ARTICLE 29 DATA PROTECTION WORKING PARTY

18/EN

WP266

Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration

Adopted on 11 April 2018

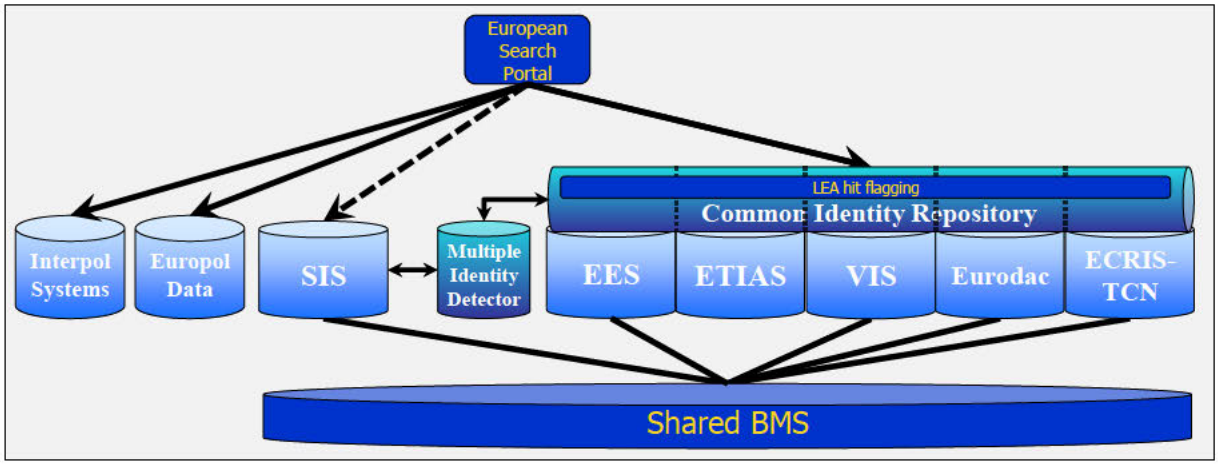
I. Introduction

In December 2017, the Commission put forward two draft regulations on interoperability between existing and future European information systems in the field of border control, migration, international protection as well as police and judicial cooperation. The two proposals COM 2017/793 and COM 2017/794 are complementary. The overall goal is to cross-link all those systems by way of forming a new system architecture.

The new architecture will cover the Schengen Information System (SIS II), the Visa Information System (VIS), the European Dactyloscopy (EURODAC), the future Entry-Exit-System (EES) as well as – in case of their adoption – the future European Travel Information and Authorisation System (ETIAS) and the European Criminal Record Information System for Third Country Nationals (ECRIS-TCN).

The intended interoperability of all those systems is supposed to make all available data on third country nationals (TCN) serviceable for national authorities in their respective tasks. One key goal is to facilitate identity checks, detect the use of multiple identities and by doing so combat identity fraud.

In the explanatory memorandum, the Commission indicates that the two draft regulations propose the establishment of four new instruments to achieve interoperability and provides this explanatory scheme of the proposed architecture:



Both drafts contain a similar chapter on data protection, including rules on responsibility, data security, confidentiality of SIS data, data breach notifications, obligations of self-monitoring for controllers, data subjects rights and data protection authorities. The transfer of data stored in interoperability components to third countries is prohibited without any exceptions.

Regrettably, the Impact assessments accompanying these two proposals fail to provide any detailed analysis concerning certain data protection aspects. In particular, no further explanation is provided to clarify which data protection regime will apply to which operation and no evaluation of the specific security measures needed for these new EU-wide databases is foreseen. In addition, no analysis of less intrusive means to reach the goals set in these proposals has been provided to justify the choices made.

As already stated in the WP29's Letter on the Entry/Exit System and other recent proposals on the large scale IT systems used for border management, visa policy and asylum procedures in 2016 the process towards the interoperability of systems raises fundamental questions regarding the purpose, necessity and proportionality of the data processing involved as well as concerns regarding the principles of purpose limitation, data minimization, data retention and clear identification of a data controller.

With the concrete proposals on interoperability at hand now, the WP29 wishes to give a more detailed analysis of the proposed legal instruments from a data protection point of view.

II. Necessity and proportionality of the four new tools

The WP29 first wishes to assess the proposed interoperability solutions to determine whether they create new or additional fundamental rights interferences (focused on Art. 7 and 8 of the EU Charter of fundamental rights) and whether those interferences can be justified in accordance with Art. 52 (1) of the Charter.

Art. 52 (1) of the Charter provides that any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be brought only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Limitations caused by the two draft regulations would qualify undoubtedly as limitations provided for by law. The WP29 assumes for the time being that the goals as described in the proposals genuinely meet objectives of general interest recognized by the Union. The following analysis will thus focus on the necessity and the proportionality of the proposals.

1) European Search Portal (ESP)

The first tool is a common European Search Portal (ESP) which is presented by the Commission as a single search interface which aims at enabling end users to conduct parallel searches in all the respective information systems as well as certain Europol and Interpol data. The access regime builds on the existing access rights and is to be implemented by the use of different access profiles.

Nevertheless, while each underlying data base already allows for searches within the strict perimeter of each data base, the question arises whether the mere capability to do one centralized search of all the underlying data bases and get one combined result can pose an additional interference in itself with the rights to privacy and data protection.

As regards the necessity of the European Search Portal, the WP29 is of the view that the justification advanced concerning the facilitation of the technical and operational implementation by Member States of existing and future new information systems cannot be considered as an acceptable demonstration of the necessity of this tool. Indeed, the current underlying data bases are already functioning, and no demonstration of failures to technically or operationally implement them has been provided. Therefore, it appears that the necessity of the ESP is rather directed at enabling the implementation of new information systems. On this aspect, the WP 29 would like to underline its doubts as regards a demonstration of the necessity of a tool which is based on the will to create new information systems.

The European Search Portal is capable of giving an overview of all the information relating to a certain TCN that is available in the connected EU information systems as well as Europol data and Interpol systems and therefore requires caution in particular in respect of the impact on data subjects' rights deriving from search tools. Even if the Portal does not accumulate the available data from these information systems with data from additional sources, the result is related to different matters such as travel, migration, international protection, law enforcement and judicial proceedings. Therefore, although this tool may not be sufficient in itself to establish a more or less detailed profile of the data subject concerned, it is important to ensure that - in particular when additional functions or additional access rights than the existing ones are envisaged -, the establishment of a European Search Portal does not lead to any additional interference with the rights to privacy and data protection.

2) Common Identity Repository (CIR)

The second tool is a Common Identity Repository (CIR), which is a new data base with the biometric and alphanumeric identity data extracted from all the underlying systems – with the exception of the SIS II which is presented as too complex in its own structure. The principle of purpose limitation is to be upheld in a first step by a logical separation

of data originating from or belonging to the different information systems. According to the explanatory memorandum of the proposals, what will remain in the separate source systems, will be data concerning the special administrative procedures.

According to Article 17 of the proposal, the Common Identity Repository is supposed to facilitate and assist the correct identification of persons registered in the separate systems, to support the functionality of multiple identity detection and to facilitate and streamline access by law enforcement authorities.

However, the use of data in the CIR for purposes distinct from those of the original collection and the consolidation of data from different information systems is intended from the beginning. This derives from Art. 19: When the Multiple Identity Detector creates a red or white link between the data of two or more of the respective information systems, instead of creating a new individual file, the CIR shall add the new data to the individual file of the linked data. This cross-matching of various sources for identification and consolidating them in a new common data base for the purpose of overall identification poses an additional interference with the rights to privacy and data protection.

- The necessity of consolidating different identification sources in a common identity register on third country nationals and using this consolidated data base for identification must be sufficiently justified regarding each of the respective administrative procedures i.e. visa application, travel authorization, border controls, application for international protection / asylum and judicial cooperation as well as multiple identity detection and combating identity fraud. In any case, this consolidation should result in an improvement of the quality of personal data kept in the systems.

Moreover, it has to be taken into account that the consolidated identity register also contains biometric data. In accordance with Article 9 of Regulation 2016/679 and Articles 10 of Directive EU 2016/680 and of regulation 45/2001, the processing of biometric data for the purpose of uniquely identifying a natural person qualifies as processing of special categories of data and is only allowed under certain additional conditions. The storage of biometric data in the CIR therefore has to be strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject.

Regarding the central storage of biometric data, the CJEU has indicated that central storage of biometrics would need to comply with more stringent requirements than their local storage in an ID-document in the possession of the data subject.[1] As already

[1] CJEU, C-291/12, Schwarz v. Bochum, 17 October 2013, para. 40; based on ECtHR, No. 30562/04 and 30566/04; Marper v. UK, 4 December 2008, para. 103.

stressed in previous opinions and letters, the Working Party repeatedly criticized instruments providing for the storage of all EU passport holders´ biometric and other data in a centralised data base of European passports and travel documents[2]. In addition, the GDPR and the directive 2016/680 reinforced the requirements provided by EU law as regards data minimization and expressly includes biometric data in the list of sensitive data deserving increased safeguards to be processed.

In this regard, there is no discussion of any alternative solutions in the Commission's Impact Assessment. For example, to issue some kind of EU identity paper including biometric identifiers and to put an obligation on TCN to carry it with them might appear a less intrusive but equally appropriate measure, for example. So far in the view of the WP29, the necessity of a consolidated database including biometric identifiers has not been established yet and the mere fact that some databases containing these types of data have already been created and constitute precedents does not demonstrate this necessity.

In any case, assuming the necessity could be sufficiently established, considerable concerns would still remain regarding the proportionality of the proposal. What is created here is in sum a database including a huge number of TCN being present in the EU (as well as TCN willing to come and TCN having already left).

The Working Party 29[3] previously underlined that "*there is a risk that the setting up of a centralized database containing personal data and in particular biometric data of all (European) citizens could infringe the basic principle of proportionality."* This was also the position expressed by the Committee on Civil Liberties, Justice and Home Affairs in a report of 25 October 2004, which underlined that *"the setting up of a centralised database would violate the purpose and the principle of proportionality. It would also increase the risk of abuse and function creep. Finally, it would increase the risk of using biometric identifiers as 'access key' to various databases, thereby interconnecting data sets.""*

The ECtHR has itself drawn a clear line in its ruling that the retention of fingerprints in a central biometric register solely for the reason of preventing future identity theft would, in practice, allow for the storage of information on the entire population, which would be clearly excessive (without additional specific guarantees, such as the effective right to obtain the deletion of the data for the concerned data subjects)[4]..

[2] See for instance opinion on implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States - 1710/05/EN WP 112 04/09/12 Opinion Adopted on 30 September 2005 - Official Journal L 385 , 29/12/2004 p. 1 - 6

[3] See previous opinion 1710/05/EN WP 112

[4] ECtHR, No. 19522/09, M.K. v. France, 18 April 2013, para. 40.

Whether a biometric register on TCN could be considered to be proportionate for the purpose of reliable identification and combating identity fraud or whether it constitutes an unjustifiable discrimination of TCN is yet to be answered. The majority of individuals whose data would be stored in the CIR would be bona fide travelers whose data would be stored side-to-side with convicted criminals (from ECRIS-TCN). Whether identity fraud is such an essential threat to the internal security as to justify the central registering of biometric identifiers of all bona fide TCN travelers, migrants and asylum seekers, is not yet sufficiently established and the proportionality of such a measure therefore highly questionable.

Furthermore, regarding identity data that is already stored in the different information systems, the proposals are not entirely clear about whether these data are to be extracted from the existing systems and consolidated in the CIR as well. This would be even more questionable, because at the time of the collection of that data, this supplementary change of purpose was not foreseeable to data subjects. Besides, the risk of duplication of data should be duly considered in order to respect the data minimization principle.

3) Shared Biometric Matching Service (sBMS)

The shared Biometric Matching Service is supposed to enable the searching of biometric data (facial images and fingerprints) from of all the underlying systems with the exception of ETIAS which does not store biometrics.. Where each of these systems currently uses a dedicated, proprietary search engine for biometric data, the shared biometric service, would provide for a common platform, where the data is searched simultaneously. The original biometric data would be retained in the underlying systems, or rather the CIR or the SIS II, while the sBMS would create and store a mathematical representation and discard the original data.

According to the Commission's Impact Assessment, the sBMS would not handle any new data and it would not modify any existing end-user access rights. It would contain "non-sensitive" biometric templates without any biographical data. Matching biometric templates in one shared system would enable better and harmonized quality control of biometric samples. It would create substantial benefits in terms of security, cost, maintenance and operation relying on one unique technological component instead of five different.

The WP29 notes, however, that in its understanding the quality of fingerprints has been a problem in the existing databases using them, and that questions about the converted templates and their reliability are likely to arise, when these are converted from low quality fingerprints as stored in the underlying systems.

Also, WP 29 takes the view that biometric templates cannot be regarded as non-sensitive data. They may contain a more limited amount of personal information than the biometric data themselves and in a coded form, but that extract serves as a preprocessed format for matching and is capable of providing unique identification in an automated matching process[5]. The special power of biometric data is their capacity to serve as a universal identifier allowing information about the same person to be linked across different information sources.[6] This is exactly the intended use of the biometric templates here and therefore a biometric template has to be qualified as biometric data.

In addition, no specifications or restrictions to the creation of the templates are foreseen in the draft regulations.

According to Article 13, the sBMS shall store the biometric templates and include in each template a reference to the information systems in which the corresponding biometric data is stored. According to Article 15, these data are to be stored for as long as the corresponding biometric data is stored in the underlying systems. Therefore, the sBMS actually constitutes a second biometric database. This data base is more limited than the CIR on the one hand, because only an extract of the original data is stored in there, but goes further than the CIR on the other hand, because it also contains biometric templates drawn from the SIS II.

Regarding the creation of a biometric register, the concerns regarding necessity and proportionality are the same as stated above regarding the CIR.

The necessity and proportionality are equally questionable here, since in addition the sBMS will not be restricted to biometric templates on TCN, but also include templates of EU citizens being subject to any kind of alert in the field of police and judicial cooperation in criminal matters.

Furthermore, the storage of templates in an additional database is also highly questionable in terms of data minimization. The pure facilitation of searching and matching procedures cannot be sufficient to prove the strict necessity of an additional storage, especially with regard to the strengthened requirement of data minimization provided in the GDPR.

Insofar the Fundamental Rights Agency in its report on interoperability has already claimed as well that a biometric matching service should not be programmed to actually

[5] See WP 193 Opinion 3/2012 on developments in biometric technologies of the WP29.

[6] Mordini, E., Green, M.: Human rights, identity and anonymity: Digital identity and its management in e-Society. Identity, security and democracy (2009), p.11.

store data but only to match it.[7] The WP29 supports this claim and call the attention to the need that such matching could be carried out only for purposes that are not incompatible to the purposes for which the data have been collected and processed.

4) Multiple Identity Detector (MID)

The fourth tool is a so-called Multiple Identity Detector (MID), which constitutes the third new data base created by the proposals. The MID fills the remaining gap between the CIR and the SIS II. Since the SIS II is described as being too complex in itself, the possibility to integrate the identity data from SIS alerts into the CIR has been ruled out. Therefore the MID is designed not only to compare CIR and SIS II data, but also to store links between different data sets.

Each time data are created or updated in any of the respective data bases, this triggers an obligation to launch a multiple identity detection. The MID performs this task by conducting a comparison in the sBMS and a comparison of certain alphanumeric data using the ESP. Whenever a hit occurs, a link is created in the respective systems and stored in the MID. Therein the match is classified by use of a predefined color scheme which triggers certain follow-up investigations and measures, if needed. That way it shall be established whether certain individuals use different identity data lawfully or unlawfully. Multiple identity detection is made an integral and obligatory part of all the administrative procedures in the field of border management, visa application, application for international protection, criminal registers on TCN as well as judicial and police cooperation on border management and law enforcement in the Schengen area[8]. The MID is established as a tool to serve this purpose this purpose of detection of multiple identity.

The system of links works as follows:

- When a yellow link is established, a manual verification of different identities is required and leads to a reclassification as green, white or red.
- A link has to be classified as green, when similar alphanumeric data belong to different biometric data which means different persons. Once classified as

[7] European Agency for Fundamental Rights: Fundamental rights and the interoperability of EU information systems: borders and security (2017), p. 24.

[8] See the explanatory memorandum of the proposals: "the MID would enable the detection of multiple identities linked to the same set of biometric data, with the dual purpose of ensuring the correct identification of *bona fide* persons and combating identity fraud."

green, future searches will not produce a hit regarding those sets of data anymore.

- A link has to be classified as red, when different identity data share the same biometric data and these different identities unlawfully refer to the same person. The follow-up to a red link shall take place in accordance with Union or national law.
- A link has to be classified as white, when the linked data share the same biometric and the same or similar identity data or the respective person legally uses different identity data or when there are similar identity data but no biometric data in at least one of the linked data sets.

The proposal does not sufficiently explain why and for how long it is necessary to retain all the different established links.

Whenever verification leads to a reclassification as red link, this should lead to follow-up actions as foreseen in Union or national law. There has to be some kind of reaction to the unlawful use of different identities, at least a correction of data, when there has been an explainable mistake. When such follow-up actions have been concluded, the red link should have served its purpose in combating identity fraud. Usually, after having served their purpose, the storage of data appears to be no longer necessary, so that they could be deleted. Without further explanation the WP 29 is not convinced of the necessity to store red links until the deletion of the linked data sets.

Only in green link situations there seems to be a comprehensible reason for keeping the links. When two different people with different biometrics share the same alphanumeric identity data, the green link will help to avoid future confusion of two different persons. When there is only one or no set of biometric data and for that reason it cannot be finally concluded whether the same alphanumeric identity data belong to one or two persons, this leads to a classification as white link. The future benefit of such a white link is not entirely clear, because a final verification was not possible in the end. The situation is quite the opposite when the linked data share the same biometric data and the same or similar identity data. It is very clear then, that there is only one and the same person. Updating the alphanumeric data in the CIR will avoid hits and yellow links in future multiple identity checks and the links has served its purpose. The future benefit of keeping the link is very unclear. The third situation leading to a white link is when a single person identified by biometrics lawfully uses different alphanumeric identity data. In such situations the white link could indeed avoid future checks in the interest of the respective person. On the other hand such links could possibly apply to police or intelligence service agents or persons under special protection like in a witness-protection-program. Storing a link between the two sets of identity data could be highly counterproductive to the purpose of the lawful use of different identities. Anyway, the authority responsible for the verification of different identities, shall – without prejudice to special requirements regarding SIS alerts –

inform the respective person of the presence of discrepancies between his or her personal data in different systems and shall provide a reference to the responsible authorities. The respective person then can contact those authorities to amend or update their data to avoid future discrepancies and the link has served its purpose. The future benefit of keeping the link is quite unclear again.

III. Additional access rights to the CIR and the underlying data bases for police and designated authorities

1) Access to the CIR by police authorities for identification purposes

Article 20 of the proposals foresees that Member States police authorities, where so empowered by national legislative measures, and solely for the purpose of identifying a person, could query the CIR with the biometric data of that person taken during an identity check.

In sum, this access right is only allowed by the proposals, but would have to be envisaged by national legislative measures which would have to specify the precise purposes of identity checks, to designate the police authorities competent and to lay down the procedures, conditions and criteria of such checks.

The Working Party therefore understands that the Commission has chosen to only avail the possibility to Member States to grant access to the CIR to their police authorities, but that they will bear the responsibility to comply with the criteria laid down by the CJEU in its Digital Rights ruling to grant these access rights under national law.

First, the Working Party would like to underline that, in its view, providing for the possibility to access the CIR for the sole purpose of identification of a person, irrespectively to the existence of access rights to the underlying data bases feeding the CIR, as it would be the case for police authorities in the context of Article 20, would raise serious concerns as regards the purpose limitation principle and the proportionality of this provision. Indeed, the mere fact that the setting up of the CIR results in the creation of a centralised data base does not justify that access to this data base for the purpose of identification of a person is justified in itself. The WP29 would like to stress its major concern as regards the creation of access rights to an EU-wide data base on the sole justification that this data base is available and that such access would be of added value, in this case for police authorities. In addition, the Working Party would like to underline that querying the CIR for the purpose of identification of a person could result in a very large number of accesses given the volume of identity checks led by police authorities.

Besides the fact that, indeed, legislative measures granting such access rights to the CIR to police authorities would have to comply with the requirements of the Court as regards access rights, and thus provide for strong safeguards surrounding access to these data, the WP 29 also would like to recall that in its Digital Rights ruling[9], the Court also underlined (see point 66 of the judgment) that the legislator was required to provide "for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data". The WP 29 therefore has strong doubts that such additional access rights granted to police authorities would comply with the requirement to have specific rules, adapted to the vast quantity of data concerned, even if in the current draft regulations, contrary to the invalidated so-called "data retention directive", a provision imposes the specific obligation on Member States to establish at least some rules at national level (specify the precise purposes of identity checks within legislative measures providing for such additional access to police authorities, designate the police authorities competent and lay down the procedures, conditions and criteria of such checks). In the view of the WP29, these requirements concerning what should be foreseen in the national measures to grant access to the CIR to police authorities are insufficiently precise to meet the requirements of the Court.

2) Two-step approach for access for law enforcement purposes

In addition to access granted under national law for the purpose of identification, article 22 of the draft regulations also provides for a new access regime for designated authorities of Member States to consult the CIR for law enforcement purposes.

Contrary to the access provided in Article 20 for identification purposes, access to the CIR "for the purpose of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case and in order to obtain information on whether data on a specific person is present in the EES, the VIS and [the ETIAS]" is directly provided for in the draft regulations and is not an option left to the Member States.

As described in the explanatory memorandum of the proposals, the so-called "hit-flag functionality" of the CIR introduces the possibility for accessing the EES, the VIS, the ETIAS and Eurodac using a two-step data consultation approach. The draft regulations do not provide a full access to the information contained in the CIR, but only to a reply indicating which underlying data base contains matching data. Full access to the data contained in EU information systems for the purposes of preventing, detecting and

[9] C-293/12 and C-594/12

investigating terrorist offences or other serious criminal offences would remain subject to the conditions and procedures laid down in the respective legislative instruments governing such access.

Concretely, as a first step, a law enforcement officer would launch a query on a specific person using the person's identity data, travel document or biometric data to check whether information on the searched person is stored in the CIR. Where such data is present, the officer will receive a reply indicating which EU information system(s) contains data on this person (the hit-flag). Only as a second step would the officer individually request access to each system that has been indicated as containing data, in order to obtain the complete file on the queried person, in line with the access rules and procedures laid down in the respective legal instruments setting up each system concerned.

The Working Party first would like to underline that the so-called "hit-flag" indicating that data on a person are stored in the CIR, constitutes in itself a personal data, and the fact that police authorities will only have access to a partial information (in the form of a "hit-flag") when querying the CIR cannot be considered as a sufficient safeguard in itself. Furthermore, the Working Party recalls that the ECJ already underlined that "to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way"[10]. The mere access right granted by the proposals to the information that personal data are stored in the CIR thus constitutes an additional interference with the fundamental rights of data subjects whose data are stored in the CIR.

Indeed, either the CIR has to be considered as a distinct, EU-centralised database, with specific purposes (which could be implied by the impact assessment when stating "*the data contained in the CIR can either be accessed for the purposes provided for in each of the existing legal bases of the underlying systems or for the purposes of the CIR, namely the facilitation of identity checks and the detection of multiple identities*") and access rights, or this data base is to be considered as intrinsically linked to the underlying databases, with a replication of the access rights foreseen in the respective legislative instruments. As the proposals themselves seem to reflect that the second option has been elected, the same access rights governing the access to the EU information systems should be foreseen to access the CIR.

The Working Party therefore recommends that the possibility to query the CIR granted to designated authorities would be strictly restricted to the situations where these

[10] Judgment of the Court (Grand Chamber), 8 April 2014 - Digital Rights Ireland - Joined Cases C-293/12 and C-594/12. - Par. 33

authorities would have the right to access all the underlying data, or that “hit flag” would be communicated only with regard to underlying data bases to which these designated authorities would have a direct access.

Should access to the CIR for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences, even in the form of a hit/no hit procedure, remain in the proposals to be adopted, the WP29 would strongly recommend to at least introduce or keep existing procedural safeguards prior to the second step access.

IV. Data protection regime

In addition to the specific chapters and provisions for each new data base (CIR, sBMS and MID), chapter VII is dedicated to data protection. It includes provisions on the respective data controllers, processor, security requirements, rights of the individuals, communication of personal data to third countries, international organisations and private parties, supervision of data processing activities and on cooperation between national supervisory authorities and the European Data Protection Supervisor.

However, despite what could be expected from a rapid reading of the provisions, the combination of all these provisions do not provide a clear view of the applicable data protection regimes and several aspects remain to be further specified, at least, if not to be provided at all.

Article 40 “Data controller” and Article 41 “Processor” should allocate the different responsibilities concerning each new data processing (CIR, sBMS and MID).

However, Article 40 merely indicates that Member States competent authorities that are controllers for the underlying data bases shall also be considered as controllers of the new EU data bases supplied with the data emanating from these underlying databases in accordance with Article 4(7) of Regulation 2016/679. In addition the European Border and Coast Guard Agency shall be considered a data controller in relation to the processing of data in the MID, in accordance with Article 2(b) of Regulation 45/2001, in addition to the Member States authorities adding or modifying the data in the identity confirmation file.

Article 41 concisely states that in relation to the processing of personal data in the CIR, eu-LISA is to be considered the data processor.

Consequently, although three new EU databases are created by these two proposals, Article 40 suggests that controllers for these new data bases will be the controllers of the underlying databases, while suggesting that Regulation 2016/679 will apply to the

new EU processing, without any mention of Directive 2016/680, while article 22 provide for additional access rights for purposes within the scope of this Directive. The latter also derives from Article 49 which refers to the supervisory authority or authorities designated pursuant to Article 49 of Regulation 2016/679. Article 41 *a contrario* implies that there is no processor for the sBMS and the MID.

This proposed allocation of responsibilities relies on the assertion that Member States competent authorities that are controllers for the underlying data processing, in particular for the SIS and for the future ECRIS-TCN system, will be considered as controllers in accordance with Article 4(7) of Regulation 2016/679 in relation to the processing of data in the context of the CIR, the sBMS and the MID.

Even if this assumption that only controllers for the underlying data bases are controllers for the new data bases created by the proposals were to be accepted, this architecture raises several concerns. First, it does not clearly indicate whether all the competent authorities (both within the same Member State for all the respective controllers of the underlying data processing systems concerned, as well as at EU level all the relevant competent authorities altogether) are to be considered as joint controllers, in accordance with Article 26 of Regulation 2016/670 in relation to the processing of data within the CIR, the sBMS and the MID. Indeed, Article 26 of the GDPR foresees that "where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers".

If the intended structure is to keep the same partition of responsibilities within the three new EU data bases, as in the underlying data processing, this should be clearly stated, including in Article 7 concerning the access rights of competent authorities via the ESP.

In addition, the status of euLISA should also be clarified. It is expressly designated as processor only in the context of the CIR within Articles 41. However, at the same time, Articles 53 of the proposals dedicated to euLISA's responsibilities following the entry into operations, also entrust this agency with for instance the technical management of the central infrastructure, with the responsibility for the national uniform interfaces, as well as with the technical management of the communication infrastructure, in cooperation with the Member States of all interoperability components. For all these activities and the others listed in Articles 52 and 53 the responsibility of the Member State's controllers towards euLISA when fulfilling these tasks should also be clarified.

To sum up, the proposals should either foresee a strict separation of controllership more clearly or expressly lay down a joint controllership for EU data bases, in which case, the procedure to take decisions as to the processing and to give instructions to the processor(s) should be further detailed.

Furthermore, article 47 on the right of access, correction and erasure, should also be amended. In its current drafting it blurs the respective responsibilities of controllers by foreseeing that since any person should be able to address him or herself to any

Member State, the Member State to which the request has been made, even where it will not be the Member State responsible, will be able to delete data from the CIR. Although this possibility could appear as a facilitation for the data subjects' exercise of their rights, this possibility granted to any requested Member State to delete data in the MID has two consequences: in terms of responsibility, this would plead for a joint-controllership status of all authorities as regards the MID. This would also imply, in accordance with paragraph 9 of Article 47, that while exercising their tasks, the competent data protection national supervisory authorities could either:

- be in a position to control the competent authorities of another Member State, and thus to exercise their powers on the territory of another Member State (by derogation from what Regulation 2016/679 and Directive 2016/680 provide);

- or would be limited in the exercise of their tasks to the sole actions taken by the authority of its Member State.

Therefore, the Working Party 29 suggests to clarify that only the responsible Member State should be responsible for correcting or amending the data in the MID, either following a direct request of the data subjects, or following the transmission of a request by a Member State to which the request will have been made. This solution would allow to both preserve a clear allocation of responsibilities between competent Member States authorities and their respective data protection authorities, and an effective and facilitated avenue for data subjects to exercise their rights.

V. Coordination of the supervision

In its previous statement concerning the revision of Regulation 45/2001, the working party 29 has already stressed that a coordinated supervision model which foresees the equal participation of the EDPS and of the national DPAs, according to their respective competences, should absolutely be preserved. It also underlined that the EDPB should be a forum where all supervisory authorities (national + EDPS) would coordinate themselves and act as much as possible on an equal footage. This is the current wording of Recital 65 of the revised Regulation 45/2001 ("*The European Data Protection Board should serve as a single forum for ensuring the effective coordinated supervision across the Board*").

In the context of these two proposals where new EU databases will be fed by the underlying databases, for which national supervisory authorities will remain competent, and where an express reference is made to Article 62 of the revised Regulation 45/2001, the WP29 recalls its position to place the coordination of the supervision under the forum of the EDPB. Indeed, the creation of new EU databases and information systems all the more justify the necessity to define a new coordinated supervision model along the lines previously suggested by the Working Party 29.

Consequently, evaluation reports, such as the report foreseen under Article 37 on the quality of data should also be transmitted to the EDPB.

VI. Specific safeguards for children, the elderly and persons with a disability

Article 5 of the proposals deals with the "non-discrimination" principle. It notably includes a reference to the particular attention which should be paid to children, the elderly and persons with a disability.

Even though this reference is welcome, it does not appear to grant the level of protection afforded in other instruments to these specific categories of persons. Indeed, to effectively ensure non-discrimination of these persons, other instruments of EU Law expressly foresee that specific safeguards should be adduced.

For instance, Regulation 2017/2226 establishing an Entry/Exit System (EES) mentions the specific safeguards to be foreseen for children[11] and Regulation 2252/2204 on standards for security features and biometrics in passports and travel documents issued by Member States[12] also foresees that children under 12 and persons where fingerprinting is physically impossible are exempted from the obligation to provide their fingerprints. These specific safeguards are designed to ensure that children, whose biometric data are not as reliable as adult's, or persons deprived from the capacity of providing these data, do not suffer adverse consequences based only on this „physical" ground.

The Working Party also underlined previously that "*fall back procedures should be available to constitute essential safeguards for the introduction of biometrics as they are neither accessible to all nor completely accurate. Such procedures should be implemented and used in order to respect the dignity of persons who could not follow successfully the enrolment process and to avoid transferring onto them the burden of the system imperfections."*[13]

In the context of its evaluation of the ETIAS proposal, the Fundamental Rights Agency as well underlined the concept of the "best interests of the child" (protected both by Article 3 of the UN Convention on the Rights of the Child and by Article 24 of the

[11] See article 10(2)

[12] in Article 1 (as modified by Regulation 444/2009)

[13] See previous opinion 1710/05/EN WP 112

Charter of Fundamental Rights) and the need to provide for specific safeguards of children's personal data[14].

The ECtHR also underlined the need to provide for an increased protection of minors' data. It notably provided that the retention of the unconvicted persons' data may be especially harmful in the case of minors, given their special situation and the importance of their development and integration in society and that particular attention should be paid to the protection of juveniles from any detriment that may result from the retention by the authorities of their private data following acquittals of a criminal offence[15].

Consequently, in the context of the two proposals on interoperability, specific safeguards should also be introduced to ensure that the data of children, the elderly and persons with a disability also benefit from a specific additional protection in the context of the CIR, sBMS and MID databases. This could for instance entail a specific mention that their biometric data were not taken, or that given their age these data are not entirely reliable, due to their specific situation, to protect them against any decision which would produce legal effects concerning them or similarly significantly affect them and which would be based solely on these biometric data or on their absence.

VII. Data retention and keeping of logs

The proposals foresee that in principle, the data stored in the CIR will be deleted in accordance with the data retention provisions of the underlying instruments (Article 23, 1)), that data in the sBMS shall be stored for as long as the corresponding biometric data is stored in the CIR or the SIS (article 15), and that data will be stored in the MID only for as long as the linked data is stored in two or more EU information systems (article 35). The retention periods of data in the three new EU data bases therefore appear directly linked one to another, and in principle ultimately to depend on the retention period foreseen in the underlying data bases given the reference made in Article 23, 1). On this aspect, the Working Party recalls that it already underlined the necessity to advance stronger justifications for the retention periods foreseen in the underlying instruments[16].

[14] Opinion 2/2017 of the Fundamental Rights Agency on the impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS) – pages 17 and 18

[15] ECtHR, No. 30562/04 and 30566/04, Marper v. UK, 4 December 2008, para. 124.

[16] For the last position on this aspect, see for instance the Appendix annexed to the letter of the Chair of WP29 sent to the Commission on proposal for establishing a European Travel Information and Authorisation System (ETIAS).

In addition, in the context of the two new proposals on interoperability, Article 23, 2) provides that the individual file (meaning the data originating from the underlying information systems and white or red links created by the MID, as it follows from Article 19, 2)) shall be stored in the CIR for as long as the corresponding data is stored in at least one the information systems whose data is contained in the CIR. Although it is also foreseen that the creation of a link shall not affect the retention period of each item of the linked data, this provision actually seem to result in a longer period of retention of the data. Indeed, if the red or white link stored in the CIR contains in itself the mention that it was created on the basis of a data which originated from an underlying system where the data has been erase in accordance with the retention period foreseen in this context, this amounts to retaining the data for a longer period in the CIR.

As regards the keeping of logs, the drafting proposed in articles 10, 16 and 24 aim at framing the purposes for which logs may be used, as well as the retention period for these logs. The Working Party welcomes the objective of these provisions. However, their drafting could be slightly amended with a view to aligning them more with what is provided in Article 25 of Directive 2016/680, in order to exhaustively list for which purposes logs shall be used and to clarify that competent supervisory authorities should also be able to be given access to the logs in order to perform their tasks and assess the lawfulness of the processing. The drafting should also be complemented as regards the retention period of logs as the one-year period foreseen seems useful and justified, but could be prolonged without any deadline for the erasure of the logs in case of ongoing monitoring procedures.

VIII. Data Security

The proposals foresee the creation of three EU centralised databases, as well as the creation of the ESP search engine to access the interoperable underlying databases. Articles 42 therefore provide for the requirements in terms of security of processing and entrust euLISA and the Member States with the responsibility to ensure the security of the processing of personal data taking place pursuant to these regulations. However, only euLISA is expressly entrusted with a list of measures to be adopted, while Member States authorities shall take measures equivalent as regards security in respect of the processing of personal data by the authorities having a right to access any of the interoperable components.

In practice, centralizing data heightens the risks for the data subjects in case of unlawful access and use and therefore requires an increased level of security, in particular for sensitive data such as biometric data.

As previously underlined by the Working Party[17], “any central database would increase the risks of misuse and misappropriation. It would also intensify the dangers of abuse and function creep. Finally, it would raise the possibilities of using biometric identifiers as 'access keys' to various databases, thereby interconnecting data sets.”

The Working Party therefore recalls the need to provide for appropriate security measures, as well as to clearly allocate responsibilities for implementing these measures and notifying security data breaches and incidents. In this regard, Articles 44 of the proposals do not appear to sufficiently fulfill this requirement. Indeed, for instance, while Member States shall notify the Commission, euLISA and the EDPS, in reverse, euLISA would not have to notify the Member States of security incidents in relation to the central infrastructure, whereas they are presented as controllers.

IV. Conclusion

In the view of the WP29, the proposals on interoperability are not limited to complementing existing and future EU centralized data bases with additional cross-matching functions. In fact, they aim at building a new system architecture with no less than three additional data bases.

Regrettably, **the impact assessments** accompanying the proposals fail to provide a detailed analysis on certain data protection aspects. In particular, it does not offer further explanation as to the applicable data protection regime for different operations and it does not evaluate the sufficiency of security measures. In addition, no analysis is provided with regard to less intrusive means and alternative solutions to reach the intended goals, which could substantiate and justify the solutions chosen.

As regards the necessity of **the European Search Portal (ESP)**, the WP29 is of the view that the justification advanced concerning the facilitation of the technical and operational implementation by Member States of existing and future new information systems cannot be considered as an acceptable demonstration of the necessity of this tool. In addition, although the ESP may not be sufficient in itself to establish a more or less detailed profile of the data subject concerned, it is important to ensure that - in particular when additional functions or additional access rights than the existing ones are envisaged -, the establishment of a European Search Portal does not lead to any additional interference with the rights to privacy and data protection.

Regarding **the Common Identity Repository (CIR)**, the WP29 is of the view that the cross-matching of various sources for identification and consolidating them in a new

[17] See previous opinion 1710/05/EN WP 112

common data base for the purpose of overall identification poses an additional interference with the rights to privacy and data protection. The WP29 is not convinced of the necessity and proportionality to establish such a mixed-purpose identification database including biometric data. Whether identity fraud is in practice such an essential threat to the internal security of the Union as to justify the central registering of biometric identifiers of all bona fide TCN travelers, migrants and asylum seekers is not yet sufficiently established in terms of proportionality and therefore remain an issue of major concern.

Even if such a common identity register for all the different purposes of the linked data bases was justifiable, the WP29 underlines that it is nevertheless highly doubtful whether it may be used for other purposes than those of the underlying data bases.In this perspective, the necessity and proportionality of Art. 20 allowing the national legislators to provide **access rights to police officers for overall identity checks** remains doubtful. The precise conditions, procedures and criteria for those checks are supposed to be described by the national legislators. The WP 29 stresses that this may result in a broad and common use of data, formerly held for quite restricted purposes and needs, while additional reasons and safeguards to justify such additional purposes are not sufficiently foreseen.

Regarding the **"hit/no hit" procedure** for law enforcement access in the context of combating terrorism and other serious crime, the WP29 wishes to stress that the so-called "hit flag" constitutes in itself a personal data and the fact that the access to a partial information by the authorities querying the CIR cannot be considered a safeguard in itself. Even considering that such partial access to information was justifiable, it is essential to keep certain thresholds and procedural safeguards for the second step which would be the access to the data stored in the different source data bases.

Concerning the **applicable data protection regime**, in the view of the WP29 the proposals should either foresee a strict separation of controllership more clearly or expressly lay down a joint controllership for EU data bases, in which case, the procedure to take decisions as to the processing and to give instructions to the processor(s) should be further detailed. The Working Party 29 also suggests to clarify that only the responsible Member State should be responsible for correcting or amending the data in the MID, either following a direct request of the data subjects, or following the transmission of a request by a Member State to which the request will have been made.

With a view to **coordination of supervision**, the WP29 underlines that the EDPB should be a forum where all supervisory authorities (national and EDPS) would coordinate themselves and act as much as possible on an equal footage. Indeed, the

creation of new EU databases and information systems all the more justify the necessity to define a new and strong coordinated supervision model.

Furthermore, in the context of the two proposals on interoperability, **specific safeguards** should also be introduced to ensure that **the data of children, the elderly and persons with a disability** also benefit from a specific additional protection in the context of the CIR, sBMS and MID databases.

Regarding **retention periods**, the WP29 recalls that it already underlined the necessity to advance stronger justifications for the retention periods foreseen in the underlying instruments. The Working Party is concerned that the system of links might lead to an even longer retention period, when a red or white link contains in itself the mention that it was created on data which originated from an underlying system where the data has already been erased in accordance with the respective retention period.

The provisions on **logging** should be aligned with Article 25 of the Directive 2016/680 in order to exclusively list for which purposes logs may be used and to clarify that the competent data protection supervision authorities should be given access to perform their tasks in assessing the lawfulness of processing.

In terms of **data security**, centralizing data heightens the risks for the data subjects in case of unlawful access and use and therefore requires an increased level of security, in particular for sensitive data such as biometric data. Therefore, the WP recalls the need to provide for appropriate security measures as well as to clearly allocate the responsibilities for implementing such measures.

Considering the number of concerns expressed, the Working Party recommends that an analysis of less intrusive means to reach the goals set in these proposals has to be provided to justify the choices made and ensure the respect of the purpose, necessity and proportionality principles, and that the proposals be substantially amended in the course of negotiations with the co-legislators in order to provide for stronger data protection safeguards and enhanced legal certainty as to the functioning of the new data bases which are intended to be created.