



# EDPS Decision concerning the investigation into Frontex's move to the Cloud

(Case 2020-0584)

## 1. Introduction and scope

1. This decision sets out the results of the EDPS' investigation into the European Border and Coast Guard Agency's (Frontex) decision to move all of its IT services into a hybrid cloud (consisting of Microsoft Office 365, Amazon Web Services (AWS), and Microsoft Azure).
2. The investigation focused on whether Frontex complied with Regulation (EU) 2018/1725 ('the Regulation')<sup>1</sup>, taking into account the EDPS Guidelines on the use of cloud computing services<sup>2</sup> (the 'Guidelines'), and in particular as regards Frontex's obligation to comply with the principle of accountability under Article 4(2) of the Regulation as well as with the obligations under Article 26 ('Responsibility of the controller') and Article 27 ('Data protection by design and by default') of the Regulation.
3. Regarding scope, the EDPS took the decision that the investigation would not include an analysis of the underlying contractual Inter-institutional Licensing Agreement (ILA) for which the European Commission is the lead contracting authority. Moreover, the EDPS decided that the investigation would not include the analysis of Frontex's compliance with the Regulation's rules on data transfers to third countries (as interpreted by the Court of Justice of the European Union (CJEU) in its "Schrems II" judgment<sup>3</sup>). The EDPS decided to assess relevant compliance in the context of other investigations on the use of the same products and services by EU institutions, bodies, offices and agencies targeting, where applicable, the EUI acting as lead contracting authority. This is without prejudice to possible related future supervisory actions on Frontex's use of cloud services.
4. This decision is addressed to Frontex, and is issued in accordance with Article 57(1)(f) and Articles 58(2)(b) and 58(2)(e) of the Regulation.

---

<sup>1</sup> 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; OJ L 295, 21.11.2018, p. 39–98. References to Articles in this document refer to the Regulation.

<sup>2</sup> EDPS "Guidelines on the use of cloud computing services by the European institutions and bodies", 16 March 2018, available at: [https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-use-cloud-computing-services-european\\_en](https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-use-cloud-computing-services-european_en)

<sup>3</sup> Judgment of the Court of Justice of 16 July 2020 in case C-311/18, Data Protection Commissioner v. Facebook Ireland LTD and Maximilian Schrems ("Schrems II"), ECLI:EU:C:2020:559.

## 2. The investigative actions

### 2.1. Opening of the investigation

5. The EDPS opened his investigation on 12 June 2020, following the receipt of a letter on 28 May 2020 from Frontex's Executive Director, Mr Leggeri. The letter concerns developments taking place at Frontex, and in particular the decision to "*move all Frontex services into the Cloud*". The letter justifies this decision by citing the need to support Frontex's current tasks as well as future tasks mandated by the new Frontex Regulation, which entered into force on 4 December 2019.
6. In the letter, Mr Leggeri explains that the decision was to "*use a hybrid cloud model that will consist of Microsoft Office 365, Amazon AWS and Microsoft Azure*". He further explains that "*Frontex is taking a graduated approach, and the first step is the implementation of Office 365. The infrastructure is in place since 21 May. Tests are being conducted as from 25-29 May. From 29 May onwards Frontex will be operational on the Cloud.*" Mr Leggeri goes on to add that, "*given the time constraints we are facing to deliver, the Record and the Data Protection Impact Assessment are not yet finalised. Thereupon, Frontex will roll out Office 365 before being able to prior consult with you, as per Article 40 of the EUDPR. Nevertheless, I want to assure you that Frontex is working on the completion of the documents and will be able to conduct ex post prior consultation on well prepared and complete documentation*".

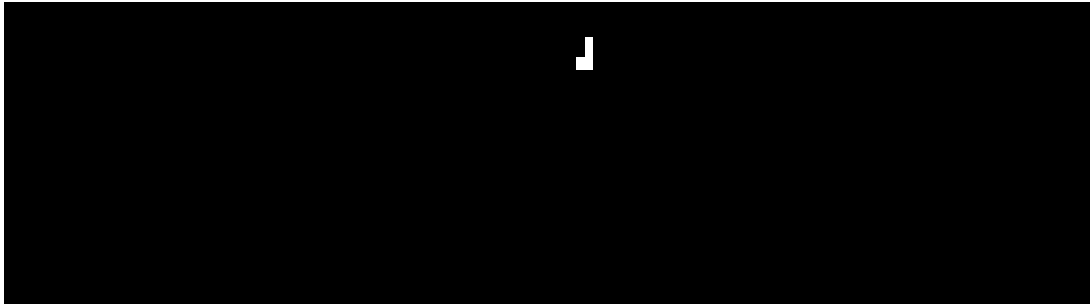
### 2.2. EDPS information requests and documentation/support provided by Frontex

7. Upon opening the investigation, the EDPS requested from Frontex: background information on the project, including its scope, planning, relevant technical documentation, any assessment of relevant data protection and security risks and used methodology, any technical and organisational measures planned or taken to mitigate those risks; the data protection impact assessment (DPIA) documentation as well as any data protection records based on Article 31 of the Regulation; information on any processing of personal data in the Cloud in the context of operations pursuant to the Frontex Regulation; and any measures to mitigate the data protection risks of operational data.
8. Frontex provided a first package of documentation on 26 June 2020, within the EDPS' set deadline. Frontex provided the DPIA and the record of processing activities ('the Record'), which the EDPS expected to receive by 12 July 2020 latest, on 11 September 2020.
9. The EDPS had planned a visit to Frontex's premises to gather on-site evidence on possible personal data flows from locally installed Microsoft applications in the context of the investigation. The situation linked to the COVID-19 pandemic did not allow for such a visit. Instead, in its letter of 12 June 2020 the EDPS asked Frontex to "*provide a laptop with standard configuration, settings and tools used by Frontex staff. The laptop should be configured with a standard Frontex setup, including installation of the versions of Microsoft products and services currently used by Frontex staff and those that will be used by the newly recruited operational staff. The laptop should have installed any tools used by Frontex to test the flows of personal data, including those to Microsoft. The EDPS is to be provided with a user profile for the laptop so that the investigation team may perform the necessary verifications and checks.*"

10. Frontex supported the EDPS audit with the rapid delivery of a laptop device for testing. However, Frontex decided to provide the EDPS with a device that did not comply fully with the EDPS's request. This is because the device offered only standard software, instead of software comprising "*any tools used by Frontex to test the flows of personal data*". Frontex stated that it was not in line with their IT security policy to install such tools on an administrative laptop connected to their network and to give EDPS staff administrative rights on that machine. As a result, the EDPS staff were unable to set up a test environment in the EDPS lab and capture the traffic exiting a laptop using Frontex's standard configuration. This is because Frontex' laptops establish a Virtual Private Network connection via an encrypted channel with Frontex's data centre, which prevents the analysis the data flows in clear text.
11. By not fully complying with the EDPS's initial request, and by not granting the EDPS staff full administrative rights on the laptop provided, Frontex has prevented the EDPS from obtaining access to all of Frontex's data processing equipment and means, in accordance with Article 58(1)(e) of the Regulation.
12. In order to advance the investigation, the EDPS audit team agreed to an evidence collection carried out by Frontex's staff under the EDPS remote supervision.

### **2.3. Procedure for the collection of data flows from a Frontex's laptop due to the use of Microsoft products and services**

13. On 3 December 2020, during a video call with EDPS investigators, Frontex collected evidence on data flows related to the use of Microsoft products deployed on a Frontex standard laptop. Frontex sent the EDPS the recorded data and the relevant documentation on 29 January 2021.

14. 

15. 





---



- opening, editing and saving a document with Word.

#### **2.4. Frontex announcement of full Microsoft 365 deployment**

16. On 1 February 2021, Frontex’s Executive Director communicated that the Agency had already “*deployed two thirds of Frontex users into the Microsoft 365*” and that “*in order to achieve desirable ICT services capacity, and to implement operational protection measures.*” Frontex had planned “*to reduce the volume of data processed in the on-premise infrastructure in favour of the usage of the M365/O365 services listed in the provided Record of Processing for all its users*” by 22 February 2021.

#### **2.5. EDPS preliminary analysis and Frontex reply**

17. On 15 July 2021, the EDPS sent Frontex’s Executive Director a letter establishing the end of the fact-finding phase of the investigation and presenting a preliminary analysis and consequent relevant conclusions. With the letter, the EDPS wished to provide Frontex with the opportunity to submit observations on the preliminary analysis, in particular on the facts mentioned therein, before any possible enforcement actions.
18. On 24 September 2021, Frontex’s Executive Director replied to the EDPS’s letter. In his reply, the Executive Director, in particular:
- repeated that the move to the cloud was made “*... in a very challenging situation to implement its new mandate, in the midst of the still ongoing Covid crisis... without the possibility of a timely consultation with your services but nevertheless fully informing you about this*”;
  - said that this exceptional situation “*... should not be reiterated in the following steps of our gradual move to the Cloud, in alignment with our ICT Cloud Implementation Plan 2020-2025*”
  - communicated that he took “*...note of your investigation’s outcome*” and that he “*... already proceeded to take corrective action internally, first and foremost by fully engaging our DPO. She will promptly inform the controller in practice of any developments at EU level and advise on the compliance of Frontex activities, considering your recently opened investigation against the Commission, and the ongoing discussions in different data protection workshops on international data transfers*”; and,
  - provided Frontex’s comments to the EDPS’ preliminary findings.
19. The EDPS has carefully assessed the letter and taken into account Frontex’s comments on his preliminary findings.

### **3. Factual background**

20. The purpose of this section is to describe all factual findings relating to the situation at the date of the opening of the investigation, while also taking into account documentation provided and tests made after that date using the services and products that were deployed at the time.
21. For his final assessment of whether there has been an infringement of the Regulation, the EDPS has not taken into account any evolution of the situation after the investigation

opening date. The EDPS has taken these actions into account when deciding which corrective powers to use as they could be treated as a mitigating or aggravating factor.

### **3.1. On the approach to the cloud computing option, the responsibility of the controller and data protection by design and by default**

#### **3.1.1. Considerations on the sequence of events in the context of the assessment of the data protection risks**

22. Based on what is reported in Frontex's DPIA on Office 365<sup>5</sup>, Frontex's decision to adopt cloud services was taken during an IT Change Advisory Board session on 26 March 2020, and rolled out in production on 28 May 2020. Frontex reported that it had originally sent the DPIA and the Record to the DPO for consultation on 23 March 2020. However, the final draft of the DPIA is dated 1 July 2020 and the final *official* version of the DPIA is dated 3 September 2020 and was not available when originally requested by the EDPS.
23. Frontex's Executive Director adopted the 'Frontex ICT Cloud Implementation Plan 2020-2025 for unclassified information' on 26 June 2020. The plan was therefore adopted after the investigation was initiated and after Frontex had commenced its move to the cloud. Frontex describes the ICT Cloud Implementation Plan as "*one of the fundamental elements in the implementation of the ICT Operational Plan 2020-2025 (adopted by decision of the Executive Director No R-ED-2020-54 of 25/03/2020)*"<sup>6</sup>. The ICT Operational Plan 2020-2025, adopted on 26 February 2020, of which the ICT Cloud Implementation Plan is part, already provided for the move to the cloud for unclassified data, including personal data.

#### **3.1.2. The assessment of data protection risks**

24. Regarding the processing activities falling within the scope of this investigation, the ICT Operational Plan and the ICT Cloud Implementation Plan describe very high level data flows. The plans identify the different types of actors at operational level (Headquarter's staff, Standing Corps, Antenna Offices, Liaison Officers, EU Bodies, Member State's administrations etc.), and whether there are flows of data to cloud services or not. They do not identify the data flows (including a description of data categories) relevant to Frontex's business processes, i.e. the activities that Frontex carries out for the accomplishment of its tasks..
25. Section 2.6 of the DPIA states that the "*Extent of information allowed to be processed and stored in cloud services is up to the level SENSITIVE NON-CLASSIFIED (SNC) as per Security Notice Information assessment and classification (Brussels, 5.3.2019 C(2019) 1903 final). EU Classified Information is not allowed and excluded from the scope.*"
26. The DPIA also lists in section 2.6 what it calls the "*Processes envisaged to be supported and run in the cloud*"<sup>7</sup>. These are the functionalities enabled by the adopted Microsoft products

---

<sup>5</sup> "Data Protection Impact Assessment (DPIA) for Office365, Data Centre and Software Development in the Microsoft Azure", page 9

<sup>6</sup> "Frontex ICT Cloud Implementation Plan 2020-2025 for unclassified information", page 4

<sup>7</sup> These are:

- *Identity and access management (Active Directory, multifactor authentication and access policies)*
- *Documents exchange by emails (Exchange Online/ Office Pro Plus Outlook)*
- *Instant messaging (Teams)*
- *Collaboration services (SharePoint Online)*
- *Storage of the documents (OneDrive for Business)*
- *Data Center (Microsoft Azure VMware Solution)*

and services. What the DPIA defines as “business processes” are listed at DPIA section 3.9. These are described in more detail in section 3.10, and are referred to in the risk assessment in section 5, as well as in the Excel sheet annexed to the DPIA. These “business processes” include IT development, deployment, operations and maintenance activities, IT security activities as well as other activities (such as: collaboration and file exchange, the conduct of virtual meetings and conference calls, chat based collaboration, exchange of e-mails) possibly enabling Frontex’s core and supporting tasks. However, the “business processes” do not describe the nature of the processing activities (collaboration and file exchange, for example, can take place while processing public information or on special categories of data and for specific purposes linked to Frontex’s tasks).

27. The only place in the DPIA where there is some reference to the nature of the processing activities to be supported by the envisaged cloud products and services is section 2.7. These processes were identified by the ICT Unit using Frontex Service Catalogue “*because of the very wide scope of the information to be potentially processed by the assumed cloud services ... to define DPIA scope and what can be processed/stored in envisaged cloud services*”. Frontex describes these processes as:

- “*Personal data used for employment lifecycle – regular employer-employee relation*”;
- “*Personal data of external experts / contractors*”;
- “*Personal data provided by the user on private usage on their own accord, voluntarily*”;
- and
- “*Personal data required for management and communication data (user identification, access management, security)*”.

28. This description is, as also signaled by Frontex, not exhaustive in describing all categories of personal data to be processed in Microsoft cloud services but represents a sample of them.

29. The Record, meant to account for the processing of personal data by Microsoft products and services, called titled “*Office 365 cloud platform, Data Center hosting in Azure, Azure DevOps developer services*”, mentions the following purposes:

- “*Providing identity and access management services*”;
- “*Documents exchange, messaging and collaboration services, storage of the documents, and Data Center and software development*”; and
- “*Providing mechanisms for automatic data classification and applying policies according to the type of data*”.

The Record does not give any further detail on the processing activities.

30. As to applications that could be deployed to the Microsoft Azure Cloud and the processing of personal data therein, the DPIA states: “*Extend to which this DPIA covers Data Center in the Azure Cloud is restricted to fundamental services like: access and identity (Active Directory, access rules), virtual networks, virtualization platform, backup, logging, security services. Each distinct application to be embedded in the cloud Data Centre, if*

- 
- *Software development (DevOps server for software development)*
  - *Data classification (Azure Information Protection)*
  - *Applying policies according to the type of data (Azure Information Protection)*

*contains or processes personal data, has to be assessed and accepted by respective data controller before moving application from on premises to the new cloud Data Center”.*

31. The EDPS understands that the DPIA did not cover any plans for possible deployment of cloud-based processing activities in supporting specific business processes in Azure. The EDPS takes the opportunity to clarify that any planned deployment of applications to the Cloud by Frontex using Microsoft Azure Cloud would be in scope of this investigation.
32. The EDPS also understands from the DPIA<sup>8</sup> that Frontex had not planned to support any activities processing core business or “operational personal data”<sup>9</sup> via the identified cloud services at the time that the DPIA was approved.
33. The analysis of the data protection risks Frontex carried out is described in chapter 5 of the DPIA and in its Annex I (Excel file). Section 6 integrates an IT security risk assessment.
34. In particular, section 5.3 summarises a risk mitigation plan and section 5.4 reports 13 residual risks that have been “accepted” (not mitigated) including the rationale for each acceptance. Annex I of the DPIA describes the detailed assessment process and the resulting risk mitigating actions or risk acceptance rationale.

### **3.2. On the demonstration of necessity to adopt Microsoft cloud solutions**

35. Frontex identified the need to move to the Cloud and adopt Microsoft solutions to support its strategic objectives, including the required capacity to support hundreds of new staff for the Standing Corps to be deployed throughout Europe and third countries, as well as for better effectiveness and efficiency in supporting Frontex’s “*critical business needs coming from the EBCG Regulation 2.0*”<sup>10</sup>.
36. Frontex did not provide the EDPS with any evidence of having investigated possible alternative solutions to Microsoft ones, despite the existence, before the completion of the assessment, of elements indicating a meaningful level of risk of non-compliance in the solutions chosen, in particular the EDPS own-initiative investigation into EU institutions’ use of Microsoft products and services<sup>11</sup>.

### **3.3. On Microsoft’s collection of personal data from Frontex’s user devices and at the server side**

37. At the date of the EDPS investigation, Frontex did not have at its disposal a sufficiently fine-grained configuration at application administration level enabling them to switch off as necessary the collection and processing of diagnostics data for Windows 10 and Office Pro Plus. As a result, Frontex relied on a layered approach for its implementation of technical measures to prevent undesired collection of personal data<sup>12</sup>.
38. This approach included, further to the available Windows 10 and Office diagnostics configuration related features, a manual configuration of local workstation files as well as a dedicated configuration of internet proxy servers, firewalls and DNS servers. These

---

<sup>8</sup> Section 2.7 of the DPIA

<sup>9</sup> See definition of “operational personal data” in Article 3(2) of the Regulation.

<sup>10</sup> From “Frontex ICT Cloud Implementation Plan 2020-2025”, section 2.

<sup>11</sup> The EDPS issued its findings and recommendations to all EU institutions, offices, bodies and agencies upon the closure of its investigation in March 2020.

<sup>12</sup> [REDACTED]

configurations allowed Frontex to block the sending of data to specific domain names (identifying remote servers managed by Microsoft or possible subcontractors). Frontex identified the domain names to block using information provided by many sources, including Microsoft technical documentation and reputable security advisory sources.

39.



40.



41. The DPIA in section 3.4 describes personal data processed by Microsoft 365 and covered by the applicable contractual terms. They include “service generated data”, i.e. data generated or derived by the use of Microsoft cloud-based applications (e.g. Office 365), collected by Microsoft at their servers and further processed for their use.
42. We could not find any description of the categories of personal data collected as “service generated data” nor any reference to them in the analysis of the risks.

## **4. Legal assessment**

### **4.1. On the approach to the cloud computing option, the responsibility of the controller, and data protection by design and by default**

43. In accordance with Article 86(1) of Regulation (EU) 2019/1896, Frontex is obliged to apply the Regulation when processing personal data.
44. Article 4(2) of the Regulation (‘accountability principle’) requires the controller to be responsible for, and able to demonstrate compliance with, the data protection principles laid down in Article 4(1). Article 26 also requires the controller to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation, taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons.
45. Article 27 requires the controller to implement the principle of data protection by design and by default, including by, among other things, selecting effective measures to integrate the necessary safeguards into the processing and implementing those measures both at the time of the determination of the means for processing and at the time of the processing itself.

---

<sup>13</sup> Ibid. section 8, “Reactive blocking of telemetry”.

<sup>14</sup> See section 6 of the document “Telemetry and Data Privacy rules on Workstations at Frontex” version 2, dated 01/2021,



46. The Guidelines provide practical advice and indicate best practices, in particular in section 3.1 of chapter 3 (Planning for procurement of cloud computing services) and in section 4.1 (Assessing the data protection appropriateness of a cloud service).
47. These obligations and guidelines apply to the Agency in its planning and decision to procure cloud-computing services.
48. The “Frontex ICT Cloud Implementation Plan 2020-2025 for unclassified information” adopted on 26 June 2020 states, *inter alia*, that:

*“All data processed and stored in the clouds needs to be encrypted and have to be located in Data Centres co-located in EU and excluded from jurisdiction of local governments (need to exclude usage of clouds that are under control of local governments). Frontex also will meet of the following EDPS’s recommendations described in “Guidelines on the use of cloud computing services by the European Institutions and Bodies”:*

- *Data and used assets must geographically reside on European territory,*
- *Algorithms and analytics must also be run in Europe,*
- *Providers must accept audits from the main EU bodies.*

*The Frontex cloud model and its implementation must be in line with Regulation 2018/1725.”*

#### **4.1.1. Considerations on the sequence of events in the context of the assessment of the data protection risks**

49. The methodological steps proposed in the Guidelines, in line with Articles 4(2), 26 and 27 of the Regulation, state that the cloud computing option and the choice of the suitable service and contract/contractor depend on the outcome of the assessment of data protection risks, which should precede any subsequent actions. In other words, Frontex should have concluded its assessment of the data protection risks before taking the final decision to process personal data in the cloud.
50. The considerations on the sequence of events of section 3.1.1 demonstrates that even though the Agency was aware of and had already commenced the necessary activities to comply with the Regulation when it took the decision to process personal, non-classified data in specific cloud-based services, it decided to adopt those services just three days after sending the draft DPIA (and the Record) to the DPO for consultation. It also went to production several months before acknowledging the final results of the assessment of data protection risks.
51. Frontex’s move to the cloud includes the use of both cloud-based Microsoft products and services and of Amazon Web Services (AWS). However, Frontex did not provide any documentation demonstrating an assessment of whether the relevant AWS would allow for a processing of personal data in compliance with the relevant rules . Nor did Frontex send any Records referring to the use of AWS.

52. The EDPS therefore assumes that Frontex had not planned any processing activities based on AWS on the date that the EDPS opened the investigation. An assessment of the data protection risks linked to the use of AWS, as well as references to AWS in relevant records of processing activities, are necessary before any processing of personal data on AWS takes place.

#### 4.1.2. The assessment of data protection risks

53. Overall, the final DPIA shows lack of clarity regarding the nature of the processing activities under its scope.

54. The list of processes in section 2.7 of the DPIA only partially describes the activities involving the processing of (personal) data. It is not clear, for example, whether all kinds of human resources related activities (i.e. management of the staff member's personal file, staff performance assessments, exchange of possible medical or other sensitive information for special leave management, staff security clearances etc.) are in scope, or what the processing activity is that involves external experts' data.

55. It is thus not possible to relate all of the risks that Frontex identified to all of the activities involving the processing of personal data that it planned to support via Microsoft services. Frontex also did not sufficiently elaborate on those activities with a view to a risk assessment.

56. The processing activities described in section 2.7 of the DPIA do not correspond with those declared in the Record provided to the EDPS, either, which, as in the risk assessment within the DPIA, are identified as mere IT functionalities (e.g. document exchange and storage). Moreover, the Record does not clearly describe the nature, scope, context and purpose of the processing activities to be supported by cloud products and services. For example, the Record does not provide detail on what activities are supported by the documents exchanged through the products and services in scope.

57. The assessment of the risks to the rights and freedoms of natural persons, as provided for in Article 26 of the Regulation, should be based on the Agency's core and supporting tasks which the IT products and services are meant to support. In particular, the assessment should refer to the relevant data processed, the concerned data subjects, the recipients, the nature and purposes of the processing activities, and the context of these processing activities.

58. This lack of clarity on the nature of the processing activities in scope and partial contradiction between what appears in the Record and in the DPIA undermines the value of the assessment of data protection risks.

59. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]


[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



### 4.1.3. Conclusion on the approach to the cloud computing option, the responsibility of the controller and data protection by design and by default

60. The considerations made in sections 4.1.1 and 4.1.2 lead together to the conclusion that the Agency did not demonstrate sufficiently to the EDPS that it had identified and implemented the appropriate measures to ensure compliance with the Regulation on the basis of an adequate assessment of the risks to the rights and freedoms of the data subjects impacted<sup>16</sup>. Nor did the Agency integrate all of the relevant safeguards for processing as an outcome of its assessment of data protection risks “*at the time of the determination of the means for processing*” or “*at the time of the processing itself*”<sup>17</sup>. Therefore, Frontex has not demonstrated that it satisfactorily implemented “*appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed*”<sup>18</sup>.
61. This is confirmed by the reply from the Agency’s Executive Director of 26 June 2020, which states: “*I am aware of your investigation on Microsoft products and services and of your findings and recommendations about the protection of personal data. Frontex ICT Unit is carefully looking into implementing organisational and technical measures to meet those recommendations*”.
62. Moreover, Frontex was aware of the existence, before the completion of the assessment, of elements indicating a meaningful level of risk of non-compliance, due to the outcome of the 2019-2020 EDPS investigation into EUIs’ use of Microsoft products and services<sup>19</sup>. Frontex did identify this level of risk but the DPIA does not provide evidence that the Agency adequately addressed it either before or after the start of the processing activities.
63. The action of the Agency in its approach to the move to cloud computing is therefore in breach of Articles 4(2), 26 and 27 of the Regulation. It does not adequately implement the recommendations in the Guidelines on how to assess the cloud computing option, either.

### 4.2. On the demonstration of necessity to adopt Microsoft solutions

64. According to Article 4(1)(c) of the Regulation, personal data processed must be “*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)*”. Article 4(2) establishes that “*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)*”.
65. The EDPS has provided guidance on the assessment of the data minimisation/necessity principle via the so-called “necessity toolkit”<sup>20</sup>.
66. The toolkit proposes a methodology and a series of steps to implement the principle. One of the steps is choosing processing activities that are the least intrusive while still being effective. This applies not only when drafting legislative proposals but also when planning

---

<sup>16</sup> See Article 26 of the Regulation

<sup>17</sup> See Article 27.1 of the Regulation

<sup>18</sup> See Article 27.2 of the Regulation

<sup>19</sup> See: [https://edps.europa.eu/data-protection/our-work/publications/investigations/outcome-own-initiative-investigation-eu\\_en](https://edps.europa.eu/data-protection/our-work/publications/investigations/outcome-own-initiative-investigation-eu_en)

<sup>20</sup> See: [https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit\\_en](https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en)

for IT products and services to process personal data. It is thus incumbent on the controller to look for alternatives (as it is usually also done in feasibility studies or legislative impact assessments) that are still effective/efficient to support the organisational tasks yet bear less risks to data subjects when processing their personal data.

67. In addition, in March 2020, the EDPS concluded its investigation into EU institutions' use of Microsoft products and services, whose findings and recommendations Frontex was aware of.
68. The Agency has failed to demonstrate the necessity of the planned cloud services, as it has not shown that the choice of Microsoft solutions was the outcome of a thorough process whereby the existence of data protection compliant, alternative products and services meeting Frontex's specific needs was assessed. This is in breach of Article 4(2) of the Regulation.

#### **4.3. On Microsoft's collection of personal data from Frontex's user devices and at the server side**

69. Based on Article 4(1)(c) of the Regulation, personal data processed shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*". Article 4(2) provides that "*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*".
70. Consequently, Frontex should allow Microsoft to only collect the minimum personal data necessary to carry out their institutional tasks and be demonstrate this.
71. The Agency showed genuine efforts in the identification of the physical diagnostics data flows towards Microsoft servers and obtained results in engineering the measures to limit the level of diagnostics beyond what offered by Microsoft at application configuration level. The EDPS appreciates these efforts and results, which Frontex documented and the EDPS acknowledges.
72. There are limitations, though, in the Agency's demonstration of data minimisation regarding Microsoft's collection of diagnostic data for Windows 10, as well as of other personal data :
  - Because data streams are encrypted, Frontex is not able to verify what personal data are collected by Microsoft in the flows that are still enabled. The EDPS has seen no evidence to suggest that Frontex made an attempt to obtain details from Microsoft on the structure and semantic of the data collected, or to obtain access to unencrypted data; nor Frontex did refer the EDPS to any available documentation.
  - An application-level diagnostics configuration, more fine-grained than the one offered by Microsoft, would have enabled Frontex to control what diagnostics data are sent for what purposes based on contractual agreements. The lack of such an application feature obliged the Agency to use a methodology that does not offer the necessary accuracy and guarantees that the Agency can be in full control of the diagnostics data flows.

- The EDPS finds no clear evidence in the provided documentation (including in the DPIA) that the diagnostics services which Frontex still enabled (e.g. in Windows 10) correspond to any identified legal basis and established lawful purposes.
- The EDPS finds no account on the description of Microsoft’s collection of personal data at server side, such as “service generated data”. We did not find any description of types of personal data collected, nor did Frontex take the collection of service generated data into account in the analysis of data protection risks.

73. Frontex’s actions are therefore in breach of Articles 4(2) of the Regulation.

## 5. Conclusions

74. In conclusion, the EDPS finds that:

- Frontex moved to the cloud without a timely, exhaustive assessment of data protection risks and identification of appropriate mitigating measures. The identification of the activity processing personal data and scope of the assessment itself is unclear. Furthermore, the assessment bears some fundamental flaws and weaknesses within the risk treatment and overall risk management. This is in breach of Article 26 of the Regulation.
- As a result, Frontex could neither integrate all of the relevant safeguards for processing as an outcome of its assessment of data protection risks “*at the time of the determination of the means for processing*” or “*at the time of the processing itself*”, nor implement “*appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed*”. This is in breach of Article 27 of the Regulation.
- Frontex failed to demonstrate the necessity of the planned cloud services, as it has not shown that the choice of Microsoft solutions was the outcome of a thorough process whereby the existence of data protection compliant, alternative products and services meeting Frontex’s specific needs was assessed. This is in breach of Article 4(2) of the Regulation.
- Frontex failed to adequately demonstrate that they limited Microsoft’s collection of personal data to what necessary, based on an identified legal basis and established purposes. Furthermore, the Agency did not give account of lawful grounds for server side collection of personal data by Microsoft, as for “service generated” data. This is in breach of Article 4(2) of the Regulation.

## 6. EDPS exercise of corrective powers

75. In identifying the corrective powers, the EDPS has taken into account the following mitigating factors:

- the overall cooperation of Frontex, despite its non-compliance with Article 58(1)(e) of the Regulation as regards the provision of a laptop with a requested configuration;
- the need for Frontex to support a “*challenging situation to implement its new mandate, in the midst of the still ongoing Covid crisis*”;

- Frontex’s commitment that this exceptional situation “... *should not be reiterated in the following steps of our gradual move to the Cloud, in alignment with our ICT Cloud Implementation Plan 2020-2025*”

76. Taking the above into considerations,

**THE EDPS THEREFORE:**

- 1) **Reprimands** Frontex in accordance with Article 58(2)(b) of the Regulation for a breach of Articles 4(2), 26 and 27 of the Regulation; and
- 2) Orders Frontex in accordance with Article 58(2)(e) of the Regulation **to review and amend the DPIA and the Record of processing activities** by 31 August 2022 based on the observations made above, in particular by:
  - a) clarifying the processing activities currently (even partially) processed by any cloud services from any provider used currently by Frontex, including their nature, scope, context and purpose, and the personal data processed in each and every of those activities;
  - b) identifying, where missing, relevant technical and organisational measures to adequately mitigate risks to data subject and assessing their effectiveness; and,
  - c) identifying and providing further information on existing data flows from Frontex (including as collected on the server side) to Microsoft, any other provider used currently by Frontex or third parties, as well as identifying the lawfulness, legal basis and purposes of those flows.
  - d) The revised DPIA and the Record of processing activities must include in their scope all processing activities carried out by Frontex through cloud-based products and services.
77. The EDPS **recommends** that Frontex liaise with the European Commission, as lead contracting authority in the procurement of M365 services, to comply with this order.
78. This is without prejudice to any follow-up or other actions the EDPS might undertake in the future with regard to the supervision of Frontex in the context of this or other files.
79. The EDPS intends to make public the facts of this investigation and the final outcome, including the actions taken in response by Frontex.

## **7. Judicial remedy**

80. Pursuant to Article 64 of the Regulation, any action against a decision of the EDPS may be brought before the Court of Justice of the European Union within two months from the adoption of the present Decision and according to the conditions laid down in Article 263 TFEU.

Done at Brussels on 1 April 2022

*[e-signed]*

Wojciech Rafał WIEWIÓROWSKI