Meijers Committee
standing committee of experts on international immigration,
refugee and criminal law

CM2110 Note on the Eurodac amendment proposal (COM (2020) 614)

July 2021

1. Introduction

The Meijers Committee expresses its concerns about the proposed amendments of the new Eurodac proposal as presented by the European Commission as part of the New Migration and Asylum Pact in September 2020. This proposal includes the earlier proposal of 2016 and amendments of that proposal in the provisional agreement of June 2018 between the Council and the European Parliament.[1] The Meijers Committee is specifically concerned about (1) the fundamental rights impact of the immense extension of content and use of Eurodac, (2) the difficulty in understanding the full scope of the subsequent legislative proposals, and (3) the close connection with other legislative proposals which are still under negotiations or have not yet been implemented. The last two aspects hamper effective scrutiny of the proposal and its practical effects and human rights impact. The fact that the scope and impact of the Eurodac proposal are closely related to the proposed Screening Regulation and the new Regulation on Asylum and Migration Management but also the future implementation of the Interoperability Regulations of 2019[2], adds to the complexity of this proposal and does not allow to assess its necessity and proportionality fully.

This note will provide an overview of the most relevant amendments and then address this proposal's impact on data protection and other fundamental rights. Finally, we submit some recommendations for improvement.

2. Significant changes to the current use and impact of Eurodac

Eurodac as a multipurpose tool – part of the interoperability scheme

The 2020 proposal entails an overall significant change of Eurodac as currently provided in Regulation 603/2013. According to the Commission in the explanatory memorandum, this proposal "aims at transforming Eurodac into a common European database to support EU policies on asylum, resettlement and irregular migration". Widening the scope of searches to all categories of data, including biometric data, would allow to follow "a pattern of irregular and secondary movements" throughout the EU and establish a person's identity in the absence of identity documents.[3]

This widened scope of use and users of Eurodac will be multiplied by the interoperability scheme as adopted in 2019. The interoperability scheme makes Eurodac part of the integrated

[1] COM (2016) 272 final, 4.5.2016. The adoption of this amended proposal was put on hold due to difficulties reaching agreement on other legislative proposals and more in particular on the proposed Dublin IV Regulation. A provisional agreement of 19 June 2018 between the Council and the European Parliament has been published on 22 June 2021 at the Public Register of the European Parliament.
[2] Regulation 2019/817 and Regulation 2019/818 on the interoperability of EU large-scale databases adopted on 14 May 2019. *OJEU* L 135, 22.05.2019.
[3] Explanatory memorandum to 2016 proposal, COM (2016) 272, p. 13.

information network between existing and future large-scale EU information systems in the AFSJ and will allow national authorities to check whether information on an individual person is recorded in any of the EU databases (VIS, SIS II, Eurodac, the Entry/Exit System, ETIAS, and ECRIS-TCN).

The interoperability scheme will have a huge impact on the practical use of Eurodac for two reasons. First, the scope of the searches will be changed since they will be based on the use of fingerprints and facial images. Biometrics will be the main tool to facilitate the interoperability to the different databases and to check whether or not a person has been registered in one of these databases, with or without knowledge of the data subject. This integration of Eurodac into a general "opaque ecosystem of biometric data processing, profiling and automated decision-making" increases the future impact on an individual's right to data protection.[4] Second, and as already pointed out by the EDPS in 2018, the interoperability regulations create "more than the sum of its parts as its components ultimately contribute together to establish a central database of third-country nationals", including their biometric data and increase the number of authorities having access to Eurodac exponentially.[5]

New objectives of Eurodac

The previous (2016 and 2018) proposals added three new objectives to the original aim of Eurodac: curbing irregular immigration and secondary movements within the EU and the goal to assist the implementation of the resettlement framework rules. The 2020 proposal adds yet another four additional objectives:

- prevent Assisted Voluntary Return and Reintegration (AVRR) shopping,
- assist in the correct identification of third-country nationals under Article 20 of the Interoperability Regulations,
- support of the ETIAS objectives, and
- support of the Visa Information System (VIS) objectives.

The 2020 proposal extends the possibility to access Eurodac to ETIAS national units and competent visa authorities to realise the last two purposes. To address the issue of secondary movements, the Commission 2020 proposal allows eu-LISA to draw up statistics using data from Eurodac by counting applicants rather than applications. This amendment may prevent double counting and would allow for more reliable data on the number of secondary movements.[6]

[4] Bianca-Iona Marcu, *Eurodac: Biometrics, Facial Recognition, and the Fundamental Rights of Minors*, European Law Blog, 29 April 2021, https://europeanlawblog.eu/2021/04/29/eurodac-biometrics-facial-recognition-and-the-fundamental-rights-of-minors/#more-7650

[5] EDPS Opinion 4/2018 on the proposed regulations on interoperability, 16 April 2018, p. 11.

[6] See also Daniel Thym, *Secondary Movements: Overcoming the Lack of Trust among the Member States?*, European Migration Law Blog, 29 October 2021https://eumigrationlawblog.eu/secondary-movements-overcoming-the-lack-of-trust-among-the-member-states/

New categories of persons and lowering of age to six years

The new proposal adds two categories of persons to be stored in Eurodac. First, illegally staying third-country nationals or stateless persons, and second, third-country nationals disembarked following search and rescue (SAR) operations which apply for international protection from the pool of irregular border crossers. Instead of registering these persons as persons crossing external borders irregularly, this new category would be necessary, according to the Commission, because of the lack of official border checks for SAR arrivals and the difficulty to define the points of entry precisely. It would also "lead to a more accurate picture of the composition of migratory flows in the EU", which implies use for statistical purposes.[7]

The Eurodac proposal lowers the age of persons to be stored into Eurodac from 14 years to six years for all categories.[8] This means that Eurodac will contain information on very young children who do not have the ability or independent power to understand or decide upon the effects of their registration into Eurodac. One of the justifications for lowering the age to six years is the goal of tracing missing children. However, it is not further explained why this is necessary or why the current use of alerts on missing persons in SIS II and cooperation between national authorities is not functioning sufficiently to trace missing children.

New categories of personal data

Based on the 2016 proposal and as agreed in the 2018 provisional agreement, Eurodac will include personal information on third-country nationals, including surname and first name (including previously used names), facial image, age, date and place of birth, nationality, and where available type, number and scanned colour copies of travel and identity documents. The 2020 proposal adds even further categories of personal data which are related to the goals of the Migration and Asylum Pact:

- the indication whether an asylum application is rejected to "reinforce the link with return procedures",
- the fact that a person could pose an internal security threat following the screening procedure, and,
- where there are indications that a visa was issued to the applicant: the Member State which issued or extended the visa or on behalf of which the visa has been issued, and the visa application number,[9]
- the fact that a person has been denied international or subsidiary protection and has not been allowed to remain in the territory,

[7] COM (2020) 614, Explanatory memorandum, p. 12.
[8] Following the 2016 proposal and the 2018 agreement.
[9] The latter category would be necessary to assist member states which are bound by the Dublin Regulation, but not by the VIS Regulation.

- the fact that voluntary return and reintegration assistance based on the AVRR has been granted.[10]

Data retention periods – deletion of 'blocking' of data

During the negotiations on the provisional agreement of 2018, no agreement could be reached on the proposal to shorten the data retention period of 10 years for applicants of international protection and long-term resident third-country nationals.[11] Whereas in the 2016 proposal, the Commission proposed to block the accessibility of Eurodac data for law enforcement purposes three years after the applicants were granted international protection, this obligation has been deleted in the current proposal (on the basis of the provisional agreement). The 2020 proposal now regulates that marked data on beneficiaries of international protection stored in the Central System and the CIR will remain available for law enforcement purposes until such data are automatically erased after the maximum data retention period. As already proposed by the Commission in 2016, the data retention time limit for irregular border crossing migrants is extended from 18 months to 5 years. This five years-period will also apply to the new categories of disembarked persons and illegally staying migrants.

The obligation of prior erasure for persons who acquired Union citizenship is maintained but no longer applies for illegally staying third-country nationals or stateless persons that were granted a residence document or who left the EU territory. Their data will be marked until the end of the 5 years-retention period and will thus remain available for law enforcement purposes. [12] In accordance with the 2020 Commission proposal, the same provision applies to persons disembarked during a SAR operation who have been granted a residence permit.[13]

Expansion of law enforcement access

The 2020 proposal provides an "expansion of scope and simplification of law enforcement access to Eurodac".[14] This extension is provided by firstly deleting the obligation first to consult VIS and, secondly, by no longer restricting access to 'specific cases', but to 'specific cases including a specific person'. The formulation of this new provision is unclear and may lead to different implementation at the national level. It should be explicitly provided that this provision does not allow searches in Eurodac which are not related to specific cases but related to 'specific individuals'. Furthermore, the proposal states that searches "shall be carried out on the basis of biometric or alphanumeric data", which is a broader definition than

[10] In order to prevent 'AVRR shopping', according to the proposal.
[11] According to the provisional agreement of 19 June 2018 published on 22 June 2021 at the Public Register of the European Parliament.
[12] Article 19 (4) 2020 proposal.
[13] See Art. 14 b(3a) in connection with 14 (a) (2) 2020 proposal.
[14] This expansion is justified in the new proposed recital 22a in the provisional agreement, version Council doc. 6016/18, stating: 'A broader and simpler access of law enforcement authorities of the Member States to Eurodac may, while guaranteeing the full respect of the fundamental rights, enable Member States to use all existing tools to ensure that people live in an area of freedom, security and justice. '

the current provision "requests for comparison with Eurodac data shall be limited to searching with fingerprint data".

Whereas the 2016 proposal limited this power to "Member States asylum experts on behalf of EASO", the 2020 proposal provides that experts of asylum support teams of the EU Agency for Asylum, "including members of Agency's own staff", may collect and transmit biometrics. This means that staff members of both agencies will have the power to collect and transmit personal data and biometrics from asylum applicants and other third-country nationals.

Considering this wide use for searches in Eurodac, the proposal should include the obligation of prior review by a court or an independent body to assess which access for law enforcement purposes is strictly necessary, as defined by the CJEU in *Digital Rights Ireland*.

3. Data protection concerns and CJEU case-law

Necessity and proportionality

According to the CJEU in the aforementioned case *Digital Rights Ireland* and more recently in *Quadrature du Net*, the legislation must provide clear and precise rules governing the scope and application of the measure in question and impose minimum safeguards to satisfy the requirement of proportionality. This ensures that the persons whose personal data is affected have sufficient guarantees that their data will be effectively protected against the risk of abuse.[15] Such legislation must be legally binding under domestic law. It must particularly indicate under which circumstances and conditions a measure providing for processing such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is even more important where personal data is subjected to automated processing, particularly where there is a significant risk of unlawful access to that data. Such considerations apply especially where the protection of beneficiaries of international protection and children of six years and older are at stake, which is the case with Eurodac.

If adopted, the proposal will grant multiple users assigned to different tasks access to Eurodac. These tasks include asylum applications, visa and immigration procedures, expulsions, resettlement and humanitarian assistance, law enforcement and intelligence authorities. This results in an increased number of authorities with access to Eurodac and a high variation of national practices because of national differences. For example, a list produced by the Commission on the authorities having access to Eurodac for law enforcement purposes in accordance with Article 5 (2) Eurodac Regulation reveals important differences.[16] Furthermore, as we mentioned before, the number of Eurodac users will increase exponentially after implementing the interoperability regulations.

[15] C-511/18, C-512/18 and C-520/18, 6 October 2020, *La Quadrature du Net and Others*, points 132 and 166.

[16] The list of 105 p. 'EU EURODAC List of authorities 191016 Art 5.2 Eurodac Regulation', submitted by the European Commission after a FOIA request, establishes for example that some MS report only two or four 'designated authorities' (Austria, resp. Greece) and other MS between fifty and even more than 200 authorities having access to Eurodac (Belgium, France, Italy).

Legal transparency

Concerning the principle of legal transparency, it is also questionable whether the proposed rules on Eurodac meet the criteria as established by the CJEU. The extensive number of data processing instruments existing aside and partially in connection to Eurodac, each with its own set of data protection rules, combined with the complex relationship between the GDPR, the LED, and the new Regulations on interoperability, does not yield a transparent legal framework.[17] This complexity of rules makes it difficult for data subjects to understand which law applies and which state or organisation should be addressed regarding their rights to access, correction or deletion of data, and, finally, their right to effective judicial protection.[18]

Extensive time limits - withdrawal duty to 'block' data

Maintaining extensive data retention periods and the withdrawal of blocking data on beneficiaries of international protection for law enforcement purposes is problematic from the viewpoint of the data protection rights of data subjects and the principle of non-discrimination. The CJEU has repeatedly underlined on the basis of Article 7 and 8 CFR the obligation of the EU legislator to provide for sufficient conditions concerning data processing to ensure its necessity and proportionality.[19] These conditions include (1) explicit justification of data storage of an entire group of persons, (2) the availability of specific limits with regard to authorities having access to data and their subsequent use, (3) prior review by a court or an independent body to assess whether access for law enforcement purposes is strictly necessary and (4) available time limits, restricting the storage of data to what is strictly necessary. As the current proposal does not include any of these safeguards, the Meijers Committee recommends adding further amendments to ensure the protection of data subjects in accordance with EU law, including shorter data retention limits and reinstatement of the obligation to block data.

The Meijers Committee notes that in *H.K. v Prokuratuur*, the CJEU defined the requirements for prior review on access to data for the purpose of law enforcement, including that the court or body entrusted with that review must have all the powers and provide all the guarantees necessary to reconcile the various interests and rights at issue.[20] Regarding a criminal investigation, the court or independent body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned. Where such a review is carried out not by a court but by an independent administrative body, that body must be able to act objectively and impartially when carrying out its duties. It must, for that purpose, be free from any external influence. This means that Member States must ensure the independence of supervisory authorities. It must also ensure that these authorities have sufficient means and

[17] This blurring of legal rules and responsibilities with regard to the use (including law enforcement use) of EU's large-scale databases and the effects of interoperability has been addressed by not only EDPS and FRA, but also many commentators: see for example Special issue on interoperability *European Public Law* 26, no. 1, 2020, p. 71-92.
[18] See also EDPS addressing this problem within the context of the interoperability legislation, Opinion 4/2018, p. 4 and 10.
[19] See specifically CJEU 8 April 2014 C-293/12, *Digital Rights Ireland*, points 56-66.
[20] C-746/18 2 March 2021 *H.K. v Prokuratuur* points 52-53.

powers for their tasks. Only monitoring capacities and no power to issue binding decisions are not sufficient in this regard.

4. Other Fundamental Rights

Human dignity and the protection of children

In earlier comments, both FRA and EDPS discouraged the use of coercion with regard to asylum seekers who often may be in a vulnerable position and/or traumatised.[21] However, the proposal maintains the already existing obligation of Member States to promptly take fingerprints and facial images from asylum seekers and irregular migrants crossing the external borders. It even extends this obligation to new categories of persons as described above, including children from 6 years and above.[22] In the 2018 provisional agreement, the European Parliament accepted the possibility for national authorities "to use a proportionate degree of coercion at last resort to ensure the compliance of minors with the obligation to provide biometric data".[23]

To accept the use of force against minors and the lack of clear criteria to protect the rights and well-being of children not only runs contradicts the FRA and the EDPS recommendations but also increases the risk of violation of children's rights as protected in 24 CFR and Articles 3 (protection of the best interests of the child) and 22 (protection of children seeking refugee status) of the UN Convention on the Rights of the Child. The EU legislator must regulate in the Eurodac Regulation that any use of coercion against minors, including detention measures as a sanction for not cooperating with the collection of fingerprints, is prohibited.

Furthermore, the Meijers Committee notes the lack of evidence substantiating the necessity or added value of lowering the age to six years. Problems regarding tracing missing children will not be solved by the general and indiscriminate storage of personal information of every minor of six years and older in Eurodac. Instead, the EU legislator and the Commission should consider further measures to improve the effective follow up of SIS alerts on missing persons in practice and strengthen the effective cooperation amongst the relevant authorities.

Storing data from the age of six years will have a huge impact on children: both with regard to the invasive practice of collecting biometric data as well as considering that their personal data will be stored for a lengthy period in a central database which can also be used for law enforcement purposes. The Meijers Committee urges the legislator not to adopt this measure and to use a minimum age of 12 years.

[21] FRA *Fundamental Rights Implications of the obligation to provide fingerprints for Eurodac*, Focus Paper 5/2015, p. 2.
[22] This obligation to implement the rules on taking migrants' fingerprints at the borders was stressed by the European Commission in the European Agenda on Migration COM(2015) 240, p. 13.
[23] Provisional agreement of 19 June 2018 between the Council and the European Parliament as published on 22 June 2021 at the Public Register of the European Parliament

Transfer to third countries and prohibition of refoulement

The Meijers Committee is particularly concerned about the proposal which abandons the current prohibition of data transfers to third countries in the current Article 35 of Regulation 603/2013. The proposed Article 38, as agreed upon in the provisional agreement, allows the sharing of Eurodac data with the country of origin for return purposes. It does not preclude the transfer of information regarding the fact that the individual concerned applied for asylum in one of the Member States. The provisional agreement of June 2018 only provides that "transfers of personal data to third countries … shall not prejudice the rights of persons […] in particular as regards non-refoulement, and the prohibition to disclose or obtain information in accordance with the provision on the current Procedure Directive [Article 30 of Directive 2013/32/EU]". This provision prohibits in general disclosure "to the alleged actor(s) of persecution of serious harm" of information regarding individual applications for international protection or the fact that an application has been made. If maintained in the new Asylum Procedures Regulation proposal, this provision is less strict than the current overall prohibition to share information with third states, and thus entails more risk of violation of the rights of asylum seekers and the prohibition of non-refoulement.

The proposal as agreed upon in the provisional agreement does provide that "the transfers of any personal data to third countries should be carried out in accordance with the provisions of Regulation (EU) 2016/679 and be conducted with the agreement of the Member State of origin". Furthermore, it provides that independent national bodies must monitor data transfers.

It is however questionable what these safeguards will mean in practice. First, third countries may easily derive from the context of data transfer and the extended categories of data to be shared, the fact that an individual has applied for asylum in one of the Member States, which may put the person at risk of refoulement. Second, it depends on the national practices how and which information will be shared with third states. Third, it is unclear how the envisaged monitoring will occur in practice, considering the current lack of means and staff of national data protection authorities.[24] The requirement in the 2016 Commission proposal that the Member State entering the data must have given its consent for the transfer to third countries and third-country nationals should be informed has been deleted. According to the amended Article 38(1) such data may be transferred or made available to a third state only "with the agreement of the Member State which entered the data".[25] However, this is a lower standard than in the earlier proposal, which said that data may be transferred or made available "only where the following conditions are satisfied" including that "the Member State of origin […] has given its consent". Fourth, data protection supervisory authorities are already overburdened and understaffed in most Member States.

Finally, the Meijers Committee notes that the provisional agreement of 2018 proposed an exception to the requirement of an adequacy decision or appropriate safeguards, transfer of

[24] Council doc. 9848/18, see amended recital 51.
[25] See provisional agreement of 19 June 2018 between the Council and the European Parliament as published on 22 June 2021 at the Public Register of the European Parliament.

personal data to third-country authorities pursuant to the Eurodac Regulation "for the purposes of implementing the return policy of the Union", and that it should be possible to use the derogation from that requirement provided for in the GDPR (Regulation 2016/679). Such an exception is unacceptable, also in the context of decisions of the CJEU with regard to data transfer agreements with third states.[26] This exception should be deleted to ensure the data protection rights, and thus safety, of third-country nationals whose data are stored into Eurodac.

Right to effective judicial protection

The complexity of the provisions in Eurodac in case the 2020 proposal is adopted (in combination with further use of personal information via the interoperability scheme) will hamper the effective use of individual data protection rights and access to effective judicial remedies as protected in Article 47 CFR.[27] The involvement of different Member States and actors in collecting and using personal data in Eurodac will make it difficult, if not impossible, for data subjects to address the competent and responsible authorities. Furthermore, the flagging of persons identified as security risks during the screening procedure may significantly impact the individual rights and mobility of third-country nationals. The current proposal does not provide any legal remedy against such a security flag nor any obligation for authorities to inform the third-country national.

The Meijers Committee proposes that the EU legislator should include an explicit right to effective judicial protection for data subjects with regard to their rights concerning the entry, rectification, completion, and deletion of their personal data in Eurodac, comparable as provided in SIS II.[28] This allows data subjects to bring an action before any competent authority, including a court, under the law of any Member State.

The Eurodac Regulation should also include the obligation for authorities to inform the individual concerned about the flagging or marking in Eurodac as an internal security threat following the screening procedure. The Regulation should also provide access to an effective judicial remedy to refute the entry of such information in Eurodac.

5. Recommendations

Impact assessment – ensure Eurodac amendment is strictly necessary

- Before adopting the Eurodac proposal extending the scope, content and use of Eurodac, an in-depth fundamental rights and data protection impact assessment on the necessity and added value of the proposed amendments should be developed.
- This impact assessment should include the evaluation of the use and effectiveness of existing databases within the field of asylum and migration policies. The specific impact of the use of Eurodac within the interoperability scheme as adopted in 2019 for data

[26] See CJEU Opinion 1/15 on the EU-Canada PNR Agreement.
[27] CJEU C-362/14, 6 October 2014 *Schrems* point 95.
[28] See Article 68 the SIS Regulation 2018/1862.

protection and fundamental rights, as well as an explicit response to the specific concerns and recommendations by earlier opinions of FRA and EDPS should be addressed.

Data retention limits and blocking of data

- Shorter data retention limits for applicants for international protection, but specifically for minors, should be ensured.
- Same standards concerning prior erasure of Eurodac data for all third-country nationals should be applied: ensuring erasure (and non-accessibility for law enforcement purposes) applies when third-country nationals receive long-term resident status, Union citizenship, and international protection.
- The blocking of data of all categories of individuals for law enforcement purposes during a three-year period once these data subjects are granted international protection, citizenship or long-term resident status should be ensured.
- The existence of a link in Eurodac to other databases should also be deleted once a record is deleted and should not be visible to national authorities.
- Safeguards in Article 4(6) should be added so that the authorities of Member States and EU bodies can see only the data that is relevant for the performance of their specific tasks, even if the records are linked in a sequence.

Collection of biometrics – human dignity and protection of minors

- As a thorough substantiation of the necessity and proportionality measure is lacking, the EU legislator should refrain from lowering the age of children to be registered in Eurodac below the age of 12 years.
- Instead, the EU legislator and the Commission should consider further measures to improve the effective follow-up of SIS alerts on missing persons in practice and strengthen the effective cooperation amongst relevant authorities.
- The EU legislator must provide in the Eurodac Regulation that any use of coercion against third-country nationals and specifically minors is prohibited.
- The EU legislator must provide in the Eurodac that administrative sanctions for not cooperating with the collection of fingerprint measures against children, including detention, is prohibited.
- The EU legislator must provide that if there is doubt with regard to the age of persons, they will be treated as minors.

Non-discrimination – complaint mechanisms

- Racial profiling, invasive checks and the abuse of discretion, also in the context of Eurodac use, should be prevented by requiring national authorities to develop guidelines, training programs, accessible complaint mechanisms and a system of consistent monitoring and evaluation of controls taking place at the external borders and within border areas.

Access to effective judicial protection

- An explicit right to effective judicial protection for data subjects concerning their rights concerning the entry, rectification, completion, and deletion of their personal data in Eurodac should be included. Such a right is comparable to SIS II, which allows data subjects to bring an action before any competent authority, including a court, under the law of any Member State.
- An obligation for authorities to inform the individual concerned on the flagging or marking in Eurodac as posing an internal security threat following the screening procedure should be included. Access to an effective judicial remedy should also be included to refute the entry of such information in Eurodac.

Supervision

- A separate provision in the Eurodac Regulation about the obligation in the current Recital 49a on the appointment of controllers with central responsibility for dealing with individual rights of access, correction, and deletion should be included.
- Data protection authorities at EU and national level should be equipped with sufficient means and staff. The EU should bear the costs of additional supervision tasks if it wants those additional supervision tasks to be taken seriously in practice.
- As already recommended by the EDPS, the single model of coordinated supervision should be included by referring to Article 62 Regulation 2018/1725, ensuring cooperation between national data protection authorities and the EDPS.