Annex 1.1: PI Letter to EC 2020

The Trust Fund Coordination Team

European Commission

International Cooperation and Development

Unit D1 – EU Emergency Trust Fund for Africa – Coordination

Rue de la Loi 41 05/081

B-1049 Brussels, Belgium

Sent by email: EuropeAid-EUTF-AFRICA@ec.europa.eu

29 April 2020

Dear Coordination Team

Thank you for your response of 28 October 2019.

As a matter of priority, we would like to thank you for underlining that the projects funded by the Trust Fund save lives. Privacy International is acutely aware of the crucial work being undertaken on which people rely. As we noted in our briefing, the fund addresses "*the needs of refugees and the most vulnerable*" and focuses on "*improving governance and preventing conflicts" as well as the "protection of vulnerable migrants*".

These clearly beneficial and vital activities supported by the Fund are not, however, the subject of recommendations aimed at ensuring the Fund supports rather than undermines the right to privacy in countries in which they are undertaken.

We respectfully disagree that it is a mere "*assertion*" to explain that the Fund "*uses instruments of external policy for internal purposes: the provision of aid and cooperation agreements to deter and manage migration to Europe*". As you are aware, the Fund was created to "*address the root causes of destabilisation, forced displacement and irregular migration*", as part of the Action Plan agreed at the Valetta Summit on Migration – held at the height of the so-called migration crisis in 2015. During the summit, Donald Tusk, President of the European Council, stated that:

The recent developments in Germany, Sweden, and Slovenia and in other countries all show with at most clarity the huge pressure member states are facing. Saving Schengen is

a race against time, and we are determined to win that race. We will launch projects to enhance employment opportunities in regions of origin and transit of migrants in East, North, and West Africa…we will facilitate returns, preferable voluntarily, by a number of concrete steps…and to help implement what we have agreed, we have launched the EU Trust Fund.[1]

Indeed, some of the projects explicitly state that the aim is to reduce migration to Europe. A project in Nigeria aims to improve the "*production and income of smallholder farmers [which] will limit migration to urban centres and thus also reduce the migration pressure to Europe*"[2]. Another aims to "*improve the livelihoods of young Nigerians between the age of 15 and 35 and thereby reduce incentives for irregular migration from Nigeria*".[3] One in Sudan aims to create "*an enabling environment for economic development, establishing pull factors and attractive conditions to settle down. This will contribute to reduce migration outside Sudan and towards Europe*".[4]

Biometrics

As you rightly point out, having an identity allows people to access key services and can be a key protection mechanism. While the provision of a "*legal identity for all, including birth registration*" is a goal of the 2030 Agenda for Sustainable Development, a 'legal identity' includes many different forms of registration, of which a biometric-based record is just one.

As you will be aware, the use of biometric data presents a unique set of concerns. According to the UN High Commissioner for Human Rights :

The creation of mass databases of biometric data raises significant human rights concerns. Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. Against that background, it is

[1] https://www.youtube.com/watch?v=qlbLt_2alOo
[2] https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/t05-eutf-sah-ng-08_pdf.pdf
[3] https://ec.europa.eu/trustfundforafrica/region/sahel-lake-chad/nigeria/skills-development-youth-employment-skye_fr
[4] https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/t05-eutf-hoa-sd-11_-_sudan_-_rdpp_incl._addendum.pdf

worrisome that some States are embarking on vast biometric data-based projects without having adequate legal and procedural safeguards in place.[5]

We are assured that you agree that "*personal data collection needs to be undertaken and managed in accordance with international data protection standards to safeguard the protection of migrants against any potential misuse of the data collected*". Indeed, data protection authorities in Europe have raised grave reservations about the proportionality of proposals that would lead to the storage of biometric data.[6] At the same time, the Grand Chamber of the European Court of Human Rights has explicitly held that indiscriminate or blanket data collection and retention practices by state authorities, such as those involving biometrics, including DNA samples or fingerprints, are not "*necessary in a democratic society*" and fail to satisfy necessity proportionality standards.[7]

The processing of biometric data, including collection, analysis, storing, and sharing must hence be undertaken with extreme caution. To ensure that such systems are lawful, they must:

- Be prescribed by law and limited to that strictly and demonstrably necessary to achieve a legitimate aim. That law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the intrusion with someone's privacy.
- Comply with the principles of necessity and proportionality
- Not indiscriminately retain personal data, given that doing so is never proportionate and necessary, even if when governments seek to justify it on grounds of protection of national security, including threat of terrorism acts.
- Be designed to only meet the goals established in the purpose of the system, and not exceed those purposes thereby creating additional privacy risks
- Only be implemented after a thorough risk assessment regarding its security and be subject to ongoing security audits.

[5] Report of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, 3 August 2018, UN Doc. A/HRC/39/29, https://undocs.org/A/HRC/39/29
[6] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp96_en.pdf
[7] ECtHR, *S. and Marper v. the United Kingdom*, App. Nos. 30562/04 and 30566/04, 4 December 2008

With regard to the systems supported by the Fund, the need for such due considerations is heightened by the fact that none of the countries currently enjoy adequacy in terms of data protection. As such, it is entirely necessary that the Fund foresees "*measures to protect human rights, notably by providing capacity building to ensure that partner countries enforce a proper legal framework*", and that training is provided "*for national authorities and support awareness raising campaigns on the use of biometric data*".

Data sharing

We understand that "[*a*]*ll data collected under the projects remain the property of the governments of partner countries and is not to be shared with the EU or any project implementing partners*". It is envisaged that Consulates will be in charge of identifying any nationals who are to be deported by EU member state authorities. Project T05-EUTF-SAH-CI-01, for example, makes it clear that the establishment of a biometric identification system in Cote d'Ivoire is aimed at making it easier to identify people who are actually of Ivorian nationality and to organize their return more easily.[8]

This will be complemented by readmission agreements as well as a mechanism which will use visa processing as leverage, whereby third countries not cooperating with readmissions will face restrictive penalties.[9] The possibilities of including leverage provisions in the Return Directive (including "*negative or positive incentives*") as well as within a new Regulation establishing an EU readmission leverage mechanism are under consideration by the Council.[10]

We also understand that the Fund plays an important role in the implementation of the "*Partnership Framework*", one of the objectives of which is to curb irregular migration and to enhance the cooperation with third countries on return and readmission.[11] A report for the European Parliament's Committee on Budgetary Control concluded that "*at the policy level there is a more-for-more approach between the potential projects for Ethiopia under the EUTF for Africa and its cooperation in the field of readmission*", noting that "*there appears*

[8] https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/t05-eutf-sah-ci-01.pdf
[9] https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/visa-policy-eu-updates-rules-to-facilitate-legitimate-travel-and-fight-illegal-migration/
[10] http://www.statewatch.org/news/2019/nov/eu-council-readmission-cooperation-13190-19.pdf
[11] https://www.ceps.eu/system/files/EUTrustFundsForEP.pdf

to be unspoken policy 'eligibility' criteria before projects are actually approved, namely cooperation on issues such as return and readmission."[12]

In effect, the development of biometric databases will be complemented with a range if other mechanisms designed to facilitate readmissions by ensuring that third country authorities provide EU counterparts with verification of the data contained within them. Therefore, whether or not the data remains the property of partner countries, EU authorities will still benefit from their operation in a way conducive towards EU (internal) migration policy, rather than development policy aimed at addressing the needs of beneficiaries in non-EU countries.

Other projects

In addition to the projects developing biometric databases, there are a number of other ones which present significant risk to people's privacy rights:

- Project T05-EUTF-SAH-NE-05 envisages providing Niger's security authorities with an international mobile subscriber identity-catcher (IMSI catcher) and a phone interception system in Niamey. An IMSI catcher is a sophisticated surveillance device capable of carrying out indiscriminate monitoring of mobile phones in a given area. They are so sensitive that authorities in the UK refuse to even confirm or deny that they use IMSI catchers.[13] Phone interception systems can and have been used to unlawfully spy on citizens, activists, journalists, political opposition and diplomats.[14]
- Project T05-EUTF-NOA-REG-05 allocated €15 million to law enforcement agencies in Algeria, Egypt, Libya and Tunisia to build identification and investigation capacities. Activities include establishing a group of 'cyber specialists' 'criminal analysts', and 'forensic specialists' capable of conducting online investigations and collecting evidence from digital devices, training them, and providing them with 'light equipment'. Presumably, the collection of evidence will be carried out the use

[12] https://www.ceps.eu/system/files/EUTrustFundsForEP.pdf
[13] https://privacyinternational.org/explainer/2222/imsi-catchers
[14] https://privacyinternational.org/feature/1120/macedonia-society-tap

of intrusive device extraction systems, which lack appropriate safeguards in European states[15] and which have been used to prosecute tortured dissidents.[16]

A number of the projects provide include vague references to 'equipment' which is likely to include electronic surveillance technology. Project T05 –EUTF –HoA –REG -09, aimed at capacity building in Eritrea, Somalia, South Sudan and Sudan, aims at "*improving data collection and promoting sharing of information by supplying government offices and border management posts with essential tools and equipment*". Project T05-EUTF-NOA-REG-07, aims to provide "*operational equipment and thereto-related trainings*" aimed at "*enhancing control and surveillance capacities*" as well as an identification system and aerial surveillance capabilities to Moroccan authorities.

Questions

As has been identified by the Fund's own risk register, it is important for the Fund to address concerns from civil society organisations, such as Privacy International, in order for them to have an accurate understanding of the Fund's work.[17] We would like to underline that we seek to help ensuring that the Fund promotes, rather than undermines, privacy protections in beneficiary countries by ensuring that it is a vehicle for promoting strong protections.

To do so, we require more information on the Fund's current policies and practices so that we, citizens of European and African countries, elected parliamentarians, and data protection authorities can have a better understanding of the challenges, opportunities and practical consequences.

To this end, in September 2019 we filed 10 access to documents requests to EU bodies regarding the transfer of surveillance capabilities to non-EU countries.[18] The requests seek documents providing information on the transfer of personal data, surveillance technology, training, financing, and legislation to non-EU countries, and were submitted to:

- Frontex
- Europol

[15] https://privacyinternational.org/campaigns/phone-data-extraction
[16] https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/
[17] https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/risk_register_eutf_0.pdf
[18] A copy of the requests is available at https://privacyinternational.org/report/3225/challenging-drivers-surveillance-eu-access-documents-requests.

- The European Union Agency for Law Enforcement Training
- The Directorate-General for Economic and Financial Affairs
- The European External Action Service
- The Directorate-General for Budget
- The Directorate-General for Migration and Home Affairs
- The Directorate-General for International Cooperation and Development
- The Directorate-General for Neighbourhood and Enlargement Negotiations
- The Data Protection Officer at the European Commission

Unfortunately, we have since then not received any documents relating to the Fund's projects. This is especially concerning given the number of documents related to the Fund which we believe should fall within the remit of our requests.

We have also filed an access to documents request to EUTF in January 2020 regarding two of the EUTF projects (T05-EUTF-SAH-CI-01 and T05-EUTF-SAH-SN-07).

We kindly ask therefore that you:

1. Provide more details on what "*measures to protect human rights, notably by providing capacity building to ensure that partner countries enforce a proper legal framework*" will be undertaken.

2. Provide more information on how the fund understands "a proper legal framework", with regard to the equipment and training being provided to non-EU countries, including information on what sources were used to inform this understanding, and who is involved in its promotion. Specific surveillance powers are governed differently across EU member states and are subject to different safeguards and oversight mechanisms. For example, some member states may require judicial authorisation for the use of an IMSI catcher, while others may not. It is crucial to know what legal framework the Fund understands to be appropriate.

3. Provide more information on how the Fund ensures that personal data collection is undertaken and managed in accordance with international data protection standards. For example, does the fund promote fundamental principles, found, for

example, in the Charter of Fundamental Rights of the EU, the European Convention on Human Rights and Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which have been ratified by all EU Member States, as well as specific EU data protection, data privacy and security standards, found, for example, in legal instruments governing the processing of personal data for either administrative (e.g. GDPR) or law enforcement (e.g. Directive 2016/680) purposes? How does the fund ensure that adherence to these standards is maintained even after the implementation/completion of the aforementioned projects?

4. Provide more information on what risk assessments or due diligence was undertaken to ensure the biometric databases being supported are lawful.

Finally, we would like to thank you very much for pointing out the factual error in our briefing, which has now been amended to note that Regulation (EU) 2018/1725 governs the processing of personal data by the Union institutions. A note has been added to highlight the correction.

We would like to thank you once again for your initial feedback to our recommendations and look forward to a response. We intend to make this letter publicly available, and would appreciate if you indicate whether you would prefer any forthcoming response to be private or made publicly available.

Yours Sincerely,

[redacted]