EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

EDPS OPINION ON A PRIOR CONSULTATION REQUESTED BY THE EUROPEAN BORDER AND COAST GUARD AGENCY

on the Integrated Return Management Application (IRMA) 2.0

(Case 2021-0991)

According to Article 40 (1) of Regulation (EU) 2018/1725 (the 'Regulation' or the 'EUDPR')[1], the Opinion of the European Data Protection Supervisor (the 'EDPS') should be sought whenever a data protection impact assessment under Article 39 of the Regulation indicates that the processing would, in the absence of safeguards, security measures and mechanisms to 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.

Having performed a data protection impact assessment, the European Border and Coast Guard (also known as Frontex) has consulted the EDPS regarding certain high risks identified by the agency in relation to the future use of the Integrated Return Management Application 2.0 ('IRMA 2.0'). The EDPS issues this Opinion in accordance with Article 40(2) of the Regulation.

The EDPS is of the opinion that the mitigating measures envisaged by Frontex in the consultation and appended documentation may be insufficient to mitigate the high risks it has identified, and has formulated several recommendations to ensure compliance of the envisaged processing with the Regulation.

[1] Regulation (EU) 2018/1725 of the European Parliament and 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, OJ, L 295, 21.11.2018, pp. 39-98.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

Table of Contents

1. PROCEEDINGS

On 20 October 2021, the EDPS received a request for prior consultation from Frontex under Article 40 of the Regulation on its planned Integrated Return Management Application 2.0 ('IRMA 2.0').

The prior consultation request contained the following:

- a cover email by the Frontex Data Protection Officer ('DPO') regarding the high risks identified by the DPO (the 'cover email');
- the Data Protection Impact Assessment on IRMA (the 'DPIA'); and
- the concept note about IRMA 2.0 (the 'concept note');
- the relevant record under Article 31 of the Regulation (the 'record') and
- the threshold assessment regarding IRMA 2.0 (the 'threshold assessment').

Alongside the prior consultation, a formal consultation was submitted on the question of controllership in the context of IRMA.

On 22 October 2021, the EDPS requested clarifications as to the exact scope of the prior consultation as the DPIA did not identify residual high risks to the rights and freedoms of natural persons after application of proposed mitigation measures. The EDPS also inquired whether all questions raised were intended to be part of the prior consultation, and in particular a set of questions on the division of responsibilities (and as such the allocation of controllership) between the actors in the IRMA 2.0 platform.

On 27 October 2021, Frontex replied indicating that it submitted all questions as part of the prior consultation and that three risks should be considered for this prior consultation, namely the issue of controllership, the encryption scheme and the envisaged hosting of the platform in Microsoft Cloud.

On 30 November 2021 a meeting took place between the EDPS and the European Centre for Returns ('ECRET') as well as Frontex' DPO. During the meeting, the EDPS posed additional questions regarding the organisation of return operations by Frontex, and raised several technical considerations for discussion.

On 1 December 2021, the EDPS requested Frontex DPO to provide the Agency's assessment on the issue of controllership and the DPO's relevant advice.

On 7 December 2021, Frontex' DPO provided her advice provided to the Agency on the matter and the power point presentation on IRMA's data flows presented during the meeting of 30 November 2021.

According to Article 40(2) of the Regulation, the EDPS is to issue his Opinion within a period of up to eight weeks of receipt of the request for consultation, with a possible extension of six weeks. As the EDPS did not exercise this possibility to extend, the deadline within which the EDPS shall issue his Opinion is **16 December 2021**.

2. DESCRIPTION OF THE PROCESSING

2.1. Current version of IRMA

As published by Frontex,[2] the current version of IRMA is an online platform, where Member States (MS) and Schengen Associated countries (SAC), Frontex, the European Commission and other EU bodies/agencies (e.g. EASO), can exchange strategic and operational information on returns.

Return means the process of a third-country national going back — whether in voluntary compliance with an obligation to return, or enforced — to:

— his or her country of origin, or

— a country of transit in accordance with Community or bilateral readmission agreements or other arrangements, or

— another third country, to which the third-country national concerned voluntarily decides to return and in which he or she will be accepted.[3]

Another important current IT tool in the field of returns is the Frontex Application for Return (FAR) of irregular migrants. FAR is a web application that facilitates information exchange on specific and punctual needs in the field of returns. It helps Member States to express their Return Operation Needs and to coordinate charter flights, scheduled flights and manage readmissions.[4] It also supports identification missions, which are visits from (or postings of) Third Country delegations to EU Member States (MS) and Schengen Associated countries (SAC), where they interview Third Country nationals with the aim of confirming their nationality (identification) and to issue travel documents in order to allow them to return to their home country.

The current IRMA as described above will be substantially altered under the IRMA 2.0 project, the subject of this prior consultation of the EDPS. The platform will be supplemented with additional features, and will be fully integrated with the FAR application. The latter is a significant step since, as the DPIA mentions,[5] the initial IRMA platform was developed and hosted by the European Commission and did not include FAR as a module. FAR has been developed and hosted by Frontex, which now wants to completely harmonise both IRMA and FAR as a one-stop-shop for MSs and the Agency in the area of Returns. This complete integration also entails that, while the current FAR was already subject to a prior check[6] by the EDPS in 2017 under the previous data protection framework (Regulation (EU) 45/2001)[7] Frontex should analyse the new way of operating the FAR for data protection risks.

The aim for IRMA is to supply rich and easily searchable content, as well as to improve

---

[2] 'Integrated return management application', Frontex, DOI 10.2819/959670, https://op.europa.eu/de/publication-detail/-/publication/7f17a76a-719e-11eb-9ac9-01aa75ed71a1.

[3] Article 3(3) of Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348, 24.12.2008, p. 98–107.

[4] Information taken from the FAR User Manual, version of 13 March 2019.

[5] Sheet 10, row 3.

[6] Inter alia, sheet 1, row 6.

[7] EDPS case 2017-0874, available on the EDPS website https://edps.europa.eu/system/files/2021-04/opinion_for_publication_2017-0874_en.pdf .

communication between the users, by providing a collaborative environment for content sharing, as well as a secure channel for encrypted communication. The platform will also provide access to return data reporting and visualisation.

2.2. IRMA 2.0 Concept

Article 48(d) and 49 of Regulation (EU) 2019/1896 (the 'EBCG Regulation') task Frontex with operating and further developing an integrated return management platform and a communication infrastructure that enables the linking of the return management systems of the Member States with the platform for the purpose of exchanging data and information.

IRMA 2.0 would implement these provisions on data exchange through a central online platform integrating a variety of operational modules (including the modules of the FAR), each with separate functionalities and processing different personal data. In other words, the aim for IRMA 2.0 is to move even further towards a '*return toolbox*' at Member State and EU-level.

As a return toolbox, where each of its parts or modules have different purposes and process different personal data, the EDPS considers it absolutely vital to analyse the platform purpose per purpose - in order to properly identify which parts may or may not pose high risks for the data subject.

From the concept note shared with the EDPS, it appears that the functioning of the IRMA 2.0 platform can be roughly subdivided into four streams: first the 'backbone' modules of the platform that are required to access it in the first place (governing access rights, account management, etc.); second, 'content management' modules that will allow stakeholders to create content pages with return-related information, to share media and work collaboratively on text documents; third, a messaging functionality between users; and finally what are called 'operational modules', used, among others, to organise charter or scheduled flights for returns.

To facilitate its features, authenticated users are able to check and search for personal data of other users registered in the platform (e.g. name, surname or email addresses) for the purpose of exchanging return related information. The platform also contains contact information of other relevant stakeholders in the area of return, for example representatives of Third Countries, contact points in MS or EU delegations in TC in order to facilitate the cooperation with those stakeholders (for the purpose of communication between the registered users).

The messaging system will be used to send/receive encrypted files that may include personal data of Third Country Nationals (TCN) in the context of a return procedure. An encryption scheme will be created to allow the exchange of files, so that only the sender and addressee(s) can decrypt them. The transfer of encrypted files is done directly between the users, with no intermediaries being involved. Frontex will not have any means to decrypt the encrypted files.[8]

Three operational modules for the system are foreseen at this stage[9]:

[8] DPIA report, sheet 1, B7.
[9] IRMA 2.0 concept note, page 2 and 3.

- **Operational module 1 - Identification Missions:**

The Identification Missions module will support the implementation of the above-mentioned Identification Missions.

From the previous notification of FAR for prior checking[10] and the present DPIA,[11] the EDPS understands that the purpose of the processing of personal data for identification missions is to facilitate the organisation of the identification mission itself, thus only processing the personal data of the third-country officials and the contact points in the MSs.

- **Operational module 2 - Charter Flights:**

This module will offer Member States and Schengen Associated Countries the possibility to implement Frontex supported returns by charter flights. It thus allows MS and SACs to request technical and operational support from Frontex for Charter flights. The module supports three types of forced returns (joint national operations, national return operations and collecting return operations), as well as two types of voluntary returns/voluntary departures (joint and national). In addition, readmission operations based on the EU – Turkey readmission agreement are currently also in the scope of this operational module, offering Frontex supported readmissions via sea and air.

- **Operational Module 3 - Scheduled Flights:**

This module will offer Member States and Schengen Associated Countries the possibility to organize and implement forced and voluntary returns by scheduled flights with Frontex support. It thus allows MS and SACs to request the support of Frontex for the coordination and organization of such flights. The module allows the users to organize DEPA return operations (return operations of escorted returnees), DEPU return operations (return operations of unescorted returnees), as well as receive technical assistance from Frontex in relation to voluntary returns (VR) and voluntary departures (VD).

The EDPS notes that in the consultation the operational modules are often put in open-ended lists, for example in the concept note[12] (which has a '...' module in the schematic), and the DPIA[13] ("the new system will integrate operational modules e.g. Scheduled Flights, Charter flights and readmissions and Identification Missions component). The EDPS reminds that, where Frontex would add new modules to IRMA, it would likely need to adapt the DPIA report to reflect this. The present Opinion only applies to IRMA 2.0 as defined in the documentation referred to in section 1 of this Opinion.

Entering personal data of returnees, TCNs returning voluntarily, supporting staff and other stakeholders throughout the different modules of the IRMA 2.0 platform will take place in multiple ways.

A first possibility is that it is simply imported into the system by a designated user via the user interface. In some cases, (e.g in case staff is deployed on board of a return operation), staff data can be inserted by the FAR Service Desk or the Organising Member State ('OMS') if applicable.

---

[10] EDPS case 2017-0874, notification page 5.
[11] Sheet 2, B19.
[12] Page 1.
[13] Sheet 1, B7.

The data can also be introduced by the national Return Case Management Systems ('RECAMAS') via the system-to-system communication infrastructure. In this case the data is actually collected via the national RECAMAS by the national authorities and transferred to IRMA 2.0. The DPIA, as well as the other supporting documentation, contain little technical information on how this direct transmission of personal data from the RECAMAS to the IRMA 2.0 platform would function. The EDPS understands that this feature may be in its early stages, however any direct personal data 'uploads' to IRMA 2.0 from the national RECAMAS would represent a major change in the processing of personal data of returnees and TCNs returning voluntarily, likely triggering the need to review the DPIA in order to address any eventual high risk to the rights and freedoms of natural persons, for instance in terms of data quality.

3. PRIOR CONSULTATION PURSUANT TO ARTICLE 40 OF THE REGULATION

3.1. The threshold assessment

Considering that the creation of a new version of IRMA, including all of its components, represents a type of processing using new technologies, Frontex has carried out a threshold assessment of the risks generated by this new processing, and identified the following elements triggering the need for a DPIA:[14]

First, special categories of personal data of data of a highly personal nature will be processed in the context of IRMA 2.0:

- The return by charters module contains the possibility to insert data on past violent behaviour so this can be taken into account when organizing the return operation.

- In the scheduled flights module, Frontex is considering the possibility to include a notification form to airlines, which contains:

    - medical information of returnees (requirements for a wheelchair, oxygen, additional seating, adjustments for deafness, other conditions);
    - identification documents (a photocopy of the travel document) ;
    - information with regard to the reason for return (illegal stay/other with requirement to specify) and;
    - a risk assessment (no risk / accompanied by police/security agents because of refused earlier departure or as outcome of risk assessment or accompanied by official/medical personnel/person of trust/interpreter).

- In scheduled flights module, another future development will include the transit request form. This will include:

    - information on the travel document (number/type/validity),
    - medical information, (i.e. if medical care is required-requirement to specify if yes, possible contagious identifiable diseases-requirement to specify if yes),

[14] Criteria from Annex 1 to the EDPS decision of 16 July 2019 on DPIA lists issued under Articles 39(4) and (5) of Regulation 2018/1725

- information on previous unsuccessful attempts with specification of reason and documents accompanying the transit request form (photocopy of travel document).

– Furthermore, the information exchange module in the IRMA 2.0 platform will support the exchange of biometric data such as fingerprints.[15]

Second, the processing of data will take place on a large scale. Frontex states that for the purpose of forced and voluntary returns, on average, the number of returnees and TCNs returning voluntarily is estimated between 300 and 2000 per month (depending on the type of flight - scheduled or charters - and the year).[16]

Third, the processing operations will relate to vulnerable data subjects as in the context of the operational modules for organizing forced and voluntary returns, the MS will communicate personal data of returnees and TCNs returning voluntarily for the purpose of organizing forced and voluntary returns.[17]

In addition to these three inherent risk areas, Frontex is further considering cloud hosting for the servers of the platform. Frontex is proposing to create a hybrid environment and extend the current on premise infrastructure with data centres located on public clouds provided by Microsoft Azure Cloud. Frontex data stored on these hosts would be encrypted by the encryption keys provided and fully controlled by Frontex. [18]

3.2. The DPIA

The EDPS notes that significant efforts have been made by Frontex while conducting the DPIA for IRMA 2.0, which as indicated earlier, is a wide-ranging platform. The EDPS is also aware that this is the first time that Frontex has submitted a prior consultation for any of its processing operations, and the process as such is relatively novel. After analysing the DPIA and the accompanying documentation, the EDPS would therefore like to take the opportunity to provide additional guidance on the DPIA process, building both on the EDPS Accountability on the Ground Toolkit[19] and the EDPS' supervisory experience since the entry into force of the EUDPR.[20]

First, the EDPS notes that, despite the IRMA 2.0 platform being designed as a toolbox comprising a number of different functionalities, the DPIA does not describe the lifecycle of the personal data on a tool-per-tool basis. In absence of such a description, it remains at points unclear in which tools risks are supposedly situated. While the EDPS agrees with Frontex that it is important to also describe the risks of IRMA 2.0 as a whole, a more multi-layer analysis may allow Frontex to pinpoint with more accuracy where mitigating measures would need to be applied.

---

15 Threshold assessment, p. 3.
16 Threshold assessment, p. 4.
17 Threshold assessment, p. 4.
18 Threshold assessment, p. 4.
19 Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation, February 2018, available on the EDPS website at https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_2_en.pdf.
20 See, for instance, EDPS case 2021-0747 regarding a prior consultation on the online assessment with remote invigilation in the context of recruitment, publicly available at https://edps.europa.eu/system/files/2021-10/pco_opinion_invigilated_recruitment_anonymised_en.pdf.

Example:

Part II. B. of the DPIA report (Risk Assessment: Assessing likelihood & impact), contains a matrix indicating whether (yes/no) certain principles of data protection may be affected by IRMA 2.0 as a whole. Among these principles, Frontex has indicated that the processing operation may cause discrimination for returnees and those voluntarily returning, however this is not further expanded upon. Equally, the risk indicated by Frontex that this processing operation would decrease the likelihood that returnees and those voluntarily returning exercise their fundamental rights is not further analysed. Here, further questions are:

A. Which modules of the IRMA 2.0 platform cause discrimination risks for the data subject?
B. At which points of the personal data lifecycle in the module are these discrimination risks introduced, and how do the mitigating measures reduce these risks?[21]
C. How do the different functions of IRMA 2.0 affect the possibility to exercise fundamental rights? How can this be reasonably mitigated?

The EDPS notes that the flowcharts included in Frontex' presentation of 30 November 2021 already contain a high-level overview of the personal data lifecycle in some modules. The EDPS encourages Frontex to build on these diagrams as a basis for its process descriptions and subsequent risk assessments.

By taking a more granular approach, Frontex will likely be able to identify more specific risks to data subjects within the different tools, allowing the Agency to apply tailored solutions. While Frontex' general approach of following data protection principles (fairness, accuracy, data minimisation, ...) can be a good way to structure the different risks of IRMA 2.0 and its modules, these risks should then also be listed and scored for each of the categories and tools.

As regards the scoring methodology, the EDPS notes that Frontex performs an initial (pre-mitigation) scoring of the risks by assigning a numerical score (out of 4) to the data protection principles at risk of being infringed. Based on the DPIA report, the EDPS understands that a score of 3 or 4 would indicate a 'high' risk (as a score of 3 is described as 'significant', and a score of 4 as 'maximum'). The DPIA report considers that a significant likelihood and impact of infringement exists for the principles of storage limitation and security - in particular, when it comes to cloud storage.

While the DPIA report lists mitigating measures for each of the data protection principles at risk for infringement, it does not score the residual risk level after mitigating measures have been applied (i.e. whether all risks have been reduced to 'level 0', or whether limited risks remain). The scoring of the residual risks is important not only in the context of the DPIA process itself, but also specifically to assess the need for prior consultation.

The EDPS also reiterates that it remains unclear whether Frontex plans to update this DPIA report (or conduct additional separate DPIAs) for features that are to be integrated into IRMA 2.0, but are not defined at this stage (such as the communication infrastructure with the RECAMAS).

[21] It may be that the risks cannot be reduced to an acceptable level, in which case management should formally accept them, in line with the accountability principle. In any case, Frontex should clearly document that it accepts the residual risks after applying mitigating measures.

3.3. Need for prior consultation and scope of the Opinion

Article 40(1) of the Regulation provides that the controller must consult the EDPS prior to processing where a DPIA under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to 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 (own emphasis)[22].

In the DPIA report, Frontex has established that the use of Cloud Service Providers would, in the absence of mitigating measures, result in such a high risk. However, the DPIA report does not establish that this high risk cannot be reduced in a reasonable way - or what the level of residual risk is after applying mitigating measures. For future prior consultations, the EDPS urges Frontex to calculate the residual risks as well in order to substantiate the need for prior consultation.

The opinion of Frontex' DPO on the DPIA[23] identifies three aspects in IRMA 2.0 that may have a significant impact on the rights and freedoms of the data subjects: the use of cloud services, the implementation of the encryption scheme and the division of responsibilities between the actors on the IRMA 2.0 platform. Even after applying mitigating measures, the DPO considers that prior consultation with the EDPS is still necessary. As such, the EDPS understands that despite the measures identified by Frontex to mitigate risks, they still may not be sufficiently mitigated by reasonable means.

In the context of the prior consultation, the Opinion of the EDPS addresses **the high risks generated by the data processing in the IRMA 2.0 proposal, as described in the notification** of Frontex and the appended opinion of the DPO.

---

[22] See also recital 57 of the Regulation, in fine: "[w]here types of processing operations involve using new technologies, or are of a new kind in relation to which no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing… a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation" and recital 58 of the Regulation: "Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to 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 terms of available technologies and costs of implementation, the European Data Protection Supervisor should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which could result also in a realisation of damage or interference with the rights and freedoms of the natural person…"

[23] DPIA report, sheet 10, row 3.

4. LEGAL AND TECHNICAL ASSESSMENT OF THE MITIGATING MEASURES IDENTIFIED IN THE DPIA

4.1. Regarding the division of responsibilities between the actors in the IRMA 2.0 platform

As part of the prior consultation, the EDPS was asked for its Opinion on the division of tasks and responsibilities between the actors operating in the IRMA 2.0 platform. While initially marked as a separate consultation, the EDPS was subsequently asked to treat the allocation of controllership as part of the prior consultation, highlighting the lack of clarity on this aspect as high risk for the data subject, particularly in relation to the exercise of his/her rights.

The EDPS notes that the primary purpose of the prior consultation procedure is for controllers to seek the Opinion of the EDPS on specific high risks that cannot be reasonably mitigated. The qualification of actors as (joint) controllers or processors generally should not be seen as such a risk, as it is a mandatory element to be provided under Article 40(3)(a) of the Regulation.[24] This question should thus be treated as a pre-requisite for the risk assessment, as additional risks for the rights and freedoms of data subjects may stem from the allocation of responsibilities.

Regardless, the EDPS agrees with Frontex that it is vital to perform the qualification exercise in sufficient detail, prior to the entry into operation of IRMA 2.0.

In this respect, the EDPS notes that Frontex has qualified itself as a controller for 'all processing operations in both IRMA and FAR'.[25] However, as indicated before it has not included a detailed description of the different responsibilities of the actors for each purpose of the platform - which would enable the EDPS to formulate his Opinion on all respective qualifications of other users as processors or (joint) controllers.

The Agency's position on the FAR modules is that controllership would be shifted from the Member States to Frontex from the moment the Member States insert the data in FAR, even though in parallel the Member States continue using FAR for their activities (incl. transfer of personal data to the third countries etc.). Therefore, the Agency sees itself and the Member States acting as parallel controllers, with Frontex being responsible for processing of personal data in FAR itself.

Article 49 of the EBCG Regulation on Information exchange systems and management of returns mandates Frontex to operate and further develop [in accordance with Article 48(1)(d)] an integrated return management platform for processing information, including personal data transmitted by the MS return management system, that is necessary for the Agency to provide technical and operational assistance. Article 49 of EBCG Regulation also defines a series of data protection safeguards that frames the kind of processing activities that can take place on the platform. The development of IRMA thus serves this primary purpose.

---

[24] When consulting the European Data Protection Supervisor pursuant to paragraph 1, the controller shall provide the European Data Protection Supervisor with:
(a)where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing; [...]

[25] DPIA report, sheet 10, B3.

Article 3(8) EUDPR provides that "controllers" means the Union institution or body or the directorate-general or any other organisational entity which, alone or jointly with others, determines the purposes and means of such processing of personal data. Where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law.

In the case of IRMA 2.0, while the EBCG Regulation does not explicitly appoint Frontex as controller or provide criteria for the nomination of the controller, it does entrust Frontex with the task of operating and developing a system that will allow Frontex to fulfil its tasks in the field of returns, including to support to MS or to organise and coordinate returns operations.

It thus appears that the primary purpose of IRMA 2.0 is to enable Frontex to fulfil its mandate and to enable Frontex to provide technical and operational assistance to MS, i.e. to give effect to one of its tasks under the EBCG Regulation (see Art. 10(1)(n)). As such, Frontex is operating and developing a platform for its own purposes (as defined above), which are not jointly determined with MS. Generally, Frontex should thus be considered as a sole (or parallel) controller of processing activities taking place in the context of IRMA 2.0.

However, the responsibilities of Frontex may be more limited where it solely facilitates the exchange of bilateral encrypted messages between other authorities. The EDPS has taken note that Frontex does not foresee to have any access to the content of the encrypted messages it is not involved in.

In that context, the EDPS highlights the EDPB Guidelines 07/2020,[26] which tackle, among others electronic communication providers. The provider of such services will normally be considered a controller in respect of the processing of personal data that is necessary for the operation of the service as such (e.g., traffic data). If the sole purpose and role of the provider is to enable the transmission of email messages, the provider will not be considered as the controller in respect of the personal data contained in the message itself. The controller in respect of any personal data contained inside the message will normally be considered to be the person from whom the message originates, rather than the service provider offering the transmission service.

As the EDPS has only limited information available on the future operation of the encrypted messaging service, it cannot take a conclusive stance on this element. However, the EDPS remains available to provide further guidance on the topic in follow-up to this prior consultation.

EDPS recommendations:

Frontex should re-assess the risks to data subjects on the basis of a clear allocation of the roles and responsibilities of the actors for each purpose of IRMA 2.0.

[26] Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0 Adopted on 07 July 2021,https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf, in particular page .

4.2. Regarding the significant risks identified in using public cloud services

The DPIA informs about Frontex' intention to use several different types of public cloud computing services to support the IRMA system, in particular Microsoft Azure, Microsoft SharePoint Online and Microsoft 365.

However, the references to public cloud services are not sufficiently explanatory about how they are meant to be used and what specific personal data will be processed in each one of them.

The EDPS also considers that some of the references are open to different interpretations, as is the case of the stated in section "Part I – Introduction" of the DPIA, which indicates that Frontex plans to use Microsoft Azure cloud as a business continuity solution, configured to have data stored exclusively on the EU:

The personal data is kept in the platform database. The servers of the platform are to be located at Frontex premises or on the Cloud. By principle cloud services are designed to be globally speeded, decoupled and highly available. This contradicts the requirement of personal data residency where data have to be placed in European Union in order to effectively enforce Data Protection regulation. To comply, the place where Frontex data is stored is set to EU.

Data centre in Cloud

Frontex is going to create a hybrid environment and extend the current on premise infrastructure that is based on VMWare for additional VMWare-enabled Data Centre located on public clouds provided by Microsoft Azure Cloud. Using VMWare clouds on Azure will enable Frontex to ensure business continuity (in case of disaster) and providing required resources and capacity for onboarding new business solutions defined by the regulation EBCG 2.0

Frontex is going to use Azure VMWare Solution. This is the service that provides dedicated and encrypted VMWare hosts located in Azure Data Centre that can be used as an extension of the current Data Centre and managed from the same management tools that are used in on premise environment. All Frontex data stored on these hosts would be encrypted by the encryption keys provided and fully controlled by Frontex.

The EDPS considers unclear what is meant with the references to the "extension" of local VMWare systems to the cloud, or to the use of Azure cloud to provide "required resources and capacity for onboarding new business solutions". Both expressions are vague regarding which personal data will be processed in the cloud. It is not clear either whether the use of the cloud-based solution will only cater for business continuity or will be used also for normal operations.

Furthermore, "Part III – Risk Treatment" of the DPIA informs that "[p]ersonal data can be inaccessible due to a technical malfunction in the SharePoint Online authentication mechanisms". More references to SharePoint Online are made in the same part of the DPIA within the "Proposed ICT controls". It is not clear what the role is of SharePoint Online in the future IRMA system.

Regarding the storage of data in the EU, the EDPS is aware that Microsoft Azure has been implementing its "data residency"[27] service, with the intention of giving customers the

[27] More available at https://azure.microsoft.com/en-us/global-infrastructure/data-residency/.

possibility to choose the geographical region where their data will be deployed, including the use of European-based datacentres.

However, since Microsoft is a U.S.-based technology company, it might be instructed to provide governmental access to the based on the Clarifying Lawful Overseas Use of Data Act (also known as the Cloud Act). This is a scenario that was not put aside in 2021's Microsoft white paper, "Enabling Data Residency and Data Protection in Microsoft Azure Regions"[28].
The EDPS considers that the privacy risks of access to data stored in the cloud services in the context of the Cloud Act must be assessed in the DPIA, also because the data involved could be related to vulnerable natural persons, such as returnees. Such an assessment has not been documented out in the received DPIA report.

In summary, the **EDPS considers that the DPIA is ambiguous regarding the objective of using cloud systems in the current data processing, and further clarifications is needed on the role of cloud systems in Frontex strategy**, in particular as relates to their use in Frontex core tasks and the processing of operational data. This limits the current assessment of relevant data protection risks.

Additionally, with a view to possible conflicts of jurisdiction with countries not offering an equivalent level of data protection, the risks of processing personal data in public could systems provided by US-based companies, such as Microsoft, are not sufficiently addressed, also considering that there might be personal data related to vulnerable natural persons.

It is worth mentioning that the EDPS is already carrying its own-initiative investigation into the decision of the European Border and Coast Guard Agency (Frontex) to move IT services into the cloud (consisting of Microsoft Office 365, Amazon AWS and Microsoft Azure). This investigation is still ongoing.

The EDPS believes it is essential that Frontex take a holistic and coherent approach in the overall cloud strategy and its impact on the protection of privacy and personal data.

EDPS recommendations:

Frontex should further clarify which public cloud computing platforms will be used, which functionalities will be used, what personal data is going to be processed in them, and how they will interact with each other and the Frontex systems.

Frontex should further clarify what it means when referring to the "extension" of local systems to the cloud.

Frontex should update the DPIA in order to clearly address the risks of using public cloud services, namely the possible accesses based on the Cloud Act.

[28] Available at https://azure.microsoft.com/mediahandler/files/resourcefiles/achieving-compliant-data-residency-and-security-with-azure/Enabling_Data_Residency_and_Data_Protection_in_Azure_Regions-2021.pdf.

4.3. Regarding risks of the proposed encryption scheme

The "Introduction" section of the Frontex DPIA[29] refers the following about the use of encryption in the IRMA system:

> (...) *personal data of returnees may* (our underlining) *be exchanged via the encrypted communication for identification purposes. The transfer of encrypted files is done directly between the users, with no intermediaries being involved. Frontex does not have the technical or legal means to decrypt the encrypted files. On a practical level, the users will create their own password and the PGP keys will be stored in the IRMA servers (with no possibility for Frontex to access them). In addition, when a file is decrypted by the recipient, a message will display informing the user that the decryption of the file was completed and the download of said file is possible (only to the recipient of the encrypted file). The users will be responsible for the creation and management of the passwords and the resetting of the passwords is not possible (once forgotten or lost, a new password will need to be created by the user).*

The "Record of processing activity on personal data for data controllers" for the processing activity of IRMA[30] particularly specifies that the encryption mechanism can be used for the exchange of personal data of Third Country Nationals (TCN):

> (...) *the users will be able to communicate via an internal messaging system to send/receive encrypted files that may include personal data of Third Country Nationals (TCN) in the context of a return procedure. The purpose of this component is to facilitate EU-cooperation in the context of particular return cases, while safeguarding the data protection rights of the TCNs.*

According to the document "*Integrated Return Management Application (IRMA) – Encryption of Exchanged Files*"[31], Frontex will implement the exchange of encrypted information by using Pretty Good Privacy (PGP) certificates arranged in a Web of Trust (WoT)[32]. The WOT, however, will have IRMA acting as a central Certification Authority (CA)[33] and verifying the authenticity of each of the PGP certificates.

However, since PGP certificates are not issued by Certificate Authorities, Frontex evaluates two options for the creation of the certificates: user-initiated (where each user makes generates its own certificate) or IRMA-initiated (where IRMA creates the certificate for each user, and delivers the correspondent Private Key to the user). In the document, Frontex describes the problems stemming from each option[34], and concludes that the second option presents no benefit in terms of complexity and user experience and convenience with respect to the user-initiated scheme and does not adequately address the security requirements,

---

[29] Sheet 1, B7.

[30] Document "IRMA 2.0 Record v0.6", received in the same email of the previous reference.

[31] Document sent by email on 01/12/2021 by the Frontex DPO to the EDPS elements that were present in the IRMA presentation held online on 30/11/2021.

[32] A decentralized trust model, alternative to the centralized trust model of a public key infrastructure (PKI) which relies exclusively on a certificate authority. In the WoT every user establishes a "direct trust" link with the users it trusts and "indirect trust" links with users which are trusted by its direct trust links.

[33] Certification Authority - A trusted organization that validates the identities of entities (such as websites, email addresses, companies, or individual persons) and bind them to cryptographic keys through the issuance of electronic documents known as digital certificates.

[34] The former being the need for the users to submit their self-generated Public Keys to IRMA and having them authenticated centrally, and the latter, the risk for confidentiality stemming from the fact that IRMA will have knowledge of every user's Private and Public keys.

therefore opting for user-initiated certificates.

Because the authenticity of self-certificates cannot be verified by a CA[35], Frontex proposes to have a "physical identification" of every user accessing the IRMA platform:

> *As a matter of fact, IRMA can be considered as a perfectly efficient solution for these purposes, since the physical identity of the IRMA users is thoroughly examined both during their initial application and periodically, while IRMA offers a secure environment for sharing the Public keys. Hence, it is not necessary to resort to the issuance of certificates from a third-party RCA for guaranteeing the authenticity of the Public keys, but IRMA can provide this functionality in an utterly reliable manner.*

In the perspective of the EDPS, the encryption solution proposed by Frontex raises certain security risks which have not been identified in the DPIA.

The first risk is the possibility of unauthorized disclosure of sensitive data, in situations where users might exchange encrypted messages with other users believing they (still) have valid certificates - when in reality they don't. Although this risk would be easily solved in a Public Key Infrastructure (PKI) (where the CA has the ability to revoke the certificates of untrusted users), in the current context it is not clear how IRMA will ensure the certificate revocation. According to the documentation provided, IRMA will act as "limited" CA, ensuring the verification of the identity of the users when they upload their public keys, and making the validated public keys available to all users. However, there is no description about how IRMA will revoke PGP certificates (or invalidate public keys) of users whenever needed.

The EDPS considers that certificate revocation is an element necessary for the security of any PKI infrastructure and, for that matter, the data controller should clearly define how this feature will be implemented in IRMA.

Also, encryption of the information should be embedded in the IRMA system, making this security measure easy and effective to use, following the principle of Data Protection by Default and by Design. The fact that users have to go through the process[36] of manually installing third-party software (Gpg4win), generating their OpenPGP private and public keys, exporting their public keys to IRMA and importing the public keys of any other IRMA users with which they might want to share encrypted content with, seems to be a lengthy process that users might be willing to avoid. Therefore, there is a high chance of users not applying encryption on sensitive information, with consequent risk for the confidentiality of data.
The proposed encryption scheme has IRMA users at its core, and certain details of the self-generation of certificates are left at their discretion (such as the structure of the secret passphrases or the security measures for the storage of the private keys). Therefore, the way users abide (or not) to the data controller's instructions for the management of certificates can have impact in the strength or the secrecy of the keys, and consequently on the overall security of the communications. The EDPS recommends the data controller to define an "acceptable use policy", to which users should abide, regarding, at least, the use of encryption for the exchange of personal data of returnees and third-country nationals, the

[35] Or by another entity providing information on behalf of the CA, commonly known as a validation authority (VA).

[36] Based on the 16-page guide provided in the "Integrated Return Management Application (IRMA) – Encryption of Exchanged Files" document.

structure of the passphrase, the storage of private keys, and the ways to proceed whenever private keys are compromised.

Ultimately, the decision to encrypt (or not) the transferred information belongs to each user of the IRMA system. From the analysis of the provided documentation, there seems to be no intention from the data controller in making the encryption functionality mandatory and/or, as mentioned above, an integral part of the system. This could lead to users applying divergent approaches on the use of encryption for the transmission of personal data that, again, might result in risks for the confidentiality of data.

EDPS Recommendations:

Frontex should build the encryption functionality into the IRMA system in a way that is easily accessible whenever there is need to apply additional security measures to personal data transfers (independently of the use of encrypted communication channels).

It should be re-examined whether the key management procedure (generation, exchange of public keys and storage of private keys) can be rendered less complex and ensure a more consistent level of security of the system.

5. CONCLUSION AND RECOMMENDATIONS

Based on all of the above, the EDPS is of the view that Frontex has insufficiently identified all of the high risks related to the adoption of public cloud services and the encrypted messaging functionality. Furthermore, the EDPS is concerned that the lack of a clear division of responsibilities as regards personal data processing in IRMA 2.0 may result in an incomplete assessment of the risks to the rights and freedoms of data subjects.

As part of its written advice under Article 40(2) of the Regulation, the EDPS makes the following recommendations to ensure compliance of the envisaged processing with the Regulation.

1. Frontex should re-assess the risks to data subjects on the basis of a clear allocation of the roles and responsibilities of the actors for each purpose of IRMA 2.0.

2. Frontex should further clarify which public cloud computing platforms will be used, which functionalities will be used, what personal data is going to be processed in them, and how they will interact with each other and the Frontex systems.

3. Frontex should further clarify what it means when referring to the "extension" of local systems to the cloud.

4. Frontex should update the DPIA in order to clearly address the risks of using public cloud services, namely the possible accesses based on the Cloud Act.

5. Frontex should build the encryption functionality into the IRMA system in a way that is easily accessible whenever there is need to apply additional security measures to personal data transfers (independently of the use of encrypted communication channels).

6. Frontex should re-examine the key management procedure (generation, exchange of public keys and storage of private keys) in order to identify whether to render it less complex and ensure a more consistent level of security of the system.

Pursuant to Article 59, the EDPS expects Frontex to provide its views and describe the measures it has taken to comply with the Regulation by **1 March 2022**.

6. JUDICIAL REMEDY

Pursuant to Article 64 of the Regulation, any action against this Opinion shall be brought before the Court of Justice of the European Union within two months of its adoption, and according to the conditions laid down in Article 263 TFEU.

Done at Brussels on 16 December 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI