From:	European Data Protection Supervisor [redacted]
To:	VAUTMANS Hilde <hilde.vautmans@europarl.europa.eu>; SANTOS Isabel <isabel.santos@europarl.europa.eu>; BRICMONT Saskia <saskia.bricmont@europarl.europa.eu>; BJORK Malin <malin.bjork@europarl.europa.eu>
Sent at:	15/07/22 07:46:50
Subject:	2022-0514 D1736 EDPS Replies to the additional questions on data protection in the Proposal for a recast of Eurodac Regulation

Dear Members of the European Parliament,

Please find herewith attached a letter and its annex, signed by Mr Wiewiórowski on the above-mentioned subject.

Yours sincerely,

EDPS Secretariat

| Tel. (+32) 2 283 17 13 | Fax (+32) 2 283 19 50 | ›
Email edps@edps.europa.eu
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
@EU_EDPS www.edps.europa.eu

EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
SUPERVISOR

Ms Isabel Santos, S&D Group
Ms Hilde Vautmans, Renew Europe
Ms Saskia Bricmont, The Greens/EFA Group
Ms Malin Björk, The Left

Brussels, 14 July 2022

WRW/AP/asj/ D(2022)1736 - **C 2022-0514**
Please use edps@edps.europa.eu for all correspondence

Subject: EDPS replies to the additional questions on data protection in the Proposal for a recast of Eurodac Regulation

Dear Members of the European Parliament,

I am writing in response to your letter of 25 January 2022 concerning the amended Proposal for a recast of Eurodac Regulation.

The EDPS has consistently stressed that the fundamental rights enshrined in the EU Charter of Fundamental Rights, are universal and do not depend on citizenship or migration status. Therefore, the EU law in the field of asylum and migration must ensure full respect to the fundamental rights of all individuals, including their right to data protection and privacy. This position is reflected in the EDPS Strategy 2020-2024 and underpins our Opinions in this field, including Opinion 9/2020 on the new Pact on Migration and Asylum and Opinion 7/2016 on the CEAS reform.

In this regard, the EDPS replies to your specific questions in the Annex to this letter should be considered in the context of the above-mentioned Opinions issued pursuant to Regulation (EU) 2018/1725.

I look forward to continuing our fruitful cooperation aimed at ensuring full compliance of the EU legislation in the area of freedom, security and justice with the EU Charter of Fundamental Rights, and in particular with the rights to data protection and privacy.

Yours sincerely,

[e-signed]
Wojciech Rafał WIEWIÓROWSKI

Encl.: Annex with the EDPS replies to the questions on the amended Proposal for a recast of Eurodac Regulation

ANNEX

EDPS replies to the additional questions on data protection in the Proposal for a recast of Eurodac Regulation

Questions concerning the establishment of a security flag

1. *Does the EDPS have any concerns about the creation of a security flag in Eurodac, bearing in mind that - according to the Commission's proposal for both Eurodac and Screening - the data subject will not be informed of the creation of such a flag?*
2. *How does the security flag rhyme with the fundamental principle of Rule of Law, that anyone is innocent until proven guilty?*
3. *Does the EDPS find the establishment of the concept of a security flag in Eurodac necessary and proportionate in the light of other existing and future tools available through EU large-scale IT systems for flagging security concerns, most notably SIS and ECRIS-TCN?*
4. *According to the proposal for the screening regulation (2020/0278 (COD)), it is foreseen that the security check leading to the security flag in Eurodac is carried out by the "competent authorities" in the respective Member State. Does the EDPS find this role as data processor sufficiently well defined, also in light of the sensitive personal data that the competent authorities shall be given access to?*

In response to your first question, the EDPS indeed expresses its particular concerns regarding the introduction of a security flag in Eurodac, in addition to the already stored information on third country nationals ('TCNs') and stateless persons. The main concerns of the EDPS revolve around the question of whether such a flag is necessary or proportionate in the first place, in light of the already existing and foreseen security procedures. In addition, the EDPS is also concerned on the way this flag is currently proposed to be implemented.

The EDPS notes that a new field would be created for the mark where, following the screening in Article 11 of the Proposed Screening Regulation or the examination referred to in Article 8(4) of the proposed Asylum and Migration Management Regulation ('AMMR'), it appears that the person could pose a threat to internal security. Persons with such a flag could be excluded from relocation in conformity with the rules in the Regulation on Asylum and Migration Management. Furthermore, for the applicants for international protection for whom a security problem has been flagged and marked in Eurodac, assessors are required to focus first on whether this flag may amount to an exclusion/rejection ground.

These far-reaching implications of a security flag in Eurodac are not accompanied by details in the legislative proposals on how and which criteria may be used to determine a security threat. Checks will be made against EU databases but also against national ones, adding the issue of lack of harmonisation and uneven/arbitrary labelling of someone as a security risk. This comes despite the heavy consequences of e.g. a denial of relocation procedure, which may

effectively deny a third country national or stateless person the opportunity to live in a country reflecting their family links, language skills, and cultural or social ties.

When considering the necessity and proportionality of the security flags, it should be kept in mind that, according to the Proposal for a Screening Regulation, a debriefing form is the issued at the end of the screening, which should contain information to be used for both the referral procedure and the subsequent procedures. This undermines the 'necessity' argument advanced for the security flag in Eurodac in order to facilitate the implementation of relocation and/or evaluation of an application for international protection, as set out in the explanatory memorandum attached to the Eurodac proposal. It would appear that the security flag would reflect information already included in the debriefing form.

The EDPS has already stressed in his Opinion 9/2020 that the decision on whether an individual constitutes a risk must be based on accurate and reliable data. In this regard, the EDPS wishes to highlight that there is a difference in impact between carrying out a one-off search across databases to check whether an individual constitutes a security risk (such as in the case of EES) and the inclusion of a long-lasting security flag in Eurodac. In fact, the latter represents the outcome of an assessment, which introduces an additional level of possible arbitrariness. Moreover, such assessment is carried out on individuals who, importantly, can occupy a position of specific vulnerability. Where the person entering the security flag is not the same person carrying out the assessment of a subsequent asylum claim, the second person may not be in a position to verify how strongly the security flag should be weighed against other aspects when carrying out the assessment of a claim.

Regarding checks against EU databases such as SIS II, the amended Proposal for a Eurodac Regulation requires authorities to check whether information on an individual person, including on security, is recorded in any of the relevant EU databases, as well as Interpol's SLTD or TDAWN, and then to introduce a security flag based on the same information obtained from the search. Therefore the security flag would risk duplicating information that is already included in other databases, which carries well-known data protection risks. For instance, the record in the underlining database may be deleted but the security flag related to that record may still remain in Eurodac.

With the adoption of the interoperability framework, Eurodac will also become part of an integrated information network with all the other large-scale EU information systems in the area of freedom, security and justice: SIS II, VIS, the Entry/Exit System, ETIAS, and ECRIS-TCN. Interoperability will make it very complex for individuals to access and rectify any potentially erroneous personal data.

The lack of information towards the data subject (including on possible legal remedies) against the issuing of proposed security flag raise additional concerns. Transparency of the processing vis-a-vis the TCN or stateless person is an essential safeguard and a prerequisite and enabler for the exercise of the other data subject rights. In this regard, the EDPS has already stressed that the right to rectify and/or supplement their personal data by the third-country nationals

and the accuracy of the information processed during the (security) screening is of paramount importance.

The EDPS notes that the legal acts establishing the consulted EU databases, such as SIS, VIS and others, provide for notification obligations in case of an alert or hit (e.g. Article 52 of Regulation (EU) 2018/1861 (SIS-Borders Regulation)). However, exceptionally the transparency could be subject to "partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the person concerned" (see e.g. Article 38 (7) of Regulation (EU) 2021/1134 (revised VIS Regulation)). The EDPS notes however that this exceptional regime may be the norm for Eurodac.

Finally, with regard to the conditions of access, the definition of "competent authorities" raises issues with regard to the type of national entities that qualify as a competent authority for the purpose of the Eurodac Regulation. The EDPS already raised this issue in the context of the VIS Regulation (cfr EDPS Opinion OJ C 181/13, 23.7.2005). Indeed, such definition leaves a large amount of discretion to the Member States to designate which bodies should have access.

In this regard, the EDPS made specific recommendation about its practical implementation in the context of the amended Proposal for a Eurodac Regulation, i.e. the staff of the Member States and the Union authorities should only see the data that is relevant for the performance of their specific tasks, even if the data sets are linked in a sequence ('need to know'). The same applies to the security flag.

Questions concerning Search and Rescue Operations

1. *How does the EDPS assess the creation of a separate category of irregular arrivals following Search and Rescue Operations in Eurodac from a data protection point of view?*

Persons disembarked following a search and rescue operations are currently registered in Eurodac under the category of persons apprehended in connection with an irregular crossing of the external border. Any differentiation between the data processing of search and rescue TCNs/stateless persons and those apprehended irregularly crossing the border should reflect a practical difference and necessity to justify it, in order not to create arbitrary provisions applying to SAR TCNs or stateless persons.

Questions concerning the access by Europol, Frontex and EUAA:

1. *How does the EDPS assess the access of "authorised users of the relevant Justice and Home Affairs Union Agencies, in particular the EUAA, the EBCGA and Europol, if such access is relevant for the implementation of their tasks"? Does the criteria of relevance render the decision making progress too arbitrary? Does the EDPS have any concerns specifically about Europol's access?*

2. *The Eurodac Rapporteur proposes to ask European Border and Coast Guard Agency and the European Union Agency for Asylum to work together with eu-LISA to develop a "technical solution" to ensure direct access for those agencies to Eurodac. How does the EDPS assess such a suggestion? Does the EDPS foresee any data protection risks from granting direct access to EU Agencies to Eurodac, as opposed to access through national access points, particularly from the point of view of determining the data controller?*
3. *Does the EDPS deem a logging mechanism for the technical interface solution alone sufficient to ensure "the lawfulness of data processing and compliance with data protection requirements", or should other safeguards complement the logging mechanism to ensure a high standard of 'privacy by design'?*

The access by law enforcement authorities to non-law enforcement systems should always be justified and satisfy the requirements of necessity and proportionality, as laid down in Article 52(1) of the Charter.

(1) Access to statistics

The EDPS however notes that the access in question ("*authorised users of the relevant Justice and Home Affairs Union Agencies, in particular the EUAA, the EBCGA and Europol, if such access is relevant for the implementation of their tasks*") relates to Article 9 'Statistics' of the Proposal for recast of Eurodac Regulation and the information in the Central Repository for Reporting and Statistics (CRRS) referred to in Article 39 of Regulation (EU) 2019/818. While in his Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability the EDPS has expressed concerns about the establishment of the CRRS, in this context he would like nevertheless to recall the fact that the CRRS contains only anonymous data (see Article 39 (3) of Regulation (EU) 2019/818).

At the same time, as pointed out by the EDPS in his Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability, the data stored in the CRRS may nevertheless lead to the identification of individuals in certain cases. Therefore the EDPS recommends limiting access to the CRRS to what is necessary in the light of specific objectives.

As to proposals for the addition made by the Eurodac rapporteur to significantly change the proposal, including by proposing the creation of new infrastructure elements, the EDPS notes that these changes are introduced after the legislative opinion of the EDPS was issued. Furthermore, the EDPS does not have sufficient information about the suggested amendments in order to assess their necessity and proportionality.

(2) Logging

Logging of processing operations such as collection, alteration, consultation, disclosure including transfers, combination and erasure, is an important safeguard for verification of the lawfulness of the processing, both internally (i.e. self-monitoring) and by external supervisory authorities such as the data protection authorities. It also helps ensuring data integrity and data security. This mechanism ensures that users follow all agreed procedures and also assist

in preventing and tracking potential misuses. In that respect the management of logs is an important factor that relates with the secure storage of logs, the access and frequent review of the logs, the enforcement of alerts in case of suspicious processing and the duration of their storage. These elements are important to ensure that the logging mechanism provides its benefits. However, logging is just one of many tools for accountability and supervision, which complement and reinforce each other, e.g. data protection by design and by default, cyber security, training of staff, etc.

Questions regarding Interoperability

1. *The Eurodac Rapporteur proposes to allow the creation of a linked dataset in the EU large-scale IT systems on the basis of a hit obtained against a facial image alone. Does the EDPS have any concerns about the use of only a facial image to create linked datasets for interoperability purposes?*
2. *In his Opinion 09/2020 on the new Pact on Migration and Asylum, the EDPS stressed that "[...] The proposals under the New Pact on Migration and Asylum further blur the distinction between the different policy areas of asylum, migration, police cooperation, internal security and criminal justice. This approach follows a trend already embedded in the interoperability framework [...]". Does the EDPS consider that the safeguards enshrined in the amended Eurodac proposal, and more in general in the EU interoperability-related legislative framework, are sufficient to avoid any disproportionate impact that such framework – and the related overlaps between policy areas - might have on individuals' fundamental rights? If not, which additional safeguards would EDPS preconize / which elements are problematic in that regard?*

(1) Facial images

Regarding facial images as a biometric identifier in Eurodac, in the 2016 Opinion the EDPS called for "[...] conducting or making available an assessment of the need to collect and use the facial images of the categories of persons addressed in the Eurodac recast Proposal and of the proportionality of their collection, relying on a consistent study or evidence-based approach". The EDPS notes that the latest Proposal foresees a study on the technical feasibility of adding facial recognition software to the Central System for the purposes of comparing facial images. The study will be carried out by eu-LISA and will evaluate the reliability and accuracy of the results produced from facial recognition software for the purposes of EURODAC. However, the EDPS observes that no data or evidence has been brought forward to justify the need to collect minors' facial images. Furthermore, and related to this point, the EDPS regrets that the foreseen study will focus only on the technical aspects and not on the necessity and proportionality of processing of facial images.

Indeed, it should be considered whether adding facial images to the fingerprint dataset by default, would lead to a necessary and substantial improvement of Eurodac that would warrant this collection of further sensitive biometric data from third country nationals and stateless persons.

(2) Interoperability

Interoperability should be viewed first and foremost as a political choice, not as a technological solution, due to its far-reaching legal and societal consequences.

Interoperability should not be an end in itself but should always serve a genuine public interest objective. Where the addition of facial images by default would (largely) not serve the main purpose of Eurodac, given the already existing fingerprints, but would rather be driven by a wish to enable interoperability, this changes the purpose of Eurodac itself.

The current interoperability legal system does provide for a number of legal and technical safeguards, for instance by preserving the specific use purposes of the interconnected information systems, ensuring the logical separation of the personal data collected in different information systems and stored in the common interoperability components, foreseeing access management rules and obligations to keep log files. At the same time, a number of elements of the interoperability framework require close scrutiny and strict safeguards, such as with regard to the accuracy of the personal data stored in the underlying databases or the data quality of the collected biometrics, both of which could lead to high level of false positive hits and result in severe consequences for vulnerable persons.

Data subjects (e.g. applicants for international protection) should be able to exercise their rights ideally simultaneously to all systems. There is a need to give further consideration to streamlining procedures for data subjects' rights within the interoperability framework so that individuals are not confronted with having to address multiple authorities and procedures to find out who is processing their data and to ascertain whether it is accurate.

It is very difficult at the moment to assess the actual impact of interoperability, including on the principle of purpose limitation, due to the complexity of the legal framework and the technical infrastructure, as well as the fact that some key elements and systems are still under development. In any case, the mere fact that the data has already been collected and available, should not permit its use for another purpose which may have a far-reaching negative impact on the lives of individuals.

Questions regarding minors:

1. *The Commission's proposal from 2016 proposes to lower the age from which biometric data is taken from children - from 14 to six. Does the EDPS find this suggested lowering of the age at which biometric data is taken necessary and proportionate to the aims of Eurodac? Is the EDPS aware of any evidence of the benefits or drawbacks of taking biometric data from children at such a young age?*

In the Explanatory Memorandum of the 2016 proposed Recast of the Eurodac Regulation, the European Commission indicated that by lowering the age for taking the fingerprints, the proposal aimed at protecting child victims of trafficking and support the identification and protection of unaccompanied children who go missing, disappear or abscond. The same objectives are indicated in the amended Proposal for a Eurodac Regulation.

The EDPS has previously provided his comments that, while the choice to include children's data was advocated for as a means to assist in locating missing children, establishing links with family members in other Member States or prevention of exploitation, none of these objectives features in the proposal (nor does it now in proposed amendments). As the EDPS has mentioned, this justification "is not convincing as such" and the mere fact that some Member States have adopted this practice does not mean that such a measure is efficient, proportionate or useful.

In the 2016 Opinion on CEAS, the EDPS therefore called for a detailed assessment of the situation of minors and a balance between the risks and harms of such procedure for the minors and the advantages that they can benefit. However, the EDPS is not aware of any such assessment being carried out so far.

Against this background and building on the 2016 Opinion, the EDPS reiterates the urgent need to carry out one or several multidisciplinary studies on the impact of such collection and processing. Such assessment should analyse all relevant aspects of the problem going beyond the technical elements[1] and also assess among others psychological, societal, fundamental rights aspects as well.

In addition, the EDPS has particular concerns regarding law enforcement access to the biometric data of minors. Given that the justification for the processing of this data is based on child protection necessity grounds, strict safeguards (such as the required involvement of child protection services) should be included to prevent law enforcement access for any other purpose.

As a positive note, the EDPS does see that additional safeguards have been integrated in the amended proposal at the level of collection (such as requiring the involvement of a trained official and in the presence of a responsible adult). However, these are auxiliary safeguards which are to be applied following the overarching necessity and proportionality assessment of the measure itself.

[1] On the technical side, the EDPS has recently published an overview document with the Spanish Data Protection Authority where it is concluded that, based to scientific evidence, the accuracy of some biometric data, like fingerprints, is dependent on the age of the individual and affected by the ageing of individuals. According recent study for children of ages 5-12 fingerprint quality is acceptable. https://edps.europa.eu/sites/default/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_auuthentication_en.pdf

Questions regarding the use of coercion

1. *In his opinion 07/2016 on the CEAS reform, the EDPS recommended, among others, "deleting the possibility to establish sanctions and penalties, including detention, in the context of the collection of biometrics, and to allow detention only when it is strictly limited to what is necessary for the identification of an individual" and "clarifying in a recital that in any event coercion cannot be used in order to obtain fingerprints of individuals". Does the EDPS consider that the current Eurodac provisional agreement, which the new amended Commission proposal builds on, is in line with such recommendations?*

The EDPS stands by his recommendation that the Union legislation should not provide for a legal possibility for sanctions and penalties, including detention, in the context of the collection of biometrics. Thus, the EDPS does not support the use of coercion in order to obtain fingerprints of individuals.

Questions regarding the 'data'-related definitions

1. *The Rapporteur wants to include this definition: "dataset" means the set of information recorded in Eurodac on the basis of Articles 12, 13, 14 or 14a, corresponding to one set of fingerprints of a data subject and composed of biometric data, alphanumeric data and, where available, a scanned colour copy of an identity or travel document.'; These datasets would be in a sequence linked to a person and also used for comparison, searches etc. The definition of "alphanumeric data" that stands in the current text (from the previous Eurodac proposal and the provisional agreement among Institutions) states: 'alphanumeric data' means data represented by letters, digits, special characters, space and punctuation marks; but at the time this would refer to a closed list of information relating to the identity of the person mostly.*
2. *However, with the updated proposal and also in view of the Screening Regulation and the provisions, relating to a form and an Annex with several information, therein, could then "alphanumeric data" mean much more than what was initially foreseen?*
3. *Does the EDPS consider that the use of the term "alphanumeric data" is appropriate, accurate and proportionate or could it be too broad?*
4. *As the content of the de-briefing form and the Annex of the screening may include a very wide range of information and no retention period seems to be defined, does the EDPS consider that these elements could/should be included in the dataset of a person?*
5. *In either case, are there any suggestions for safeguards?*

The EDPS notes that the term "alphanumeric data" is legally defined and used in a number of EU legal instruments, e.g. Article 4(11) of Regulation (EC) No 767/2008 (VIS Regulation), Article 4(7) of Regulation (EU) 2019/818 (Interoperability - police Regulation) and others.

At the same time, in the 2020 Opinion the EDPS highlighted that the information recorded in the de-briefing form may to a great extent determine the situation of the data subjects, including their procedural rights. Therefore, the EDPS stressed the crucial importance of the accuracy of the information and of the right of the third country national, subject to the screening, to rectify and/or supplement the personal data about him or her.

In this regard, the EDPS considers as particularly problematic the last point 16 'Comments and other relevant information' of the standard de-briefing form, provided for in the Annex to the Proposal for Screening Regulation. The EDPS recalls that the CJEU has already scrutinised the issue of the processing of data contained under a so-called 'free text' heading. In particular, in paragraphs 160 and 163 of the CJEU Opinion 1/15 on the draft Canada-EU PNR Agreement, the Court reached the conclusion that heading 17 'General remarks' "*does not set any limitation on the nature and scope of the information that could be set out thereunder. In those circumstances, heading [17] cannot be regarded as being delimited with sufficient clarity and precision*" and as a result "*do not delimit in a sufficiently clear and precise manner the scope of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter*". The EDPS believes that the same considerations apply, *mutatis mutandis*, to the collection and processing of personal data in the context of security screening of third-country national envisaged in the Proposal for a Screening Regulation.

In addition, the EDPS also recommended the future legislation to lay down a data retention period for the de-briefing form. In this regard, for instance, the legislator may choose either a fixed retention period, or to link the storage to the duration of the relevant asylum or migration procedure.