIS Reference Implementation software.	**Load Index Application** •**Description:** the cost element Load index Application includes the development and maintenance of a software application that will load the data files (such as XML files) received from Member States into the central ECRIS TCN index-filter. •**Assumptions**: the Load Index Application will be integrated with existing ECRIS application, namely the ECRIS Reference Implementation. **User Interface** •**Description**: the cost element includes cost related to the development maintenance and support (helpdesk) of a graphical user interface for the ECRIS TCN search. •**Assumptions:** the user interface will be integrated in the already existing graphical interface of the ECRIS Reference Implementation. **Search Application** •**Description:** the cost element Search Application includes the development and maintenance of a search intelligence software with the following characteristics: o search requests: collection of end-users requests based on search criteria; o search results: production of a response to the user(s) by displaying the results on the users interface immediately after the search request transmission;

Stake-holder Group	Cost element for the decentralised option	Cost elements for the centralised option
Costs for the EU		**Search Application** •**Assumptions:** the search application will be integrated in the already exiting search engine of the ECRIS Reference Implementation. The cost estimates include the purchase of a dedicated license for a search engine (i.e. WCC Elise). It is assumed that the ECRIS TCN System will enable advanced intelligent searches. **Monitoring and Analytics application** •**Description**: the cost element includes the development (configuration) and maintenance of a software application that would monitor the provision of data files to the central database (traceability/audit mechanism to allow tracking of who has provided which data and when it was provided) and provide statistics reports on end user searches. •**Assumptions:** approximately 25 additional reports of average complexity (including software client license and server scheduler (I.e. Crystal Reports)) are assumed to be integrated in the already existing module of the ECRIS RI. No dedicated database tables are expected to be used than the one used in the ECRIS TCN transactional tables.

Stake-holder Group	Cost element for the decentralised option	Cost elements for the centralised option
		Infrastructure of the central index •**Description:** the cost element infrastructure includes the acquisition of the required hardware and software, and the following installation, configuration and connection. The cost element also includes the maintenance of hardware and software, connections and support (helpdesk). •**Assumptions**: the following technical specifications of the Central hit/no hit system were considered: o availability: 97%; o restore time: return to normal operation should not exceed 1 week; o performance: 2 times batch updates per day; o volumes of queries: approximately 10K queries per day; o type of queries: exact and advanced intelligent searches; o query response time: 3-4 seconds; o data retention: depending on the national policy; scalability: approximately 7.5 million of records as initial storage with an average growth rate per year of 700 000 records.
Costs for the EU	**Training** •**Description:** the training cost element includes the training of the end users of the Decentralised hit/no hit system. •**Assumptions**: training will be provided once per year with duration of 3 working days involving 2 representatives per Member State. The expenses include are travel costs, accommodation, subsistence expenses for the participants and the trainers. A 'train-the-trainer' approach is assumed.	

Stake-holder Group	Cost element for the decentralised option	Cost elements for the centralised option
Costs for the EU	**Project Implementation** •**Description**: the Project implementation cost element includes the management of the implementation of the ECRIS TCN system including: planning, business requirements analysis, functional requirements analysis, coordination activities, testing and roll out. •**Assumptions:** this cost item accounts only the efforts on coordination activities performed by the DG JUST. The cost of project implementation is included in the cost element Application software.	**Project Implementation** •**Description**: the Project implementation cost element includes the management of the implementation of the ECRIS TCN system including: planning, business requirements analysis, functional requirements analysis, coordination activities, testing and roll out. **Assumptions:** the project implementation activities are carried out by eu-LISA. Coordination and follow-up activities performed by DG JUST staff is included.
Costs for Member States	**Extract identification data on convicted TCN** •**Description:** the cost for extracting identification data on convicted TCN includes the development, and maintenance of a software application (routine/script) that will automatically and regularly extract data from the national criminal records and load it in the software application. •**Assumptions:** the extraction is performed by means of a routine/script under the form of a web service. The update is assumed to be done at least twice a day. Given that this is already the case for ECRIS, the cost related to this element is significantly lower than in the centralised solution where a connection to a not yet established central entity is foreseen.	**Extract and transmit identification data on convicted TCN** •**Description:** this cost element includes the development, maintenance and support of a software application (routine/script) that will automatically and regularly extract data from the national criminal records and transmit it to the central index-filter via the secure EU network (sTESTA). •**Assumptions:** the extraction is performed by means of web services. The update is assumed to be done at least twice a day. A web server will be exposed with a central entity through the secure EU network (sTESTA). Therefore it is anticipated that the cost related to this application is a sensibly higher than for the decentralised solution**.**

Stake-holder Group	Cost element for the decentralised option	Cost elements for the centralised option
Costs for Member States	**Infrastructure (hardware + software)** •**Description:** the cost element infrastructure consists of the acquisition, overall set-up (some development), maintenance and support of the hardware, software and network connections. •**Assumptions:** the hardware lifecycle is longer than 5 years and therefore hardware update cost is not considered in the estimations. **Adapting the national AFIS** •**Description:** the cost element consists of the adaptation the national AFIS, maintenance and support of the hardware, software and network connections. •**Assumptions:** even if some Member States have an existing AFIS (and even if the national AFIS is interconnected with ECRIS), more storage capacity such as additional hard disks and processing capacity is anticipated to handle fingerprints for ECRIS TCN purpose. In addition, the fingerprints will be anonymised.	**Infrastructure (hardware + software)** •**Description:** the cost element infrastructure consists of the acquisition, overall set-up (some development), maintenance and support of the hardware, software and network connections. •**Assumptions:** the hardware lifecycle is longer than 5 years and therefore hardware update cost is not considered in the estimations. **Adapting the national AFIS** - **Description:** the cost element consists of the adaptation of the national AFIS, maintenance and support of the hardware, software and network connections. - **Assumptions:** even if some Member States have an existing AFIS (and even if the national AFIS is interconnected with ECRIS), more capacity such as additional storage capacity and processing capacity is anticipated to be needed to handle fingerprints for ECRIS TCN purposes.

Table 1 Detailed description of the costs elements for both options

2. General assumptions

2.1. Scalability of the central system

The volume of criminal records of TCN: a relevant aspect for development of the ECRIS TCN system is the magnitude/size of the future database that needs to be established. The number of criminal records of TCN has a direct impact on the cost as well as the scalability of the system, which should be able to accommodate a certain level of entries into the ECRIS TCN database.

The following Table 2 provides an overview of the most recent volumes (in thousands of convicted TCN) provided by Member States through questionnaires submitted in 2010, 2012, 2014 and 2015[64].

Table 2 Number of convicted TCN (in thousands) provided through several surveys

Surveys	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK	Total
2010																				1,0									1,0
2012				21,0	18,0			2,5				714,7														5,0			761,2
2014	44,4										6,9			9,3			3,0												63,6
2015		304,5				817,2			598,4	790,8			2,7			971,0		9,1	94,9		534,0	30,3	42,7	0,03	73,8				4269,5

Where data was not submitted, estimates were calculated on the basis of Member State TCN population (BG, DK, IE, SK and UK).

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK	Total
Estimates			61,0				44,7								52,9												2,3	500,0	660,9

Total
5.756,2

It is reasonable to assume that there are at least 6 million[65] convicted TCN in the EU in 2014.

For scalability purposes a margin was taken of approximately 20%. Subsequently, it is reasonable to assume that at least 7.5 million records should initially be stored into the ECRIS TCN database.

[64]   Studies: in 2010 (Unisys study) and 2015 Study on Assessment of ICT impact dated 04 December 2015 ('Kurt Salmon study', to be published).

[65]   Surveys based on similar data obtained through consultation with Member States estimated that that there were approximately 3 million convicted TCN in the EU in 2009 (Unisys survey, page 211) and around 4 million convicted TCN in the EU in 2011.

Based on the information collected from Member States, an average of approximately 700 000 convictions of TCN were recorded per year across all Member States in the period 2010-2014.

2.2. Daily Labour Rates

According to the Better Regulation Guidelines, the costs for development, support, maintenance and training are collected in person days from all stakeholder groups. In order to monetise these costs, the collected persons days are computed using the daily labour rates to convert person days into Euros. The labour rates are provided by Eurostat's structural earnings' survey of 2010 for occupation group ISCO 3 (Technicians and associate professionals). The figure below represents the daily labour rates per Member States in Euro.
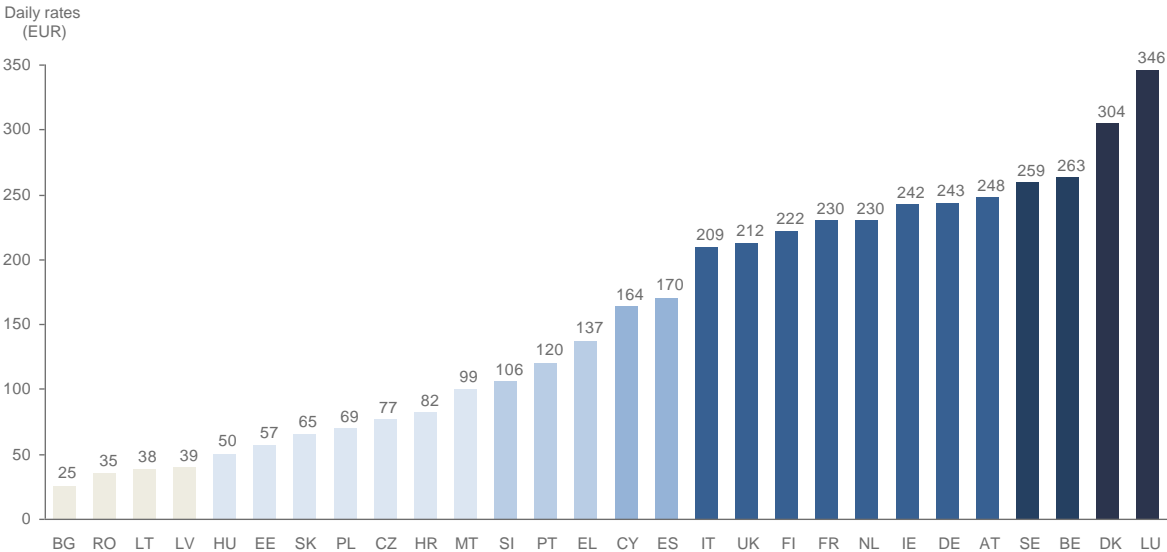
The following table gives an example on the impact of the daily labour rate when monetising the effort (person days) using for example the Member State with the lowest (Bulgaria) and the highest (Luxembourg) daily labour rate.

MS	Daily Labour Rate (in €)	Effort for maintenance of the infrastructure (in persons days)	Costs for maintenance of the infrastructure (in €)
BG	25.33	24	608
LU	345.96	24	8303

2.3. Cost for using the sTESTA network

The costs of communication infrastructure s-TESTA connecting Member States and EU were not considered, as it is assumed that all Member States use this infrastructure already under the current ECRIS framework.

2.4. No modification required of national criminal record systems

The extraction of identification data on convicted TCN from the national criminal records to a file in a format such as XML is assumed to be of low complexity for all Member States. This assumption is based on the fact that all Member States confirmed[66] to:

- store electronically the same information on convicted TCN as on convicted EU nationals;
- store electronically the criminal record information on TCN in the same national register as for EU nationals; and
- store electronically the criminal record information on TCN in a single (central) database.

2.5. Average cost values used for the development of the extraction routine

In the centralised option:

The costs for extracting identification data on convicted TCN includes the development and maintenance of a software application (routine/script and web services) that will automatically and regularly extract data from the national criminal records and load it in the software application. A web server will be exposed to other Member States through the secure EU network (s-TESTA).

Where no data was available or inconsistent data was provided by the Member States, the following average costs values were considered:

- Development: 60 person days (one-off cost). This value is an average based on the provided estimates and corresponds to an implementation effort of 3 months. This seems a reasonable assumption as it is comparable to the average effort made in ECRIS for the extraction of data from national criminal record register.

- Maintenance: 12 person days (on-going cost representing 20% of the development cost).

In the decentralised option:

The cost for extracting identification data on convicted TCN includes the development and maintenance of a software application (routine/script and web services) that will automatically and regularly extract data from the national criminal records and transmit it to the central index-filter via the secure EU network (s-TESTA).

Where no data was available or inconsistent data was provided by the Member States, the following average costs values were considered

- Development: 80 person days (one-off cost). The cost related to this element is sensibly higher than in the decentralised solution because there is not yet a central entity established.
- Maintenance: 16 person days (on-going cost representing 20% of the development cost).

---

[66] Source: responses to section 2 of the on-line survey on ICT cost assessment conducted in July 2015, Study on Assessment of ICT impact dated 04 December 2015 ('Kurt Salmon study', to be published).
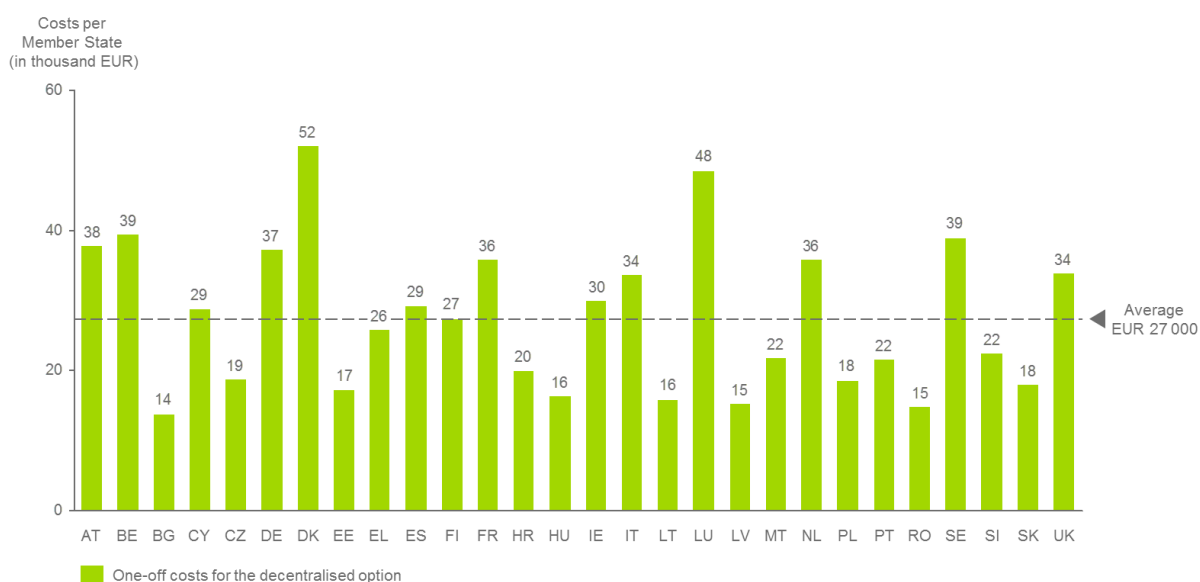
3. Costs associated with the decentralised option

Table 3 summarises the total costs (one-off and maintenance per year) incurred for the European Union and for 28 Member States to implement the decentralised option.

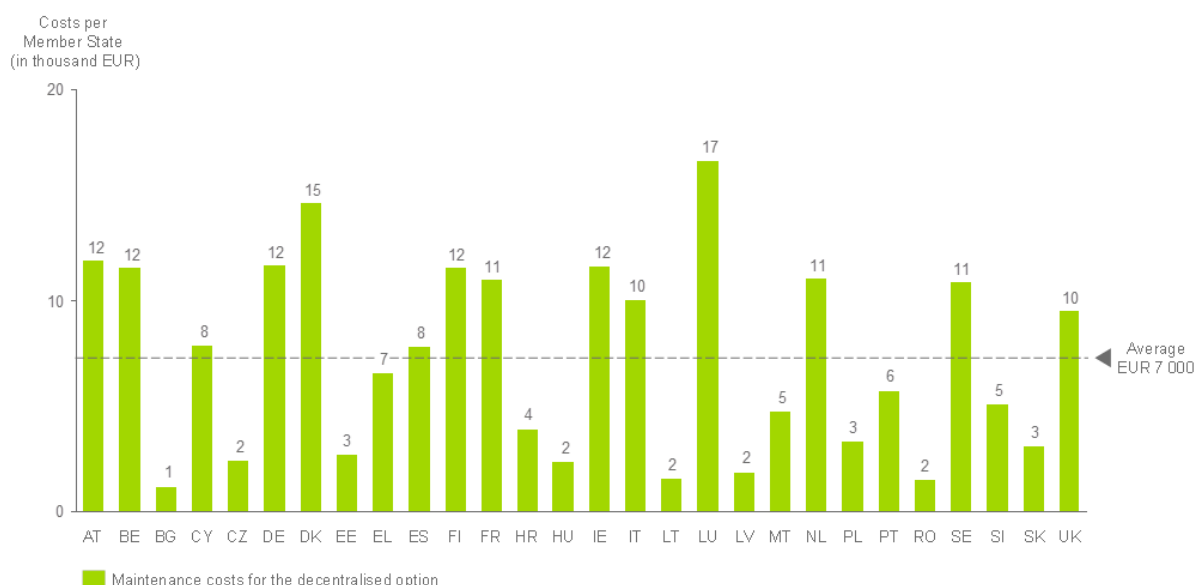| Estimated costs (in €)	One-off costs (in €)	Maintenance costs per year (in €)
Decentralised option without mandatory fingerprints		
For the EU	1 089 000[67]	502 000
For 28 MS	768 000	204 000
Total	**1 857 000**	**706 000**

Table 3 Summary of the costs related to the decentralised option

The following Graph 1 and Graph 2 provide the costs incurred per Member State for the decentralised option.

Graph 1 One-off cost per MS for the decentralised option

---

[67] The one-off costs of ECRIS established in 2012 were approximately € 3.5 million.

Graph 2 Yearly maintenance cost per Member State for the decentralised option

4. Costs associated with the centralised option

Table 4 summarises the costs incurred by the European Union and for 28 Member States to implement the centralised solution.

Estimated cost (in €)	One-off costs (in €)	Maintenance costs per year (in €)
Centralised option without fingerprints		
For the EU	5 274 000	1 285 000
For 28 MS	856 000	227 000
Total	**6 130 000**	**1 512 000**

Table 4 Summary of the costs related to the centralised option

The following Graphs 3 and 4 provide the costs incurred per Member State for the decentralised option.
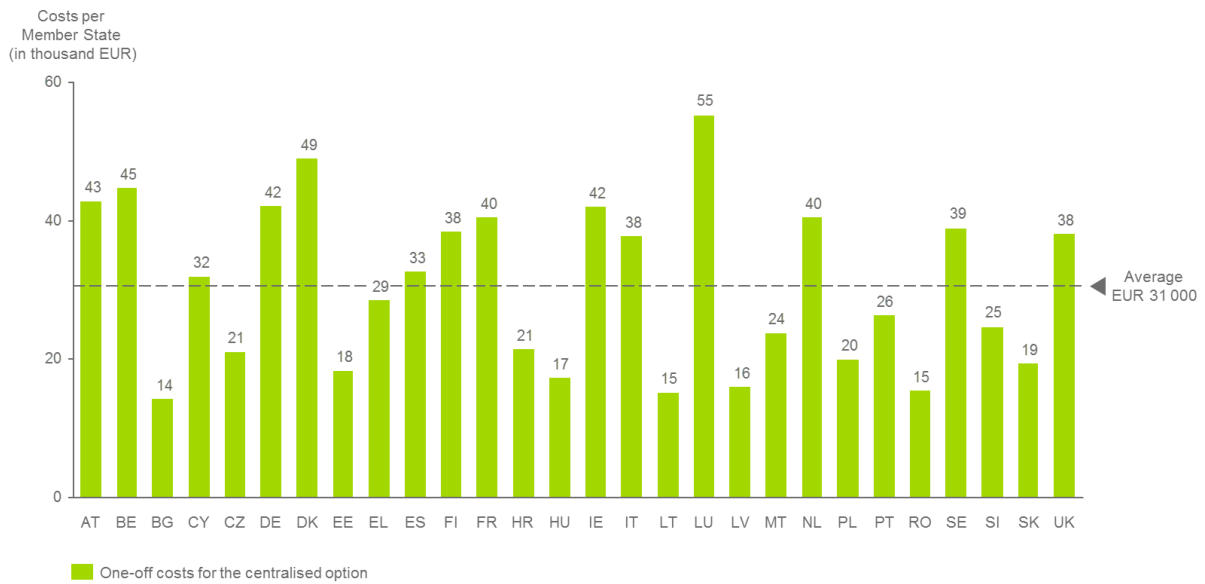
Graph 3 One-off cost per Member State for the centralised option
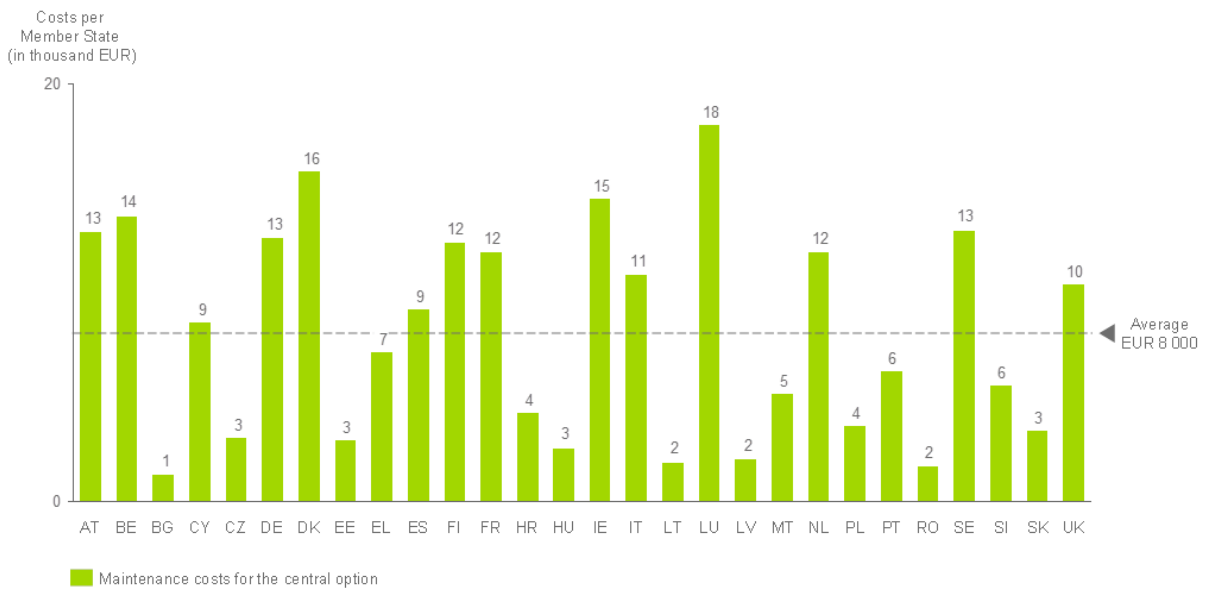
Graph 4 Maintenance cost per Member State for the centralised option

5. Use of fingerprints

5.1. For the decentralised option

The research conducted confirmed that the implementation of fingerprint matching functionalities enabling search for convicted TCN using fingerprint data is feasible.

The research found that matching fingerprints could be done by linking the ECRIS TCN system to the already available fingerprint matching systems in the Member States (national existing AFIS). This might imply adding a dedicated server at national level on which fingerprint matching software is installed and interconnected with ECRIS.

At present, all Member States have an existing AFIS[68].

Estimated one-off costs for MS[69]:
- With an anticipated high volume of activity: € 3 000 000.
- With an anticipated modest volume of activity: € 1 000 000.
- With an anticipated low volume of activity: € 500 000.

Estimated recurring yearly maintenance costs for the MS[70]:
- For MS with a high volume of activity: € 900 000.
- For MS with a modest volume of activity: € 300 000.
- For MS with a low volume of activity: € 150 000.

The volume of activity is related to the number of TCN convictions. The volume of TCN convictions is described in more details in Annex 11.

The implementation of fingerprints matching functionality would imply additional costs (for all MS) of € 58 000 000 as one-off costs and € 17 400 000 for maintenance. Table 4a presents the estimated costs for implementing a fingerprint matching function for the decentralised solution.

Estimated costs for all the MS (in €)	One-off costs (in €)	Maintenance costs per year (in €)
Implementation of a decentralised fingerprint matching functionality (including infrastructure)	37 500 000	11 500 000

Table 4a Cost for implementing fingerprint matching functionalities for the decentralised option for all MS

In addition to the costs referred to above, it is anticipated that the common ECRIS Reference Implementation software will be adapted in order to include the fingerprint anonymisation

---

[68] Study on Assessment of ICT impact dated 04 December 2015 ('Kurt Salmon study', to be published).

[69] The estimated costs of adapting the national AFIS is based on costs provided by EU-LISA (KurtSalmon Study, to be published) and experience from other EU AFIS systems. For MS with an anticipated high volume of activity, the cost for adapting the existing AFIS is estimated to be € 3 000 000; for MS with a modest volume of activity, € 1 000 000 of a central EU AFIS, and for MS with a low volume of activity, € 500 000.

[70] For common IT systems the maintenance costs are in the order of 20% of the one-off cost (such as in ECRIS for example). For specialised IT systems with specific technologies such as fingerprints matching systems, a share of 30% of the one-off cost was considered for yearly maintenance.

and matching software. This would be developed by the EU. Consequently, the implementation of fingerprints anonymisation and matching functionality would also imply additional costs for the EU as presented in Table 4b.

Estimated costs for the EU (in €)	One-off costs (in €)	Maintenance costs per year (in €)
Adaptation of the ECRIS Reference Implementation to handle the fingerprint matching functionality (including anonymisation).	5 000 000	1 000 000

Table 4b Cost for implementing fingerprint matching functionalities for the decentralised option for the EU

5.2. For the centralised option

The research conducted confirmed that the implementation of fingerprint matching functionalities enabling search for convicted TCN using fingerprint data is feasible.

This initial research confirmed that matching fingerprints in the decentralised option could be done by storing the fingerprint data in the central ECRIS TCN database which would allow the fingerprints to be searched against other fingerprints sent by a Member State. The implementation of fingerprints matching functionality would imply additional costs of € 1 970 000 as one-off costs and € 450 000 for maintenance. Table 5 presents the estimates for implementing a fingerprint matching function within the ECRIS TCN centralised solution.

Estimated costs for the EU (in €)	One-off costs (in €)	Maintenance costs per year (in €)
Implementation of a central fingerprint matching functionality (including infrastructure)	1 970 000	450 000

Table 5 Cost for implementing fingerprint matching functionalities for the centralised option for the EU

At present, all Member States have an existing AFIS[71].

Estimated one-off costs for adapting of the existing AFIS to include the fingerprint capacity for ECRIS for MS[72]:
- With an anticipated high volume of activity: € 3 000 000.
- With an anticipated modest volume of activity: € 1 000 000.
- With an anticipated low volume of activity: € 500 000.

Estimated recurring yearly maintenance costs for the MS[73]:

---

[71] Study on Assessment of ICT impact dated 04 December 2015 ('Kurt Salmon study', to be published).
[72] The cost of adapting the national AFIS is based on costs provided by EU-LISA (KurtSalmon Study, to be published) and experience from other EU AFIS systems. For MS with an anticipated high volume of activity, the cost for adapting the existing AFIS is estimated to be € 3 000 000; for MS with a modest volume of activity, € 1 000 000 of a central EU AFIS, and for MS with a low volume of activity, € 500 000.

- For MS with a high volume of activity: € 900 000.
- For MS with a modest volume of activity: € 300 000.
- For MS with a low volume of activity: € 150 000.

The volume of activity is related to the number of TCN convictions. The volume of TCN convictions is described in more details in Annex 11.

The implementation of fingerprints functionality would imply additional costs (for all MS) of € 37 500 000 as one-off costs and € 11 500 000 for maintenance. The Table 6 presents the estimated costs for implementing a fingerprint matching function for the decentralised solution.

Estimated costs for all MS (in €)	One-off costs	Maintenance cost per year
Adaptation of the existing AFIS to include and store fingerprint for ECRIS	37 500 000	11 500 000

Table 6 Costs for adapting the national AFIS for all MS in the centralised solution

[73] For common IT systems the maintenance costs are in the order of 20% of the one-off cost (such as in ECRIS for example). For specialised IT systems with specific technologies such as fingerprints matching systems, a share of 30% of the one-off cost was considered.

Administrative costs[74] are calculated on the basis of the average cost of the required administrative activity multiplied by the total number of activities (frequency) performed per year. The cost is estimated by multiplying a tariff (based on average labour cost per hour in each Member State) and the duration required per activity.

1. List of activities (workflow) for the baseline scenario (option 1) compared to the different options

The baseline scenario is the situation 'as-of-today'. To date there are 25 Member States exchanging criminal record information. 3 Member States (PT, MT and SI) out of 28 are not yet exchanging criminal record information.

In both options (centralised or decentralised) it's assumed that the mechanism to exchange criminal record for TCN will be implemented by 28 Member States.

Table 1 describes the administrative activities performed in the baseline scenario, in the centralised option and the decentralised option.

---

[74] Since 2006, the Commission has been working to reduce the regulatory burdens (e.g. reporting and monitoring) created by EU legislation – making administrative processes easier and more efficient for citizens and businesses. More details on the Standard Cost Model to apply is to found here: http://ec.europa.eu/smart-regulation/refit/admin_burden/scm_en.htm

No	Activity	Baseline scenario (ECRIS with 25 MS)		Decentralised option (28 MS)		Centralised option (28 MS)	
		Frequency of the activity	Duration (in minutes)	Frequency of the activity	Duration (in minutes)	Frequency of the activity	Duration (in minutes)
1	**Storing or updating information about convictions** in the national criminal record system.	= Number of TCN convictions for 25 MS	5	= Number of TCN convictions for 28 MS	5	= Number of TCN convictions for 28 MS	5
2	**Extracting information on convictions** from national criminal record system.	= TCN requests in ECRIS	0-10	= 70% of number of TCN convictions for 28 MS	0-10	= 70% of number of TCN convictions for 28 MS	0-10
3	**Anonymisation of TCN conviction data.**	This activity is not performed in the current workflow in ECRIS		= 70% of number of TCN convictions for 28 MS	0	This activity is not performed in the centralised workflow scenario	
4	**Sending TCN identification data.**	This activity is not performed in the current workflow in ECRIS		= 70% of number of TCN convictions for 28 MS	0	= 70% of number of TCN convictions for 28 MS	0

No	Activity	Baseline scenario (ECRIS with 25 MS)		Decentralised option (28 MS)		Centralised option (28 MS)	
		Frequency of the activity	Duration (in minutes)	Frequency of the activity	Duration (in minutes)	Frequency of the activity	Duration (in minutes)
5	**Searching for a convicted TCN**	This activity is not performed in the current workflow in ECRIS		= Number of TCN convictions for 28 MS	15	= Number of TCN convictions for 28 MS	15
6	**Sending a request**	= TCN requests in ECRIS	5	=120% of TCN convictions	5	=120% of convicted TCN	5
7	**Replying to a request** (also in case of a hit through ECRIS TCN).	= TCN requests in ECRIS	10	=120% of TCN convictions	10	=120% of convicted TCN	10

Table 1 Workflow of the baseline ('As-is' situation) compared to the different options

2. Assumptions

For the calculation of the administrative cost the following assumptions were considered.

2.1. Calculation methods

As can be seen from the list of activities (workflow) above (Table 1), there is no difference between type, frequency and duration of the activities between the decentralised and the centralised systems. Therefore, the same calculation method is used for both options. The method of calculation for the baseline scenario is different, as explained in the following assumptions below.

2.2. The number of stored or updated convictions for baseline scenario

In the baseline scenario, centralised and decentralised option

For the calculation of the administrative cost, when known the exact number of TCN convictions per Member States was used, based on average across all Member States in the period 2010-2014. Where data was not available, estimates were calculated.

2.3. The level of automation of Member States for the different tasks

The tasks should be partly or fully automated, depending of the level of automation of each Member State. Even for highly automated systems, manual interventions are expected for the validation of returned data, the adjustment of the search parameters, etc.

- AT, BE, CY, CZ, DE, ES, FI, FR, HR, HU, IT, PL and RO are considered as Member States with a high level of automation. This implies that the duration of some activities such as for example the extracting or updating of TCN data from their national criminal records system, the sending to the central system or to the anonymisation server, the sending of one or more requests is negligible.

- BG, DK, EE, GR, IE, LT, LU, LV, MT, NL, PT, SE, SI, SK and UK are considered to be Member States with a low level of automation. This implies that the duration of some activities such as the extraction or updating of TCN data from the national criminal records system sends them into the ECRIS TCN system is estimated to 10 minutes.

2.4. Duration for the execution of some activities such as the handling of an ECRIS request

When the answer provided was a range between 5-10 minutes, a limit value such as 10 minutes was used. Where data was not available or not provided, the median value from the provided answers[75] (the median is the middle value) was used.

---

[75] Answers were provided by MS during the on-line survey carried out in July 2015

2.5. The number of request and responses to request per year

In the baseline scenario

For the calculation of the administrative cost of the baseline scenario, the numbers of requests sent by each Member State are based on ECRIS statistics in 2014. Each request is answered, even if there are no past criminal record convictions. Subsequently the number of replies is equal to the number of requests.

In the centralised or decentralised option

Statistics in ECRIS as illustrated in the Table 2 show that 30% of responses to requests contain one or more convictions. A similar percentage of positive responses is assumed for TCN requests. It means that a search for TCN convictions would yield a positive response match in 30% of the searches.

In addition searches in any of the options could yield several matches. For example, an advanced search on 'Mr BRASI' could yield an exact with the same name and other matches with other spellings such as for example 'Mr Braassi' or 'Mr Brashi', etc. For each match, the end-users will send a request to the corresponding Member States. Considering the administrative burden incurred by the handling of requests by the other Member States, the end-users are expected to narrow down the search to a reasonable and workable amount of matches. Therefore it is anticipated that end-users will stop searching when the number of matches is between 2 and 6. For the calculation of the administrative cost, the average figure of 4 matches is considered.

Therefore, the 30% of searches/requests (leading to positive response) is multiplied by 4. This means the estimated number of requests = 120% of the number of TCN convictions in each Member State.

Each request is answered, even if there are no past criminal record convictions. Subsequently the number of replies is equal to the number of requests.

ECRIS - Responses to requests per year						
	2012[76]		**2013**		**2014**	
Response with no convictions	31.901	67%	80.926	65%	127.513	62%
Response contains one or more convictions	14.248	**30%**	38.251	**31%**	63.498	**31%**
Denial - not allowed to answer	300	1%	726	1%	3.863	2%
Problem: Multiple persons found	443	1%	1.414	1%	6.303	3%
Problem: Person deceased	101	0%	30	0%	84	0%
Problem: Not a national	460	1%	2.839	2%	4.804	2%
Problem: Fingerprints do not match main identity	1	0%	4	0%	23	0%
	47.454	100%	**124.190**	100%	**206.088**	100%

Table 2 ECRIS responses to requests (for the period 2012-2014)

2.6. Duration of the search for previous TCN convictions

When a search returns several hits, associated requests/replies will need to be issued. Given the administrative burden associated with the handling of responses, it is anticipated that end-users will narrow down the number of hits to a manageable amount. For example end-users are expected to adjust their search criteria by adding for example date of birth, country of birth, to lower the number of hits. For estimation purposes, a conservative assumption of 15 minutes was used.

2.7. Frequency of search for previous TCN convictions in the options

In a scenario of full implementation, each TCN convicted will trigger a search for previous convictions. However, based on ECRIS statistics, the search for past convictions increased gradually over the years. Assuming a similar approach for TCN, it's reasonable to consider that the number of searches will gradually increase over the years starting from more or less 30% of the volume of TCN convictions up to 100% of the volume of TCN convictions at max in normal operations.

2.8. Frequency of extracting or updating TCN data

Every time there is a new TCN convicted or when related identity data changes (for example: change of name after marriage), Member States need to extract or update the identification data of the TCN from the national criminal records system and send them into the ECRIS TCN system.

---

[76] Go live in April 2012, 8 months of ECRIS exchanges.

This frequency is not necessarily the same as the number of TCN convictions in that Member State, as a new conviction could be linked to an already convicted person. As stated earlier, statistics in ECRIS show that 30% of responses to requests contain one or more convictions.

Therefore it was estimated that the frequency of extracting or updating TCN data in the decentralised or centralised system is 100% - 30% = 70%.

3. Administrative costs associated with the baseline scenario

The total administrative cost for the baseline scenario is estimated at approximately € 1 465 000, with average of € 59 000 per Member State as illustrated in Table 3. The calculation was based on the exact spread of TCN requests per Member State and the average labour cost per hour in each Member State.

Member State	Administrative cost of ECRIS for the baseline scenario per year (in €)
AT	29.000
BE	72.000
BG	2.000
CY	5.000
CZ	3.000
DE	18.000
DK	121.000
EE	265.000
EL	40.000
ES	11.000
FI	87.000
FR	1.000
HR	1.000
HU	8.000
IE	42.000
IT	151.000
LT	1.000
LU	48.000
LV	1.000
NL	301.000
PL	7.000
RO	1.000
SE	43.000
SK	3.000
UK	204.000
Total (in €)	**1.465.000**
Average (in €)	**59.000**

4. Administrative costs incurred by 'blanket' requests

In a fully implemented system, each TCN convicted will trigger a search for past convictions. The administrative cost associated with this hypothetical scenario is estimated at approximately € 78 500 000 per year as illustrated in Table 4.

No	Activity	Duration (in minutes)	Frequency of the activity	EU hourly rate (in €)	Cost (in €)
1	Storing or updating information about convictions in the national criminal record system.	5	700.000	23,2	1.350.000
2	Extracting information on convictions from national criminal record system.	10	700.000	23,2	2.710.000
6	Sending a request to 27 member states (blanket)	5	700.000	23,2	1.350.000
7	27 member states replying to a request	10	700.000 x 27	23,2	73.120.000
	Total Administrative cost with blanket requests for 28 MS (in €) per year[77]				**78.530.000**

Table 4 Costs incurred by Member States blanket requests

5. Individual cost of a 'blanket' request

Another way of measuring cost effectiveness is by comparing the individual cost of requests in the different options against the baseline scenario. A 'blanket' request in the hypothetical baseline scenario should trigger 27 replies. Consequently the associated cost per request is estimated at €106, as illustrated in Table 5 below.

No	Activity	Duration (in minutes)	Frequency of the activity	EU hourly rate (in €)	Cost (in €)
6	Sending one request to 27 Member States (blanket request)	5	1	23,2	2
7	27 Member States replying to one request	10	27	23,2	104
	Administrative cost for one request sent (in €)				**106**

---

[77] The figure is rounded.

Table 5 Costs of one 'blanket' request with 27 responses (baseline scenario)

In options 3 and 4, a request is only sent to those Member States identified as holding criminal record information. A conservative assumption would that there are on average 2 hits per search. Consequently there will be 2 replies. The cost per request in the ECRIS TCN option is €10, as illustrated in Table 6 below.

No	Activity	Duration (in minutes)	Frequency of the activity	EU hourly rate (in €)	Cost (in €)
6	Sending one request to several Member States (who have hits)	5	1	23,2	2
7	Several Member States replying to one request	10	2	23,2	8
	Administrative cost for one Request sent (in €)				**10**

Table 6 Cost of one request in any of the ECRIS TCN options

6. Administrative costs associated with the option(s)

6.1. Cost summary

As mentioned in the Assumptions section of this Annex, it is reasonable to consider that the number of searches will gradually increase over the years starting from **more or less 30%** of the volume of TCN convictions **up to 100% of the volume of TCN convictions at max in normal operations**. Therefore, the administrative cost is estimated at approximately starting from € 5 100 000, which represents in average € 180 000 per year per Member State, up to € 12 600 000 which represents in average € 450 000 per year per Member State in normal operations. This is illustrated in Table 7.

	Administrative cost of ECRIS TCN per year (in €)		
Member State	**30% of TCN Convictions are Searched**	**50% of TCN Convictions are Searched**	**100% of TCN Convictions are Searched**
AT	54.000	87.000	141.000
BE	172.000	278.000	449.000
BG	2.000	4.000	6.000
CY	7.000	12.000	19.000
CZ	5.000	8.000	12.000
DE	1.109.000	2.142.000	3.826.000
DK	208.000	265.000	358.000
EE	40.000	68.000	113.000
EL	157.000	221.000	327.000
ES	202.000	313.000	494.000
FI	4.000	9.000	15.000
FR	735.000	1.185.000	1.917.000
HR	2.000	2.000	4.000
HU	20.000	32.000	51.000
IE	94.000	132.000	194.000
IT	392.000	632.000	1.023.000
LT	1.000	1.000	1.000
LU	150.000	197.000	273.000
LV	300	400	700
MT	2.000	3.000	4.000
NL	592.000	755.000	1.020.000
PL	10.000	16.000	25.000
PT	59.000	84.000	124.000
RO	1.000	1.000	1.000
SE	157.000	214.000	308.000
SI	50.000	91.000	157.000
SK	2.000	4.000	6.000
UK	842.000	1.190.000	1.757.000
Total (in €)	**5.100.000**	**7.900.000**	**12.600.000**
Average (in €)	**180.000**	**280.000**	**450.000**

Table 7 Administrative costs associated to the options

6.2. Examples of Member State calculations

AT (Austria)

No	Activity	Duration (in minutes)	Frequency of the activity	Hourly rate for AT (in €)	Cost (in €)
1	Storing or updating information about convictions in the national criminal record system.	5 (EU median)	7.186 (Number of TCN Convictions)	31	19.000
2	Extracting information on convictions from national criminal record system.	0 (automated)	5.030 (70% of number of TCN convictions)	31	0
5	Searching for a convicted TCN, including the fine-tuning of the search results.	15	2.084 (30% Number of TCN Convictions)	31	16.000
6	Sending a request	5 (EU median)	2.501 (120% of TCN convictions)	31	6.000
7	Replying to a request (also in case of a hit through ECRIS TCN).	10 (EU median)	2.501 (120% of TCN convictions)	31	13.000
	Administrative cost for AT (per year)				**54.000**

Table 8 Administrative costs associated with the option(s)

7. Comparison of the administrative costs

Comparison of the Administrative cost (in €)	Total cost per year (in €)		Average cost per year (in €)	
	At Start	**Max**	**At Start**	**Max**
Baseline scenario (for 25 Member states)	1 465 000		59 000	
Decentralised or centralised option (for 28 Member States)	5 100 000	12 600 000	180 000	450 000

ANNEX 9: PROVISIONAL TIMETABLE

European Criminal Record Information System (ECRIS)

Implementation of the exchange of criminal record information extracted from the criminal record registers for Third Country Nationals (TCN)

T_0	Adoption of the legal basis
T_0+6 months	Technical Architecture, Security Analysis and Business Analysis
T_0+8 months	Detailed Technical Specifications and Logging, Monitoring and Statistics Analysis
T_0+9 months	Verification of Conformity Analysis and ECRIS RI Fit gap analysis
T_0+12 months	Development and customisation of the ECRIS TCN solution (including the adaptation of the ECRIS RI)
T_0+15 months	Release of the prototype demo software version
T_0+17 months	Release of final ECRIS TCN software solution and training of end-users
T_0+18 months	Roll out and go-live in Member States (installation and set-up)

	Who	Purpose	Identifiers	Where and how	Retention period
VIS	Schengen States and Denmark	• Visa purposes • Fighting terrorism/organised crime • Asylum/first MS of entry	Fingerprints	<u>EU-Lisa</u> Central database	5 years

SIS II (replaces SIS)	• Schengen States
	• Associated countries: Switzerland, Norway, Iceland
	• Other EU-Member States for law enforcement cooperation: Bulgaria, Romania, UK
	• preparatory activities to integrate into the SIS: Cyprus, Croatia, Ireland
		• Border control: Alerts on TCN with objective to prevent them from entry
		• Law enforcement: Alerts on missing or wanted person/objects
		• Contains also for alerts:
		  • a statement why person is sought
		  • instruction on the action to be taken
		• Vehicle registration: Check legal status of vehicles presented
			Set of identification data; where available: fingerprints, photograph
			
			more detailed, bilateral info-exchange through Sirene bureaus, through structured exchange of standardised forms
				<u>EU-Lisa:</u>
				operates central-system and communication software
				
				MS operate national systems at single contact point (Sirene bureau)
				Alerts are entered into the national systems and are automatically transferred to and made available at the central system
					Until purpose has been achieved

PRÜM (Council Decisions 2008/615/JHA and 2008/616/ JHA	EU MS	Combat and prevent crime, Cooperation between police and judicial authorities	DNA/Fingerprints/ Vehicle registration	MS allow each other searches in the DNA analysis files and fingerprint identification systems (AFIS) and vehicle registration data bases. MS obliged to operate these data bases; <u>Decentralised</u> search mechanism on hit/no hit basis. Done by national contact points. Bilateral contacts through SIENA (secure communication channel), works with references (anonymisation)	
EIS (Europol Information	28 MS	Support MS in combatting organised crime, terrorism and other serious crimes	Crime relevant information on suspected person from national law	Central database at Europol, Can be searched and fed by	data to be deleted if purpose has been

			enforcement records (customs, border, police etc) convictions are stored, if related to Europol's compe-tences; fingerprints possible	Europol national units in MS, Possible: a hit/no hit mechanism with direct contacts afterwards	achieved, checked every three years
Eurodac (European Dactyloscopy) Regulation No 603/2013	28 MS	Identification of asylum applicants	Fingerprints	Centralised system operated by the Commission, fed by MS, reference code connect the fingerprints to particular person, request dealt with within 24 hours	10 years

Based on the information collected from Member States, averages of convictions of TCN were recorded per year across all Member States in the period 2010-2014.

Table 1 shows the collected data for the number of convictions of TCN in the EU.

MS	Number of TCN convictions in the EU
	Average (over the period 2010-2014)
AT	7.186
BE	21.577
CY	1.457
CZ	2.379
DE	228.607
ES	47.211
FI	1.506
FR	105.512
GR	25.356
HR	623
HU	13.028
IT	61.820
LT	407
LU	11.483
LV	124
NL	39.644
PL	4.372
PT	11.026
RO	458

Table 1 Number of TCN convictions in the EU (average over the period 2010-2014)