Wojciech Wiewiórowski
European Data Protection Supervisor
Rue Wiertz 60
B-1047 Brussels
email: edps@edps.europa.eu

19 October 2021

Re: Human rights groups submit complaint to European Ombudsman and call for investigation into EU surveillance aid to non-EU countries

Dear Mr Wiewiórowski,

On 19 October 2021, Privacy International (PI), Access Now, Border Violence Monitoring Network (BVMN), Homo Digitalis (HD), International Federation for Human Rights (FIDH), and Sea-Watch e.V. ('the undersigned organisations'), submitted a complaint [1] before the European Ombudsman against:

- the European Commission;
- the European Border and Coast Guard Agency (Frontex);
- the European Union Agency for Law Enforcement Training (CEPOL); and
- the European External Action Service (EEAS).

Our complaint argues that the aforementioned EU institutions have failed to carry out (prior) human rights risk and impact assessments, in the context of transfers of surveillance capabilities to third countries.[2]

It is our understanding that EU institutions are under an obligation to conduct human rights risk and impact assessments, including data protection impact assessments, before

[1] PI, Human Rights Groups Submit Complaint to EU Oversight Agency Calling for Investigation into EU Surveillance Aid (19 October 2021), https://privacyinternational.org/news-analysis/4652/human-rights-groups-submit-complaint-eu-oversight-agency-calling-investigation.
[2] PI, Complaint on EU surveillance transfers to third countries (19 October 2021), https://privacyinternational.org/legal-action/complaint-eu-surveillance-transfers-third-countries.

engaging in any form of surveillance transfer.[3] Prior risk and impact assessments are needed to ensure that any surveillance transfer will not result to serious violations of the rights to privacy and data protection, or that it will not facilitate other human rights abuses. However, our research suggests that in most of these cases no (prior) human rights risk and impact assessments, including data protection impact assessments, seem to have been carried out prior to the engagement of the aforementioned EU bodies with authorities of third countries.[4]

We believe that such practices may not only result in impeding transparency and public scrutiny, but they may also seriously undermine the rights and freedoms of both EU and non-EU citizens, including human rights defenders and journalists. Such transfers will very often involve extremely intrusive forms of surveillance that, without the proper (prior) assessments, could be left prone to abuse by regimes that fail to respect human rights.[5]

We further consider that these practices raise serious concerns that pertain to the mandate of the European Data Protection Supervisor (EDPS) as the European Union's independent data protection authority that monitors and ensures the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals.

PI also asserts that despite its constant efforts to have access to more information around the compliance of the aforementioned institutions with their EU law obligations, by filing, among others, a series of access to documents requests under EU Regulation 1049/2001,[6] it is still unclear whether and how human rights considerations, including but not limited to considerations with regard to individuals' privacy and data protection rights, are taken into consideration by the aforementioned EU institutions.

The complaint to the European Ombudsman:

- provides an overview of the key institutional frameworks that we have identified as enabling EU transfers surveillance capabilities to authorities of third countries;
- details the previous engagement and exchanges PI had with the European Commission and other EU institutions as part of its access to documents requests and other avenues;
- describes the legal framework, under which we understand that EU institutions are obliged to carry out human rights risk and impact assessments before engaging with

[3] See Complaint to European Ombudsman, pages 9-12.
[4] PI, Revealed: The EU Training Regime Teaching Neighbours How to Spy (10 November 2020), https://privacyinternational.org/long-read/4289/revealed-eu-training-regime-teaching-neighbours-how-spy.
[5] PI, Borders Without Borders: How the EU is Exporting Surveillance in Bid to Outsource its Border Controls (10 November 2020), https://privacyinternational.org/long-read/4288/borders-without-borders-how-eu-exporting-surveillance-bid-outsource-its-border.
[6] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

authorities of third countries in the context of transfers of surveillance capabilities; and, finally,

- highlights the grave human rights concerns arising in the context of surveillance transfers and provides further evidence of lack of (prior) human rights risk and impact assessments.

For further information, we invite you to refer to the complaint annexed to this letter. Both the complaint and its accompanying annexes are published on PI's website.[7]

The undersigned organisations submit that such practices raise significant concerns about the compliance of the aforementioned EU institutions with their obligations under EU law and could amount to violation of their obligations under EU data protection laws.

Regulation (EU) 2018/1725 lays down the rules governing the processing of personal data by EU institutions, bodies, agencies, and offices.[8] Article 39 of the Regulation places an obligation of the EU institutions, bodies, agencies, and offices to conduct a data protection impact assessment. It specifically states:

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks [...]

2. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

    (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

    (b) processing on a large scale of special categories of data referred to in Article 10, or of personal data relating to criminal convictions and offences referred to in Article 11; or

    (c) a systematic monitoring of a publicly accessible area on a large scale.

Moreover, Article 40 (Prior consultation of the European Data Protection Supervisor) of Regulation 2018/1725 requires entities acting as controllers, i.e., EU institutions, bodies, offices, and agencies, to consult with the European Data Protection Supervisor. It states:

> prior to processing where a data protection impact assessment under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to

[7] PI, Complaint on EU surveillance transfers to third countries (19 October 2021), https://privacyinternational.org/legal-action/complaint-eu-surveillance-transfers-third-countries.
[8] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

> mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation.

According to the EDPS:

> The DPIA [data protection impact assessment] process aims at providing assurance that controllers adequately address privacy and data protection risks of 'risky' processing operations. By providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs help organisations to comply with the requirement of 'data protection by design' where it is needed the most, i.e., for 'risky' processing operations.[9]

On 16 July 2019, the EDPS adopted a decision under Articles 39(4) and (5) of Regulation (EU) 2018/1725 that contains a list of processing operations that could require the carrying out of a DPIA by controllers.[10] These are contained in Annex 1 (List of criteria for assessing whether processing operations are likely to result in high risks) of the decision and, among others, include:

- Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting.
- Systematic monitoring: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces. This may cover video-surveillance but also other monitoring, e.g. of staff internet use.
- Sensitive data or data of a highly personal nature: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or data of highly personal nature.
- Data processed on a large scale, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage.
- Data concerning vulnerable data subjects: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified.
- Innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage. Indeed, the personal and social consequences of the deployment of a new technology may be unknown.

Regarding the concerns raised by the sharing of personal data between third country authorities and EU bodies or institutions, we understand that it is the EDPS, who is primarily

[9] European Data Protection Supervisor, Accountability on the ground, Part II: Data Protection Impact Assessments & Prior Consultation, v1.3 July 2019, page 5, https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf.
[10] European Data Protection Supervisor, Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA Lists issued under Articles 39(4) and (5) of Regulation (EU) 2018/1725, https://edps.europa.eu/sites/default/files/publication/19-07-16_edps_dpia_list_en.pdf.

tasked with the monitoring of the compliance of EU institutions with governing data protection laws, namely Regulation (EU) 2018/1725.[11]

While the undersigned organisations might have not been directly affected by the activities described above, we nevertheless urge the EDPS to *proprio motu* exercise his investigative powers under Article 58 of Regulation (EU) 2018/1725, particularly the power to initiate an investigation in the form of data protection audits,[12] to order the EU institutions and bodies concerned to provide more information with regard to their data processing activities in connection with third country authorities,[13] as well as to obtain access to all evidence and means necessary to better support his investigation.[14] Finally, we invite the EDPS to work closely with the European Ombudsman in any investigation that may follow our submissions.

We remain fully at your disposal should you have any further queries or questions. You can contact us by email at ioannisk@privacyinternational.org and ilia@privacyinternational.org.

Yours sincerely,

Privacy International

Access Now

Border Violence Monitoring Network (BVMN)

Homo Digitalis (HD)

International Federation for Human Rights (FIDH)

Sea-Watch e.V

Annex: Privacy International (PI), Access Now, Border Violence Monitoring Network (BVMN), Homo Digitalis (HD), International Federation for Human Rights (FIDH), and Sea-Watch e.V. complaint to the European Ombudsman.

[11] Article 52, Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
[12] Article 52(1)(b), ibid.
[13] Article 52(1)(d), ibid.
[14] Article 52(1)(e), ibid.