Frontex; the processing of personal data under the 2019 regulation

Referring to the Frontex Regulation 2019, the Returns Directive Recast Proposal, some UK domestic legislation and the GDPR.

What changes have taken place regarding Frontex's processing of personal data?

Frontex had been processing personal data in the context of joint return operations since at least 2009 (EDPS opinion 2010), apparently without adopting measures to implement Regulation 45/2001 on data protection.

The competence to process personal data was formally introduced in 2011 amendment to the Frontex regulation. This amendment also introduced the role of an internal Agency Data Protection Officer, as well as the competence of the European Data Protection Supervisor to monitor all Agency activities.

The 2019 Frontex Regulation extends

- the types of data contained in IT systems and databases used and controlled by the Agency
- the purposes for which the data can be used.

Additionally, under the umbrella of "interoperability", the systems themselves are being interconnected.

The purposes for which the Agency may process data in the Regulation are extensive, covering all tasks, including "administrative tasks".

The main issue with this extension of data processing appears to be that the regulation combines the development and operation of these centralised information systems, managed by Frontex for the purpose of coordinating expulsion operations, with exemptions from data protection obligations in certain cases.

These exemptions are justified in the preamble to the 2019 Regulation under recital 100:

> *"…the exercise of the right to the restriction of processing may significantly delay and obstruct the performance of the return operations. Furthermore, in some cases the right of access by the data subject may jeopardise a return operation by increasing the risk of absconding should the data subject learn that the Agency is processing his or her data in the context of a planned return operation. The right to rectification, on the other hand, may increase the risk that the third country national in question will be misleading the authorities by providing incorrect data.* ***To this end, the Agency should be able to adopt internal rules on such restrictions."***

Overview of relevant Articles referring to personal data processing and rights of data subjects

Article 10 on the tasks of the Agency, includes:

Development and operation of information systems that enable swift and reliable exchanges of information regarding emerging risks in the management of external borders, illegal immigration and return, in close cooperation with the Commission, Union bodies, offices and agencies as well as the European Migration Network established by Decision 2008/381/EC.

These tasks already existed, and are maintained in the 2019 Regulation.

The 2019 Regulation adds these as tasks of the Agency:

- Development of technical standards for information exchange.
- Management and operation of the False and Authentic Documents Online (FADO) system referred to in Article 80
- Support to Member States by providing support for facilitating detection of document fraud
- Fulfilment of tasks and obligations entrusted to the Agency referred to in Regulation (EU) 2018/1240 of the European Parliament and of the Council [establishing ETIAS]
- Setting up and operating the ETIAS Central Unit in accordance with Article 7 of that Regulation.

Article 49 on return, allows or obliges Frontex to:

- provide technical and operational assistance to Member States in return, including
    - (i) in the collection of information necessary for issuing return decisions,
    - the identification of the third country nationals subject to return procedures and other pre-return and return-related and post-arrival and post-return activities of the Member States to achieve an integrated system of return management among competent authorities of the Member States, with the participation of relevant authorities of third countries and other relevant stakeholders;
    - in the acquisition of travel documents, including by means of consular cooperation, without disclosing information relating to the fact that an application for international protection has been made or any other information that is not necessary for the purpose of return;
    - to "develop, in consultation with the fundamental rights officer, a non-binding reference model for a national IT return case-management system describing the structure of such systems, as well as provide the technical and operational assistance to Member States in developing such systems compatible with the model."
    - To operate and further develop an integrated return management platform and a communication infrastructure that enables the linking of the national return management systems of the member states with the platform for exchange of data and information, including the automated transmission of statistical data, as well as provide technical and operational assistance to Member States in connecting to the communication structure

This refers to the Returns Directive recast proposal in circulation up to November 2019, which contains an obligation for member states to set up national systems compatible with Frontex central interface.

Article 50 on information exchange systems and the management of return, describing the personal data they shall contain as:

- The personal data may only include biographic data or passenger lists if the transmission of such data is necessary for the purposes of the Agency assisting in the coordination or organization of return operations to third countries, irrespective of the means of transport.
- Such data shall be transmitted to the platform only when a decision to launch a return operation has been taken, and shall be erased as soon as the operation is terminated.
- Biographic data shall only be communicated to the platform where it cannot be accessed by members of teams in accordance with Article 17 of Regulation (EU) 2018/1860 on the use of Schengen Information System for the return of illegally staying third-country nationals.
- The platform may also be used by the Agency for the purpose of secure transmission of biographic or biometric data including all types of documents which can be considered as proof or prima facie evidence of the nationality of third country nationals subject to return decisions, if the transmission of such personal data is necessary for the purpose of the Agency to provide assistance in confirming the identity and nationality of third-country nationals in individual cases and at the request of Member State.
- Such data shall not be stored on the platform and shall be deleted immediately following a confirmation of receipt.

Article 51, on the Rolling Operational Plan (first introduced in 2016), also authorizes Frontex teams to, prior to the return of any returnee, consult the Schengen Information System in order to check whether the return decision is suspended or the enforcement of the return decision postponed.

Article 56 on Frontex's authority to share personal data with third countries, or destination countries, and consular cooperation in order to acquire travel documents.

Although the Regulation prohibits the Agency to disclose if the individual applied for international protection, the interaction with the proposed recast Returns Directive raises the risk, if this legislation is accepted, that Frontex will communicate a person's identity with a third country automatically, as soon as an individual receives a negative asylum decision.

Article 74 on cooperation between the Agency and Third Countries (for purposes other than return), including that Status Agreements must be submitted to the EDPS for approval.

Article 88 on the purposes of processing of personal data allows the agency to process personal data for the performance of its tasks, including a wide range encompassing the coordination of joint operations, pilot projects, rapid border interventions, migration management support, pre-return and return activities and operations, operating return management systems, providing technical and operational assistance to Member States and third countries for return, facilitating exchanges of operations (with member states, EU bodies and Agencies, international organisations, European Maritime Safety Agency, European Aviation Safety Agency, European, Fisheries Control Agency, national law enforcement authorities, Europol and Eurojust), risk analysis, tasks under EUROSURE, operation of FADO, administrative tasks.

This article allows the Agency to use personal data provided by a member state or Union agency for a different purpose than the one identified by that data provider, on a case-by-case basis, following an assessment that this secondary purpose is compatible with the initial purpose.

Article 89 on processing of personal data collected during joint operations, return operations, pilot projects and rapid border interventions and by migration management support teams assigns Frontex and the host member state the role of joint data controllers, with overall responsibility to be indicated in operational plans, rolling plans or "an arrangement". The Article specified that this agreement shall be available to the data subjects, and indicate a contact point for the data subjects.

Article 90 on the processing of personal data in the framework of EUROSUR defers to Regulation (EU) 2016/679 and, where applicable, Directive 2016/680. Ship and aircraft identification numbers are the only personal data that may be accessed in the European situational and specific situational pictures and the Eurosur Fusion Services, though the processing of other personal data may exceptionally be required.

Any exchange of information under Articles 73(2), Article 74(3) and Article 75(3) which provides a third country with data that could be used to identify persons or groups of persons whose request for access to international protection is under examination or who are under a serious risk of being subjected to torture, inhuman and degrading treatment or punishment or any other violation of fundamental rights, shall be prohibited.

Article 90a on processing of operational personal data allows the Agency to exchange personal data with Europol or Eurojust, where the transmission of such personal data is strictly necessary for the performance of their respective mandates, and with the competent law enforcement authorities of member states where it is strictly necessary to those authorities for the purposes of preventing, detecting, investigating or prosecuting serious cross border crime.

Article 90b on data retention obliges the agency to delete personal data as soon as they have been transmitted to the competent authorities of Member States, other Union Agencies and EASO, or transferred to third countries or international organisations or used for the preparation of risk analyses. Risk analyses will use anonymised data, and data retention cannot exceed 90 days (or 30 days after the end of return-related tasks).
The Agency shall decide on the continuous storage of personal data, in particular the personal data of victims and witnesses, until the following review, only if such storage is still necessary for the performance of the Agency's tasks under Article 90a.
The above provisions will not apply to personal data collected in the context of FADO.

Overview of exemptions from data protection obligations

By omission

The 2019 Regulation does not clarify if Frontex is obliged to consult Member States to assess exemptions.

There is no specific requirement for either the Data Protection Officer (internal) or the EDPS to have oversight of the processing of personal data in the context of Frontex return operations.

Exemptions included in the text

Exemptions to data protection provisions were first introduced by the 2016 regulation:

Article 29(2), superseded by **Article 51(2)** of the 2019 Regulation allowed the Agency "on a case by case basis" …"as long as the exercise of such right would risk to jeopardise the return procedure" to deny individuals access to their data.

Additions under the 2019 Regulation include:

Article 87 authorising the Agency, through the Management Board, to adopt "internal rules on restricting the application" of a number of rights and obligations set out in the EU data protection regulation, including the right to receive information on personal data processing, rights of access, rectification and erasure, the right to request restriction of processing, the requirement that data controllers inform the subject in case of a personal data breach.

All restrictions must be necessary and proportionate to the objectives and respect the "essence" of fundamental rights and freedoms.

Article 87 focussing particularly on return activities: "In particular the Agency shall, for the performance of the Agency's tasks in the area of return activities, provide for internal rules on restricting the application of those rights on a case by case basis as long as the exercise of such right would risk to jeopardise the return procedure."

Article 87(3) permitting international data transfers "insofar as such transfer is necessary for the performance of the Agency's tasks"- which covers returns and all other areas of activity.

What are the data sharing and storage platforms referred to?

Officials deployed by Frontex and the European Asylum Agency will have the power to add files to **EURODAC**- the "European Asylum Dactyloscopy Database"

Frontex officials will have access to data stored in the **Entry and Exit System** to carry out risk analyses and vulnerability assessments, though without allowing for individual identification.

States are obliged to insert decisions on returns and entry bans into the **Schengen Information System**, to be checked by Frontex operatives prior to return operations.

The Agency will establish a "technical interface" to the central SIS database for searches by Frontex operatives. In theory this is a safeguard, but it relies on States systematically entering this information.

- A CPT report on a Joint Return Operation coordinated by Frontex from Italy in 2015 indicated that some of the deportees were subject to removal while court appeals relating to their asylum requests were pending- therefore this safeguard depends on the suspensive effect of appeals, and therefore possibly the outcome of the recast Returns Directive proposal.

Frontex officials will have access to the **Visa Information System** under certain conditions. Frontex must establish a central access point to request access to the system.

Frontex will continue to operate two central information systems to coordinate deportation:

- **IRMA: Irregular Migration Management Application**- "a secure electronic platform which connects Member States and Schengen Associated States, DG Home, ECBGA, relevant EU funded programmes at operational practitioner level, in order to build synergies and to enable work in a mutually enforcing way"
  - Uses more general data to enhance the ability of the EU and Member States to coordinate and conduct deportations
  - Assists with needs assessments and increase efficiency of returns through the collection of data on activities at member state level covering expulsion proceedings and decisions.
- **FAR: Frontex Application for Return**- for individual cases, to rationalise and streamline the implementation of return operations.
  - Will be linked with national return case management systems developed by Member States.
  - Pulls together planned return operations of Member States, announcement of participating states in those operations, all communications relating to particular Frontex coordinated return operation and pre-return assistance.
  - FAR approved by the EDPS in 2018- but neither Frontex proposal or EDPS opinion is public.
    - A withdrawn note about FAR by Frontex to the EDPS made it clear that lists of returnees would be handed over to destination states
  - FAR holds: name and surname, destination of departure and arrival, date of birth, nationality, gender, country of origin, type and validity of travel document, health, voluntary or forced return, and security risk assessment of deportees.
  - The Data Protection Notice for the FAR states that returnees have the right to rectification of inaccurate data, to request restrictions on processing, or object to processing of their data.
    - Exercise of these rights depends on the right to access data. As discussed, this right may be restricted, on a case by case basis, for reasons of national security, public security, defence of member states. Frontex has no specific legal competence in those areas.

The European Data Protection Supervisor's opinion on the 2019 Regulation

Not having been consulted, the European Data Protection Supervisor issued formal comments on the proposal, before the final compromise text was agreed. Some of the EDPS suggestions do seem to have been taken into account.

Overall, the concerns logged by the EDPS refer to the imprecision of the legislation where it deals with personal data, including:

Lack of clear allocation/definition of responsibility between EBGC and member states.

Lack of clear identification of, and distinction between, purposes of data processing.

Uncertainty on conditions or limits for sharing data with other agencies, states and third countries, and on available remedies for individuals.

Risk of non-compliance with existing data protections rules

This reflects how the new regulation challenges the principle of purpose limitation. **Articles 88 and 89** in particular cause concern over the likelihood of data being processed for a purpose other than that for which it was collected.

Regarding the Regulation's impact on Frontex's use of and authority over databases governed by their own Regulations, and Frontex Officers' increased capacity in border and return operations, the EDPS noted that the Regulation "would affect (and may not always be consistent with) the relevant (administrative) substantial rules and procedures set out in other EU legal instruments (in particular, the regulation on the Visa Information System; the 'recast Eurodac Regulation'; the 'Asylum Procedures Directive'; the 'Return Directive').

The 'blurring of accountability' foreseen by the EDPS between the EBCG and the Member States "may lead to uncertainties relating to the data protection obligations (identification of 'controller') and, ultimately, to the identification of the entity towards whom the person concerned shall exercise his or her data protection rights (for example, of rectification)." The executive powers awarded under the Regulation puts operations under EBCG, not member state, authority, but without clearly defining the Agency's responsibility as data controller.

The EDPS also noted that the 2019 Regulation did not incorporate recommendations made by the EDPS on the 2016 Regulation, gaining "increased importance…notably in relation to: (i) the (lack of clear) allocation and definition of responsibilities between the EBCG and the Member States; and (ii) the (lack of clear) identification of and distinction between the purposes of the data processing (border control, security, police and judicial cooperation)."

What personal rights under the General Data Protection Regulation are affected?

Article 13 and 14 on informing the data subject of the processing of their personal data.

The data subject should receive adequate information to allow them to exercise the following rights, including information on the contact details of the data controller, and the consequences of failing to provide personal data, and any existence of automated decision making

Article 15 on the right of access by the data subject.

Where personal data are being processed, the data subject should have access to the information itself and to information on the purposes of processing, categories of data concerned, recipients of the data (especially recipients in third countries or international organisations), how long the data will be stored, the right to request rectification or erasure of personal data, restriction or objecting to its processing, lodging a complaint with the supervisory authority, the source of the data (where not provided by the data subject) and the existence of any automated decision making. This includes a copy of the data being processed.

Article 16 on the right to rectification

Any inaccurate data should be rectified without undue delay.

Article 17 on the right to erasure

If the data is no longer necessary for the purposes for which it was collected, there are no overriding legitimate grounds for processing, or it is processed unlawfully, the data subject can obtain erasure.

- This right shall not apply to the extent that processing is necessary for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject, or for the purpose of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Article 18 on the right to the restriction of processing

If the accuracy of the data is contested, the processing is unlawful or the data is no longer needed, the subject can obtain a restriction of processing.

Article 21 on the right to object to data processing

The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Article 22 on the right not to be subjected to automated individual decision making.

Article 23 on the restrictions to individual rights

Restrictions may be valid when safeguarding a long list of objectives, including national security, public security, protection of public interest and defence, and where the **legislative measures contains specific provisions.**

What do parallels with exemptions under domestic law suggest about risks?

Fairly direct comparison is possible with the UK's Immigration Act as amended in 2018.

Schedule 2, part 1, paragraph 4 of this Act contained exemptions for purposes of effective immigration control and detection of activities undermining the maintenance of effective immigration control.

These broadly include the same exemptions as the Frontex Regulation, including the right to confirmation of processing, the right to access to data, and safeguards for third country transfers.

Issues that have come to light under this Act:

The Act was challenged in UK High Court over its lack of definition of "immigration control", which widens the issue even further than migrants' rights to their own data, because the breadth of the term means *any* data controller can exercise the exemption, for a non-exhaustive list of matters that could fall under "immigration control". E.g. Hospitals, universities, schools.

Open Rights Group and *the3million* have challenged the Immigration Act on the grounds that mistakes and errors in personal data can have dangerous implications, including the lack of opportunity to challenge wrongful refusal of immigration status and wrongful deportations. An individual cannot exercise their right to data rectification if they have no confirmation that their personal data are being processed, or the right to access it. This could prevent people gaining access to information needed to appeal government decisions regarding their immigration status.

To illustrate the potential gravity of this, from 2005 to 2015, there were 250,000 such appeals against the Home Office, and the Independent Chief Inspector of Borders and Immigration had a 10% error rate. If Frontex is handed incorrect or incomplete data by a Member State, an individual cannot establish whether there is an error.

The lowering of legal standards, the removal of certain rights and protections, the lack of access to legal assistance, the risk of poor decision making, along with the introduction of exemptions to individuals' right to access their data leads to a compounded possibility that mistakes made at the national level will go uncorrected.

PICUM have lodged a complaint to the EU – the first GDPR complaint – against the UK law for violating the data rights of foreigners "without the knowledge of the affected individuals and with virtually no accountability". The outcome of this case me be pertinent to analysis of the Frontex Regulation.