EUROPEAN DATA PROTECTION SUPERVISOR

EDPS SUPERVISORY OPINION ON A PRIOR CONSULTATION REQUESTED BY THE EUROPEAN MEDICINES AGENCY ON THE DATA PROTECTION IMPACT ASSESSMENT FOR THE EUDRAVIGILANCE SIGNAL AND SAFETY ANALYTICS PLATFORM

(Case 2024-0531)

This Opinion addresses the question of whether mitigating measures identified by the European Medicines Agency ('EMA') in a Data Protection Impact Assessment (DPIA) can be considered sufficient to appropriately address the high risks identified by EMA in relation to its use of the EudraVigilance Signal and Safety Analytics Platform (EV SSAP). The European Data Protection Supervisor (the 'EDPS') has issued this Opinion in accordance with Article 40(2) of Regulation (EU) 2018/1725 (the 'EUDPR')[1].

The EDPS is of the opinion that the mitigating measures envisaged by EMA are sufficient to mitigate the high risks it has identified, provided that the EDPS recommendations put forward in this Opinion are implemented. In that sense, the EDPS makes several recommendations to assist EMA in ensuring compliance.

[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 No1247/2002/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

Contents

1. PROCEEDINGS

1. On 5 June 2024, the European Data Protection Supervisor (EDPS) received a request for prior consultation under Article 40(1) of Regulation (EU) 2018/1725 ('the EUDPR') regarding the Data Protection Impact Assessment (DPIA) for the EudraVigilance Signal and Safety Analytics Platform (EV SSAP) from the European Medicines Agency (EMA).
2. The request for prior consultation sent by EMA contained:

   - a cover letter explaining the context of this consultation (cover letter);
   - a DPIA and respective signed-off sheet.

3. Attached to the request for prior consultation were the following supporting documents:

   - record of the data processing regarding the EV SSAP;
   - EMA's data protection notice regarding the EV SSAP;
   - the contractual clauses between the controller and processor in a third country;
   - a Transfer Impact Assessment (TIA).

4. According to Article 40(2) EUDPR, 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 by six weeks.

5. Taking into account the complexity of the intended processing, the EDPS informed EMA on 5 July 2024 that the deadline would be extended by six weeks.

6. Taking into account that this period was suspended[2] until the EDPS obtained further information that he has requested[3], the deadline within which the EDPS shall issue his Opinion in this case is 16 October 2024.

7. Furthermore, on 27 and 28 March 2023, the EDPS carried out an audit to EMA regarding the EudraVigilance database, which was followed by an audit report on 2 May 2024 including several recommendations to improve EudraVigilance data protection compliance. Some of those recommendations are relevant in the context of this prior consultation, as we will further detail.

[2] Article 40(2) of Regulation 2018/1725.
[3] In the present case, the deadline was suspended for 35 days: from 5 July 2024 to 9 August 2024.

8. Additionally, EMA states that transfers of personal data outside the EEA to a third country are subject to the appropriate safeguards provided for in Article 46 of Regulation (EU) 2016/679 (the 'GDPR')[4], namely the transfers between EMA and RxLogix in the US and in India. Nevertheless, the DPIA also refers to contractual clauses between EMA and RxLogix in the US, in accordance with Article 48(3)(a) EUDPR tailored to this specific processing on behalf of EMA and which were submitted for approval to the EDPS. The EDPS will perform the assessment of those clauses in a separate case file (EDPS case file 2024-0532).

2. DESCRIPTION OF THE PROCESSING

2.1. Current EudraVigilance Data Analysis System

9. At the moment, EMA is using the EudraVigilance Data Analysis System (EVDAS) to perform pharmacovigilance analytics. [redacted]. As a consequence, EMA intends to deploy a new system, the EV SSAP.

2.2. Description of the New EudraVigilance Data Analysis System

10. According to EMA, '[t]he EV SSAP is intended as a new pharmacovigilance analytics platform which is an essential tool in the safety monitoring of medicines and the data-driven decision-making process of the European Medicines Regulatory Network (EMRN)'[6]. This new platform is provided by the company RxLogix. RxLogix is a US pharmacovigilance solutions company specialized in software and consulting services.

11. The **purpose** of the processing activity using the EV SSAP is safety monitoring and signal management (including signal detection, validation, confirmation and

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, DPIA p.19.
[5] EMA's cover letter to the EDPS consultation, p.1.
[6] Ibidem.

assessment) of adverse reactions that patients had while using authorised medicinal products or during clinical trials.

12. In order to function, EV SSAP uses data originating mainly from EudraVigilance, namely the Individual Case Safety Reports (ICSR) - where adverse reactions relating to individuals are described -, lookup data (with information regarding the country dose, form, etc.), substances/products and related hierarchies (scientific products, product indexes, etc.).

13. The EV SSAP will process personal data from the ICSR [redacted], but also name, contacts, cookies logging of the EV SSAP users.

14. The EV SSAP includes **three modules**: i) **PV Signal**, which is used to detect signals, uncover patterns and recognise emerging trends in spontaneous adverse events reported; ii) **PV Reports**, which generates reports and safety monitoring visualisations related to the detection, assessment, understanding and prevention of adverse effects or other pharmacovigilance issues; iii) **PV Data Hub**, the internal storage to support the other two modules.

15. The **categories of data subjects** affected by the processing include:

    a. citizens, stakeholders (individuals working for marketing authorisation holders and sponsors of clinical trials, consumers, patients) or individuals who are subject to suspected adverse reactions of medicinal products;
    b. reporters of adverse reactions (e.g. physicians, pharmacists, lawyers);
    c. study participants in clinical trials or non-interventional studies
    d. registered users in EV SSAP from EMA, European Commission (EC) and National Competent Authorities (NCAs).

16. The **categories of personal data** processed include:

    a. ***special categories of data (category 1)*** - pseudonymised ICSR (including health data and case narratives), name of the safety assessor of EMA, NCAs or the independent expert appointed by the EC;
    b. ***user and service-generated data (category 2)*** - name, email address, user interface session cookies, IP address, operation system, browser, timestamp,

user generated events (records created, deleted, exported, logs - including fail attempts to login) and logs[7];

c. ***support activities data (category 3)*** - name, email address, and the following optional data: phone, photo, title, language, time zone, Department and Service, office address, manager, contract type (staff or contractor).

17. Category 1 data is **stored** on Amazon Web Service (AWS) datacentre **in** [EU], including back-ups that will be spread across multiple zones in the same region. Category 2 data is stored in EMA's account management system [8] or in the file system in the servers dedicated for EMA in the AWS [EU] **region** (service-generated data). Category 3 data is managed solely within EMA's service desk portal (data centres within the EEA). To sum up, according to EMA, all data included in EV SAAP is stored in [EU].

18. Regarding the **data flows** for signal and safety analytics, EMA explained in the DPIA the following approach:

a. **Submission of Reports**: Individual Case Safety Reports (ICSRs), which include personal data about patients, are submitted to EMA. These reports come in through two channels:

- The 'EudraVigilance Web Interface'.
- The 'Axway Gateway'.

b. **Processing and Initial Storage**: The ICSRs meant for EudraVigilance are processed and stored in an Database located on Amazon Web Services (AWS) servers in EU]. However, some parts like XML messages and attachments (which may contain detailed case narratives or medical tests with personal data) are stored separately in [9] housed in an Azure datacentre in the [EU].

[7] See DPIA, p. 36, p. 121 and p. 122. Additionally, logs of administrator activities are also stored. See also "Privileged Access Manager (PAM) at RxLogix".

[8] service. It provides a secure and centralized way to manage user identities, control access to applications, and enforce policies within an organisation.

[9] 1. The EDPS notes that EMA is using to store XML messages and attachments from the ICSR from the EV SSAP. The EDPS reminds EMA that it has issued a decision on 8 March 2024 following the investigation into the European Commission's use of Microsoft 365. Given that the same inter-institutional contract with Microsoft analysed by the EDPS in that decision also governs EMA's use of operated on the Azure platform [EU], EMA should carefully study that decision and implement similar measures to those imposed on the European Commission, including as regards international transfers and unauthorised disclosures.

c. **Preparation for Safety Monitoring**: A simplified version of the data, containing only the essential attributes needed for safety monitoring and signal detection, is copied to an EMA staging area[10], which is an intermediate storage area used for data processing during the extract, transform and load (ETL) process.

d. **Data Transfer to RxLogix**:

- EMA uses the AWS Simple Storage Replication service to copy files from the EMA staging area to the RxLogix staging area.
- Once the files are successfully copied, they are deleted from the EMA staging area.

e. **Processing by RxLogix**: RxLogix runs an ETL process that takes the files from their staging area and loads the data into the PV Signal database. After the ETL process is successfully completed, the files are deleted from the RxLogix staging area. RxLogix administrators activate masking policies using [redacted], as per the agreement with EMA.

19. EMA administrators grant access to the RxLogix technical support team located in India and the USA.

20. This team applies the masking policies to hide sensitive data columns, ensuring that personal data cannot be accessed improperly.

21. Purpose of Data Transfer: Personal data is transferred from EMA to RxLogix for three specific reasons:
    - To provide and improve the services that RxLogix has been contracted to deliver, including their Pharmacovigilance Software as a Service (PV SaaS) platform.
    - To keep these services up to date.
    - To ensure the security of the EudraVigilance Signal Management and Analytics Platform (EV SSAP).

22. Nevertheless, where a user of the EV SSAP raises a service request, the request will be assessed first by EMA using EMA's request a service process. Only when the issue cannot be resolved by EMA, EMA staff will raise it with a technical expert of RxLogix, who will access remotely EMA's Service Desk portal to provide technical support.

[10] A staging area is an intermediate storage area used for data processing during the extract, transform and load processes.

23. According to the information provided by EMA, when RxLogix needs to further organise an internal response to the case, their support engineers may raise an internal case in [redacted]. However, no personal data in relation to EV SAAP is allowed to be copied into this case, and only a link or reference to the original case in EMA's Service Desk portal is authorised.

24. The DPIA identifies EMA, the European Commission and the Member States represented by NCAs as joint-controllers[11].

25. RxLogix, which is established in the USA, will be the processor. To deliver the required services, this processor will rely on AWS as a sub-processor for physical and environmental controls and safeguards regarding the physical data centers, virtual infrastructure components and encryption at rest. RxLogix (processor) will enter into a contract with AWS (sub-processor) to provide the cloud environment to store the RxLogix pharmacovigilance Software as a service (SaaS) platform.

26. According to the DPIA, personal data is intended to be subject to appropriate safeguards based on contractual clauses between the controller and the processor established in a third country, which are subject to authorisation by the EDPS[12].

27. RxLogix is not included in the 'Data Privacy Framework List'[13], whereas Amazon Web Services, Inc. is covered by the inclusion of Amazon.com, Inc. on that List.

3. LEGAL AND TECHNICAL ASSESSMENT

3.1. Need for prior consultation pursuant to Article 40 EUDPR

28. Article 40(1) EUDPR provides that the controller is obliged to consult the EDPS prior to processing where a data protection impact assessment under Article 39 EUDPR

[11] See DPIA, p.17.
[12] This EDPS Opinion is linked to the case file 2024-0532.
[13] On 10 July, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework. The adequacy decision concludes that the United States ensures an adequate level of protection – compared to that of the EU - for personal data transferred from the EU to US companies participating in the EU-U.S. Data Privacy Framework. See Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under document C(2023)4745), OJ L 231, 20.9.2023, p. 118–229.

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. The controller is to seek the advice of the data protection officer on the need for prior consultation.

29. The DPIA on the EV SSAP identified several high risks to data subjects and proposes mitigation measures to reduce the impact and likelihood of those risks. Nevertheless, even after the suggested mitigation measures, EMA still identifies one high risk concerning potential unauthorised international data transfers related to the transfers to the processors.

30. The Data Protection Officer (DPO) of EMA was consulted regarding the EV SSAP operations and EMA drafted a DPIA on this data processing.

31. The EMA provided the necessary documentation in accordance with Article 43 EUDPR. Therefore, the conditions for a prior consultation are fulfiled.

3.2. Scope of the Opinion

32. The Opinion of the EDPS on this prior consultation aims at assessing if the intended processing by EMA regarding EV SSAP would infringe the EUDPR, in particular whether the controller has insufficiently identified or mitigated the high risks it identified in the DPIA, in light of Article 40(2) EUDPR. Therefore, this Opinion will focus on key aspects of the EV SSAP that raise issues of non-compliance with the applicable data protection legal framework or otherwise merit further analysis, in particular the appropriateness of the measures envisaged to mitigate the high data protection risks identified by EMA, **as described in the notification** of 5 June 2024 and appended documentation.

33. This Opinion does not include in its scope the authorisation of contractual clauses under Article 48(3)(a) EUDPR in the context of the services provided by RxLogix and AWS, which will be separately analysed by the EDPS in another Opinion[14].

34. Furthermore, this opinion does not assess the processing of personal data in EMA's use of [redacted] in the context of the EV SSAP. This opinion is also without prejudice to the ongoing investigation by the EDPS into the transfers outside

[14] See EDPS Opinion in case 2024-0532.

of the EEA when EU institutions, bodies, offices and agencies use cloud services provided by Microsoft and Amazon under the respective Cloud II contracts. The legal assessment in this Opinion only concerns the EUDPR and it does not encompass a GDPR assessment.

35. The EDPS took note of the risks to data subjects considered medium and low by EMA in the DPIA under analysis. In this regard, considering their reduced impact on data subjects and the mitigation measures put in place by EMA, the EDPS has decided not to include them in the scope of this Opinion.

3.3. Assessment of the DPIA

36. In light of the information in the DPIA and the supplementary clarifications provided by EMA on 9 August 2024, the EDPS takes note of the thorough analysis and response foreseen by EMA regarding the processing operation under analysis.

37. In order to provide useful comments for EMA, the EDPS has decided to assess the measures envisaged in the DPIA for the mitigation of the high risks therein identified. Having said so and to clearly associate the EDPS assessment to the risks and respective mitigation measures, the EDPS followed the same structure of risks mentioned in section "8 Risks and mitigating measures" of the DPIA.

38. According to Article 2(1) EUDPR, the EUDPR is applicable to EMA since it is a EU Agency, as defined in Article 3(10) EUDPR.

39. According to Article 3(1) EUDPR, 'personal data' means any information relating to an identified or identifiable natural person. As such, the data listed above in paragraph 17 of this Opinion, constitute personal data, within the meaning of Article 3(1) EUDPR.

40. Additionally, according to Article 3(3) EUDPR, 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. EMA's operation of collecting, using and storing the above mentioned personal data to fulfil pharmacovigilance obligations constitutes processing within the meaning of Article 3(1) EUDPR, in respect of which EMA is a controller, within the meaning of Article 3(8) EUDPR.

41. In accordance with Article 3(19) of the EUDPR, 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about their health status. The processing of special categories of data, such as data concerning health, is prohibited, unless one of the conditions mentioned in Article 10(2) EUDPR is applicable, as we will analyse below.

3.3.1. Unauthorised international data transfers

42. EMA identified as a high risk in the DPIA[15] the possibility of unauthorised international data transfers. This was the only high risk in the DPIA that remained high after the application of mitigation measures by EMA.

43. According to the European Data Protection Board (EDPB)[16], a processing operation may be qualified as a transfer when three cumulative criteria are met: (1) a controller or a processor ('exporter') is subject to the GDPR for the given processing, 2) the exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ('importer'), and 3) the importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation.[17]

44. The EDPS finds that for transfers meeting the three cumulative criteria and which are envisaged under a contract, i.e., transfers that the controller knows or should foresee in the broader context of the execution of the contract, or under other organised relationship, a transfer tool under Chapter V EUDPR must be relied upon before any such transfers occur.

45. In that vein, remote access from a third country constitutes a transfer when it happens if the three above-mentioned criteria are met.[18] Equally, remote governmental access under third-country laws to personal data located and processed in the EEA, when it takes place, results in transfers of personal data.[19]

[15] DPIA, p. 62.
[16] The EDPS by analogy relies on guidance issued by the EDPB in the context of its interpretation of the Regulation where the interpreted provisions and principles, like in this case, are the same.
[17] EDPB Guidelines 05/2021, point 9.
[18] EDPB Guidelines 05/2021, point 16.
[19] By analogy see point 24 of the EDPB Guidelines 05/2021.

46. However, in the EDPS opinion, the mere risk that remote access by third country entities to data processed in the EEA may take place, does not constitute a transfer subjected to Chapter V of the EUDPR.

47. The EDPS considers that transfers resulting from unauthorised access by third country entities, which are merely potential and in no way foreseeable in light of the content or purpose of a contract or another stable relationship between the parties, do not fall under the scope of Chapter V of the EUDPR. The unlikely and unplanned character of such risks of such unauthorised access renders them unsuitable to be ex ante subjected to regime of Chapter V of the Regulation. It follows that for such potential and unplanned transfers a transfer tool under that Chapter is not required.

48. The EDPS recalls that the risks of such potential transfers resulting from the application of third-country laws to processors located in the EEA must be part of controller's analysis and assessment in line with the principle of accountability[20]. Before engaging a processor, the controller must assess the possible application of third country extra-territorial laws in order to ensure that, as required by Article 29 EUDPR, it only uses processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing is in line with the EUDPR.[21] Where the processor complies with a disclosure request in violation of the controller's instructions and thus Article 29 EUDPR, that processor shall be, in line with Article 29(10) EUDPR, considered an independent controller of that processing.

49. When concluding contractual arrangements and providing instructions to the processor in line with Article 29 EUDPR, particular attention should be paid to the observance of the principles of integrity and confidentiality under Article 4(1)(f), and the related Articles 33 and 36 EUDPR laying down requirements for security of the processing operations and security and confidentiality of electronic communications, systems and networks.

50. In the case at hand, transfers resulting from possible remote governmental access to data located in the EEA, while theoretically possible under the laws of the United States and India, are not envisaged nor planned under the contract between EMA and RxLogix. In that sense, EMA does not plan for such transfers to take place in the

[20] See also Section 3.6 'Risk of access by foreign governments when using non-EU CSPs storing data in the EEA' of the 'EDPB report '2022 Coordinated Enforcement Action Use of cloud-based services by the public sector' adopted on 17 January 2023

[21] By analogy, see point 24 of the EDPB Guidelines 05/2021. See also Section 5 'Points for attention for public bodies', in particular page 32, of the EDPB Report on the 2022 Coordinated Enforcement Action.

broader context of the execution of that contract or its stable relationship with RxLogix and AWS.

51. Furthermore, EMA will mask the fields configured as sensitive to prevent access to such personal data whenever it needs the technical support from the US and India.

52. Based on the above, the potential transfers of data located in the EEA data centres resulting from the application of third-country laws are not covered by Chapter V of the EUDPR, and EMA does not need to provide for appropriate safeguards for them by means of contractual clauses.[22]

3.3.2. Use of Cloud services

53. The EDPS also notes that part of the EV SSAP will be deployed and operated on the AWS cloud infrastructure procured by EMA's processor RxLogix.

54. Article 29 EUDPR details the obligations of controllers regarding processors. In particular, that the controller should only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the EUDPS requirements (Article 29(1) EUDPR). Furthermore, Article 29(2) EUDPR states that the processor cannot engage another processor without prior specific or general written authorisation of the controller.

55. The EDPS reminds EMA that it has an ongoing investigation into the transfers outside of the EEA when EU institutions, bodies, offices and agencies use cloud services provided by Microsoft and Amazon (AWS) under the respective Cloud II contracts. The ongoing investigation will, among other issues, assess whether effective technical and organisational measures have been implemented to ensure an essentially equivalent level of protection as required by EUDPR where personal data is transferred outside of the EEA and to ensure the integrity and confidentiality of personal data processed within and outside of the EEA, including to ensure that no unauthorised disclosures take place. This ongoing investigation may be therefore relevant in the present case.

[22] However, should RxLogix or any sub-processors receive a request from a third country for access or disclosure of data in EMA's use of RxLogix services and RxLogix or AWS intend to positively respond to such a request, EMA must ensure that such a transfer pursuant to the access request complies with Chapter V of the EUDPR.

56. Following the outcome of the ongoing investigation, as well as in any future development of the EV SSAP or in any changes on how Microsoft and AWS provides IaaS and PaaS[23] cloud services to EMA and its processor, EMA should:
    i) **make additional assessments on whether the safeguards and measures EMA and its processor have in place for the AWS and Microsoft (Azure) cloud services used for the EV SSAP are still effective (Recommendation 1)**, and
    ii) **ensure additional measures are taken for the AWS and Microsoft (Azure) cloud services used for the EV SSAP and for any new AWS or Microsoft cloud services envisaged for the EV SSAP, including changes to the contracts in order to ensure compliance with EUDPR and other EU law applicable to the data in the EudraVigilance and the EV SSAP (Recommendation 2)**.

57. Additionally, **EMA may consider assessing if any measures similar to those imposed under the EDPS decision of 8 March 2024 (in particular measures under paragraphs 592.1., 592.2.1., 592.2.2., and 592.2.3. c), f) and g of that decision) need to be taken for the AWS cloud services used for the EV SSAP, including necessary changes to the contracts, and data flows to third countries (Recommendation 3)**.

58. Furthermore, **EMA should assess not only the risks of unauthorised transfers, but also the risks of authorised transfers. Therefore, EMA has to assess potential remote access to support requests to prevent fraud and abuse and if the transfer is requested by RxLogix, including transfers by default, transfers that could be opted-out and transfers that cannot be stopped (Recommendation 4).**

3.3.3. Lack of transparency

59. EMA identified three high risks in the DPIA related to the lack of transparency[24]: the lack of transparency during data collection or at any stage of the processing; incomplete information provided to the data subjects in scope of the processing; and the lack of transparency in the case of data sharing and international data transfers.

60. Article 4(1)(a) EUDPR establishes that personal data must be processed in a transparent manner in relation to the data subject (principle of transparency). Recital

[23] Infrastructure-as-a-Service and Platform-as-a-Service.
[24] See DPIA pp. 63-66.

20 EUDPR mentions that '[t]he principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of personal data. ...'

61. Furthermore, the EDPB[25] states that 'transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights'. Moreover, the EDPS issued guidelines on transparency[26] to support EU institutions, bodies and agencies to understand their obligations under Articles 14 to 16 EUDPR. There is also relevant CJEU case law regarding transparency obligations, namely on the information about recipients[27].

62. In the case at hand, EMA will put in place an EV SSAP data protection notice to mitigate the risk of lack of transparency, which is included in the Annex II of the DPIA.

63. As explained by EMA, the EV SSAP data protection notice provides a baseline set of general information regarding the data processing in scope of the platform that will help the data subjects in scope of the processing to understand the terms of the processing operation at issue. In addition, the EV SSAP data protection notice outlines the main data processing operations within the EV SSAP, the applicable legal bases for the processing operations, the rights of data subjects and how these can be exercised in accordance with the provisions of the EUDPR.

[25] Article 29 Working Party - Guidelines on transparency under Regulation 2016/679 (last revised and adopted on 11 April 2018), p. 4.
[26] EDPS Guidance on Articles 14 - 16 of the proposal for a Regulation on the protection of individuals 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.
[27] See CJEU C-154/21 (Österreichische Post).

64. As part of EMA's commitment to the principle of transparency, EMA will make available the EV SSAP data protection notice online at EMA's website.

65. EMA will review and update the EV SSAP data protection notice periodically to ensure that the actors involved on the processing are up to date, and to reflect the type of processing activities that it has allowed and that may occur from the US and the India.

66. Moreover, EMA will invite the joint-controllers to align their communications and data protection notices with the one updated by EMA. In particular, EMA will liaise with NCAs, sponsors of clinical trials and MAHs to include a reference to the EV SSAP data protection notice in their transparency initiatives to raise awareness of the data subjects concerned.

67. Consequently, the EDPS notes that EMA will be able to mitigate the risks identified and comply with the transparency principle under article 4(1)(a) EUDPR, provided that EMA publishes the EV SSAP data protection notice online at EMA's website, informs the data subjects via the most suitable communication channels and commits to invite the other joint-controllers to include a reference to the EV SSAP data protection notice in their transparency initiatives to raise awareness of the data subjects concerned.

68. In order to have more transparency and to inform data subjects how they will be informed about this processing operation, **the EDPS recommends that EMA also mention in the DPIA specific examples of the communication channels that will be used to inform the data subjects (i.e. information displayed at the moment when a data subject fills in an online form) (Recommendation 5).**

3.3.4. Lack of fairness

69. EMA identified as a high risk in the DPIA the breach of trust by data subjects[28]. In particular, EMA has identified as a high risk the fact that the concerned data subjects may be surprised about the use of their personal data within the EV SSAP. As indicated by EMA in the DPIA, the reasonable expectations of data protection and privacy of individuals whose personal data is under processing within the EV SSAP may be breached.

70. In order to mitigate such risk, EMA explained in the DPIA that they will provide a baseline set of general information regarding the data processing on their public

[28] See DPIA, pp. 66-68.

website to help data subjects understand the processing, as explained in the section 3.3.3 'lack of transparency'. In addition, EMA will review the content of the EV and EV SSAP data protection notices on a regular basis.

71. Article 4 (1)(a) EUDPR states that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (principles of lawfulness, fairness and transparency). These principles are also echoed in Articles 14, 15 and 16 EUDPR, regarding the way of providing certain necessary information to data subjects.

72. The principles of lawfulness and fairness are intrinsically linked. In this sense, the EDPB recommends the use of layered privacy statements/ notices[29], 'which allow website visitors to navigate to particular aspects of the relevant privacy statement/ notice that are of most interest to them'. In line with the fairness principle[30], the EDPB recommends that 'the first layer should contain information on the processing which has the most impact on the data subject and processing which could surprise them'.

73. In the case at hand, the provision of an online-layered data protection notice is not entirely envisaged by EMA in the data protection notice (Annex II of EMA's DPIA). The information is segmented in different sections, includes tables with detailed information about the personal data categories, retention periods, etc., but does not provide a first glace quick overview.

74. Considering the length of the data protection notice and to better address the layered approach, the EDPS recommends that EMA use a table of contents with hyperlinks to the respective sections of the data protection notice at the beginning, as well as a 'in a nutshell' initial section with the **information on the processing activity which has the most impact on the data subjects (i.e., safety monitoring activities), the purposes of the processing operations, the identification of the joint-controllers and a description of the data subject's rights**, in line with the principle of fairness (Article 4(1)(a) EUDPR) **(Recommendation 6).**

75. Moreover, in accordance with the EDPB Guidelines on transparency under Regulation 2016/679 regarding the principle of fairness, EMA should, wherever possible, provide the information about the risks, rules, safeguards and data subjects rights regarding the processing of their personal data well in advance[31], namely with

[29] Article 29 Working Party - Guidelines on transparency under Regulation 2016/679 (last revised and adopted on 11 April 2018), p 11.
[30] Article 4(1)(a) EUDPR.
[31] Article 29 Working Party - Guidelines on transparency under Regulation 2016/679 (last revised and adopted on 11 April 2018), p. 16.

the support of the other joint-controllers. Therefore, **the EDPS recommends that EMA contact the other joint-controllers to provide the data protection notice to data subjects as soon as possible (Recommendation 7).**

76. Finally, still in light of the principles of lawfulness, fairness and transparency (Article 4(1)(a) EUDPR) and in light of Articles 14(1) and 16(1)(e) and (f) EUDPR, **the EDPS deems necessary** that EMA **either notify data subjects - whose personal data is already being processed - with the joint-controllers support, of the changes in EudraVigilance**, including the potential impact of the changes upon them (including stemming from new transfers of personal data outside the EEA), and the modality used to communicate the changes, and be able to demonstrate how the timeframe between notification of the changes and the change taking effect; **or EMA document the assessment and the reasons not to perform such notification of the changes to data subjects, under Articles 4(2) and 16(5) EUDPR (Recommendation 8). Otherwise, the EDPS considers that the EMA would violate the data subjects right to information under Articles 14(1), as well as 16(1)(e) and (f) EUDPR.**

3.3.5. Purpose limitation

77. EMA identified three high risks in the DPIA related to the purpose limitation principle: excessive, unspecified, and unlimited purposes of data uploading or data collection within the EV SSAP; further use of the personal data for a purpose which is incompatible with the original purpose; and personal data processing for incompatible purposes.

78. As explained by EMA in the DPIA, failure to comply with the purpose limitation principle[32] will prevent restricting further uses of personal data beyond EMA's mandate set out in the pharmaceutical legislation. In addition, EMA explained that it will also restrict the mapping of security issues, which may lead to higher risk of identification and potential suffer data breaches.

79. Article 4(1)(b) EUDPR states that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

80. The purpose limitation principle is linked to the principle of fairness. In this sense, the EDPB observes that the controller should always specify the purposes of the

[32] Article 4(1)(b) EUDPR.

processing at the time of collection[33]. Therefore, EMA has to define clearly the purposes so the concerned data subjects know what to expect. This requires EMA to clearly state for which purposes it processes which types of personal data.

81. In the case at hand, EMA has determined and documented the purposes of data processing within the EV SSAP, in line with the applicable legal framework. EMA has recorded this in the Section 5.2 of the DPIA and the necessary information is included in the applicable data protection notices, in line with Article 4(1)(b) EUDPR.

82. Furthermore, in order to restrict the processing beyond the agreed purposes, EMA will put in place appropriate contractual provisions for the data processor(s) and EMA will set up instructions for the EV SSAP users. EMA explained in the DPIA that in case a new purpose is to be defined for the EV SSAP, which goes beyond the legal obligations set out in the pharmaceutical legislation, a compatibility assessment will be performed, in order to comply with the purpose limitation principle[34].

83. In light of the above, the EDPS takes note that EMA **has put in place appropriate measures to mitigate the risks identified in relation to the purpose limitation principle**. In addition, **the EDPS takes note that EMA will document the purposes of data processing within the EV SSAP in the corresponding record of processing activities held by EMA, as well as in the applicable data protection notices.**

3.3.6. Data minimisation

84. EMA identified as a high risk in the DPIA the fact that unnecessary amount of personal data is processed within the EV SSAP, during the development of the platform and in production[35].

85. As EMA explained in the DPIA, the lack of privacy controls to limit the data processing would increase the risk of identification for data subjects, leading to consequences such as possible stigma and discrimination. The potential impact for the data subjects would be the loss of confidentiality.

[33] Article 29 Working Party - Guidelines on transparency under Regulation 2016/679 (last revised and adopted on 11 April 2018), p 14.
[34] Article 4(1)(b) EUDPR.
[35] See DPIA, pp. 70-73.

86. Article 4(1)(c) EUDPR states that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

87. In the case at hand, EMA has established a process whereby only personal data required for the safety monitoring and analysis are transferred from EV to the EV SSAP, in line with Article 4(1)(c) EUDPR. The details of the process flow can be found in the section 5.1.2.1. of the DPIA 'Safety monitoring in the pre- and post-authorisation phase of medicinal products'.

88. Therefore, regarding the proportionality principle, the EDPS notes that the processing of personal data within the EV SSAP is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and such processing operation comply with the requirements established under Article 4(1)(c) EUDPR.

89. As explained in section 8.6 of the DPIA, EMA will explicitly document and maintain the extraction of data from EudraVigilance. In addition, EMA will put processes in place in EudraVigilance to ensure the deletion of personal data in case of errors in the uploading/provision in the EV SSAP, in order to comply with data minimisation principle[36].

90. Consequently, the **EDPS considers that EMA complies with data minimisation principle, under Article 4(1)(c) EUDPR, provided that the necessary [redacted] policies are developed and tested**.

3.3.7. Pseudonymisation and masking

91. EMA identified as a high risk in the DPIA the fact that 'personal data may be inadequately anonymised/pseudonymised / masked where this is required'[37], which may lead to unauthorised reversal of pseudonymisation.

92. Article 33(1) EUDPR states that taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

[36] Article 4(1)(c) EUDPR.
[37] DPIA, p. 72.

93. EMA anonymises all personal data at source in all non-production environments[38].

94. As regards production environments, the ICSRs are pseudonymised at source meaning that either the marketing authorisation holder (pharmaceutical company) or the national Competent Authority of the respective Member State pseudonymise the ICSRs before sending them to EMA. The marketing authorisation holders and the Competent Authorities are required to apply the rules on pseudonymisation laid down in guidelines on good pharmacovigilance practices, EMA/873138/2011 Rev 2 from 28 July 2017, p. 63. EMA is working on the implementation of an EDPS recommendation on how to apply masking[39].

95. All ICSRs are delivered to EMA in pseudonymised format and stay in this format through the entire process.

96. EMA claims that identifiers of the pseudonymisation process stay with the authorisation holder respectively the national Competent Authority and that they are not capable of identifying the individuals in the ICSRs.

97. Furthermore, to mitigate the risk that staff of the service providers with privileged access level could access personal data without authorisation in the RxLogix-owned database (PV Signal database), EMA will develop, implement and test [redacted] policies for column level data masking[40]. Column-level masking in [redacted] is a security feature that allows organisations to protect sensitive data by masking specific columns within database tables.

98. By implementing the [redacted] policies, EMA will ensure role-based access to different user groups when needed. This means that end-users can access the data via the application level while neither the processor's support engineers nor the processor's administrators have the means to access[41] the data in the database even when using direct access via administration tools.

[38] Non production environments are environments used for developing, testing, training or other activities that do not impact the end users or live operations.
[39] This is a recommendation deriving from a Data Protection Audit at the European Medicines Agency (2023-0042).
[40] Data Protection Impact Assessment (DPIA) of the EudraVigilance Signal and Safety Analytics Platform (EV SSAP), chapter 8.2 p. 62: "[redacted] policies will be put in place for column level data masking".
[41] Data Protection Impact Assessment (DPIA) of the EudraVigilance Signal and Safety Analytics Platform (EV SSAP), chapter 5.1.2.2 p. 29: "This is a standard functionality in [redacted] databases that allows for data masking even when accessing the database directly".

99. EMA still needs to design, implement and test [redacted] policies[42] in order to effectively mask the relevant personal data in the [redacted]. These [redacted] policies include inter alia [redacted].

100. The [redacted] policy allows a user with [redacted] privileges[43] to configure [redacted] policies (e.g. add, alter, drop...)[44] whilst the [redacted] allows a user with [redacted] privileges to create Data Redaction policies (which can mask data)[45].

101. Thus, [redacted] privileges on these policies must only be granted to trusted users as they could provide access to the personal data located in the RxLogix-owned database (PV Signal database).

102. **In order to ensure the controller is implementing all the necessary technical and organisational security measures, the EDPS deems necessary that EMA carefully select the trusted users receiving the [redacted] privileges on [redacted] policies in such a way as to implement the principle of least-privilege, in light of Article 33(1) EUDPR. Furthermore, the EDPS deems necessary that EMA verifies the proper implementation of the aforementioned policies (Recommendation 9).**

3.3.8. Data accuracy

103. EMA identified as a high risk in the DPIA[46] the fact that inaccurate, outdated or incomplete data is processed within the EV SSAP, when the data is first uploaded or at a later stage, which could lead to incorrect, biased or unfair decisions for trial subjects or patients, or that they could not update, nor correct their personal data.

104. Article 4(1)(d) EUDPR states that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy principle).

[42] Data Protection Impact Assessment (DPIA) of the EudraVigilance Signal and Safety Analytics Platform (EV SSAP), chapter 9.1 p. 105, recommendation 7.

[43] [redacted]

[44] [redacted]

[45] [redacted]

[46] DPIA, pp. 74-76.

105. The EDPS notes that EMA must make all reasonable efforts to ensure that the data processed within the EV SSAP is accurate, since decisions based on wrong information may have negative impacts on the data subjects and may expose EMA to liability.

106. To mitigate such risk, EMA will put in place the following processes within the platform in order to comply with the data accuracy principle[47]: report amendment, ETL to trigger and update any changes related to source data, and ad-hoc process to delete corrupted, incorrect or unlawfully processed data. In addition, EMA will implement measures to ensure continuous monitoring of the information included in the EV SSAP, in line with Article 4(1)(d) EUDPR.

107. As explained in the section 8.7 of the DPIA, EMA is developing and monitoring the ETL process to ensure data accuracy. Moreover, EMA has already implemented a process based on the ISO ICSR/ICH E2B(R3) standard to ensure that personal data can be adequately maintained or deleted as applicable.

108. Consequently, **the EDPS considers that EMA complies with data accuracy principle, under Article 4(1)(d) EUDPR, provided that a report amendment system is implemented, the ETL process is developed and tested and a continuous monitoring system is in place.**

3.3.9. Storage limitation

109. EMA identified three high risks in the DPIA in relation to the storage limitation principle: the fact that the retention periods and policies are not clearly defined for any category of personal data; intrusive data retention legal provisions for law enforcement purposes; and the risk that the personal data are not permanently erased by the (former) CSP.

110. As EMA explained in the DPIA, the undefined retention periods and availability of personal data increases the risks of identification and permanently exposes personal data to external and internal threats, which may aggravate the risks for personal data breaches.

111. Article 4(1)(e) EUDPR states that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation principle).

[47] Article 4(1)(d) EUDPR.

112. Article 31(1)(f) EUDPR states that the controller must maintain a record of the processing activities under its responsibility, including where possible the envisaged time limits for erasure of the different categories of personal data.

113. According to the EDPB[48], 'the purpose of the processing shall be the main criterion to decide in how long personal data shall be stored'.

114. In the case at hand, EMA has defined and reflected the retention periods of personal data in the point 11.3 of the EV SSAP Data Protection Notice, in line with Article 4(1)(e) EUDPR.

115. Moreover, EMA will request confirmation from RxLogix as regards the effective deletion of personal data related to the EV SSAP after the end of the services, in order to comply with the storage limitation principle[49].

116. In light of the above, the EDPS notes that EMA have put in place appropriate measures to mitigate the risks identified in relation to the storage limitation principle. However, as a good practice, **the EDPS recommends that EMA document the envisaged time limits for erasure of the different categories of data in the corresponding record of processing activity (EV SSAP ROPA), in accordance with Article 31(1)(f) EUDPR (Recommendation 10).**

3.3.10. Integrity and confidentiality

117. EMA identified as a high risk in the DPIA the poor design and implementation of inadequate offline and online security measures, failure of compliance with security measures by processors and sub-processors and loss of confidentiality[50].

118. Article 4(1)(f) EUDPR mentions that personal data must be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality principle).

119. Article 33(1) EUDPR states that taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as

[48] EDPB Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default (adopted on 20 October 2020), p.25.
[49] Article 4(1)(e) EUDPR.
[50] DPIA, pp. 79-92.

well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (...) and
d) a process for regularly testing, assessing and evaluating the effectiveness of those measures for ensuring the security of the processing.

120. Moreover, Article 33(3) EUDPR states that the controller and processor must take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless they are required to do so by Union Law.

121. EMA is planning to implement controls for confidentiality and integrity during the entire data flow.

122. EMA will establish an identity and access management service for user accounts based on EMA's [redacted][51]. This provides the necessary governance for the provisioning of the access required for the authorisation, in accordance with EudraVigilance access process. The EDPS understands that currently there is [redacted] implemented[52] and EMA is assessing if this would provide additional value.

123. The service provider (RxLogix) will run a privileged access management (PAM) solution to monitor administrator access to the system components. The EDPS understands that currently, there has not been an agreement between EMA and RxLogix concerning access to the log files of the PAM; EMA and RxLogix are discussing the possibility to access these log files in the PAM solution- the exact process is still to be defined.

[51] [redacted] service. It provides a secure and centralized way to manage user identities, control access to applications, and enforce policies within an organisation.

[52] The EDPS made a recommendation on [redacted] on the Data Protection Audit at the European Medicines Agency (2023-0042).

124. Access to PAM is limited to the RxLogix security team. Further documentation received by the EDPS[53] describes that the "logs are stored in an immutable format, meaning once they are written, they cannot be altered or deleted."

125. Having access to these log files will permit inter alia detecting misuse of privileged accounts[54], attempts to access the personal data in the PV Signal database and attempted modification of the [redacted] policies[55].

126. **As such, the EDPS deems necessary that EMA and RxLogix develop a policy and procedure to transfer these log files to EMA for regular review. These logs should be in a readable format for EMA. On its side, EMA should implement a tool to sift through these log files in order to facilitate detecting unauthorised operations, which could lead to unauthorised access or modification of personal data in the database against the instructions of the controller. In case such unauthorised operations are detected, the security incident management process should be triggered (Recommendation 11). Otherwise, the EDPS considers that the EMA would violate Articles 4(1)(f), 33(1)(b) and (d) and Article 33(3) EUDPR.**

127. The data will be
   a. transferred in an EMA-owned [redacted] database,
   b. extracted to an EMA-owned staging area,
   c. replicated to a RxLogix-owned staging area and
   d. uploaded to a RxLogix-owned [redacted] database. All these storage locations are considered "data at rest". When the data is being transferred from one storage location to the other it is considered "data in transit".

128. EMA explained in the DPIA that data in transit will be encrypted via [redacted][56] [redacted]. **The EDPS recommends that EMA either apply [redacted] or ensure using the most up-to-date cryptographic settings [redacted] (Recommendation 12)**.

129. EMA-owned [redacted] database will have implemented access controls of [redacted] databases.

[53] Titled "Privileged Access Manager (PAM) at RxLogix".
[54] Such as the [redacted] account.
[55] See also para. 99 of this Opinion.
[56] [redacted]

130. The data stored on EMA-owned and RxLogix-owned staging areas will be encrypted applying [redacted] In particular, [redacted][57]. EMA explained that RxLogix will not have direct access to the encryption keys.

131. For the upload of the data from the RxLogix-owned staging area to the RxLogix-owned database, an application [redacted] will decrypt the ICSR data and process it in clear. This application will be under full control of the service provider. EMA explained that they will test the proper functioning of this application. This will be a black-box test without knowing the source code of the application.

132. **The EDPS recommends that EMA either audit the source code of the upload application or ensure that the only upload destination is the RxLogix-owned [redacted] database (Recommendation 13)**.

133. In its DPIA[58], EMA mentions that "Physical deletion with a [redacted] is an exceptional but possible process, always upon request and confirmation by EMA."

134. Given that the use of a [redacted] could affect the integrity and/or the confidentiality of the personal data in the database, **the EDPS recommends that EMA systematically include, in any process which uses such [redacted], the obligation by EMA to check the activity (logs) of the [redacted] (Recommendation 14).**

135. EMA identified as a high risk in the DPIA the lack of a procedure to perform an identification, analysis and evaluation of the information security risks potentially affecting personal data and the IT systems supporting data processing.

136. To mitigate such risk, EMA, in liaison with the processor, has assessed the security vulnerabilities and requirements of the EV SSAP and designed relevant measures in handling online and offline security risks. Moreover, EMA will put in place monitoring and reporting policies to ensure ongoing security screening. Therefore, the EDPS considers this risk mitigated.

---

[57] The [redacted] compliant which means that they are designed to prevent physical tampering with tamper-evident seals, intrusion sensors, and self-destruct mechanisms.
[58] DPIA, p. 77.

3.3.11. Accountability obligations

137. EMA identified in the DPIA as high risks some accountability obligations, namely the lack of joint-controllership arrangement between joint-controllers, lack of agreement with third-party data processors, Internet surveillance by governments and security services[59].

138. Article 28 EUDPR mentions that joint-controllers must determine their respective responsibilities for compliance with their data protection obligations by means of an arrangement. In this regard, the EDPS and the EDPB have published guidelines on the topic of joint-controllership[60].

139. The EDPS takes note that EMA has already a joint-controllership agreement in place and that a review to assess the need for adjustments will occur prior to the launch of the EV SSAP. Therefore, this risk is considered mitigated.

140. Regarding the risk of lack of agreement with third-party data processors, EMA mentioned that the 'lack of allocations of responsibilities could result in poor compliance with the GDPR and EUDPR, leading to loss of control over personal data and loss of confidentiality for data subjects'[61].

141. Article 29 EUDPR details the obligations of controllers regarding processors. In particular, that the controller should only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the EUDPS requirements (Article 29(1) EUDPR). Furthermore, Article 29(2) EUDPR states that the processor cannot engage another processor without prior specific or general written authorisation of the controller.

142. In order to address such requirements, the 'EMA has developed a process to review the processor's services, and its data protection practices'[62], including a Cloud and Data Protection Risk Assessment for Vendors, the RxLogix EMA Transfer Impact Assessment and Guidance for data controllers using the RxLogix PV SaaS platform.

143. However, the DPIA only mentions one processor and one sub-processor, in spite of the public references to the use of around 90 sub-processors (AWS entities

[59] Ibid., pp. 92-96.
[60] EDPS Guidelines on the concept of controller, processor and joint-controllership under Regulation (EU) 2018/1725 and EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
[61] DPIA, p.93.
[62] Ibidem.

and others) by AWS[63]. EMA did not mention any of them, nor assessed the risks relating to their involvement in the processing operation under analysis.

144. Therefore, the DPIA does not properly assess the risks of processors and sub-processors both in EEA and outside, including the risks stemming from third-country laws applying to those processing operations. Transfer Impact Assessments (TIA) for certain countries may lead to the conclusion that such transfers cannot be compliant with Article 48 EUDPR.

145. In light of the above, **the EDPS deems necessary that EMA check which sub-processors are entailed in the use of AWS and properly assess the risks of all processors and sub-processors therein involved (Recommendation 15). Otherwise, the EDPS considers that the EMA would violate Article 29 EUDPR.**

3.3.12. Data subjects rights

146. EMA identified as a high risk in the DPIA[64] EMA's lack of policies and mechanisms to handle and reply to questions and complaints from data subjects regarding the EV SSAP.

147. According to Article 15(1)(a) and 16(1)(a) EUDPR, the controller has the obligation to inform data subjects about its identity and contact details regardless of whether personal data is collected from data subjects or has not been obtained from them. Notwithstanding, the controller must also inform data subjects about the contact details of the DPO, according to Article 15(1)(b) and 16(1)(b) EUDPR.

148. The data subjects' right to be informed about the contact details of the controller and its DPO above mentioned, allows them to exercise their rights under the EUDPR directly by the controller.

149. In order to address the risk mentioned in para. 138 of this Opinion, EMA will make available a data protection notice informing data subjects about their rights, including the right to lodge a complaint to the EDPS. Moreover, EMA will provide data subjects with control over their personal data via a secured website portal.

150. In this regard, EMA has in place in the EV joint-controllership agreement a dedicated section on how to handle data subjects requests. Additionally, EMA

[63] https://aws.amazon.com/compliance/sub-processors/.
[64] DPIA, pp. 97-98.

mentions that it will also enter into an agreement with the processor for handling data subjects' requests.

151. Furthermore, it is said in the DPIA that EMA's DPO is available to manage any data protection related request.

152. The contact details of both EMA and its DPO are provided in the data protection notice. Therefore, **the EDPS considers that EMA has put forward mitigating measures that address the risk of EMA's lack of policies and mechanisms to handle and reply to questions and complaints from data subjects regarding the EV SSAP.**

3.3.13. Lawfulness

153. Despite not being seen as a high risk in the DPIA, the assessment of the adequate legal basis will be analysed in this Opinion, in light of its relevance for the lawfulness of the entire processing operations and for the sake of completeness.

154. The processing of any personal data is only lawful if at least one of the grounds for lawfulness listed in Article 5(1) EUDPR is applicable. For the processing of special categories of personal data, including data concerning health, one of the requirements of Article 10(2) EUDPR must also be fulfilled. According to EMA, the proposed ground for the lawfulness of the processing operation, i.e. processing of personal data for pharmacovigilance purposes, is grounded on **Article 5(1)(a) EUDPR**, since the **processing is necessary for the performance of a task carried out in the public interest**, as detailed in the legislation mentioned below.

155. In accordance with Article 24(1) of Regulation (EC) No 726/2004[65], EMA, in collaboration with EU Member States and the European Commission, has set up and

[65] Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency (Consolidated version : 28/01/2019); ELI: http://data.europa.eu/eli/reg/2004/726/2019-01-28
Article 24
1. The Agency shall, in collaboration with the Member States and the Commission, set up and maintain a database and data processing network (hereinafter the 'Eudravigilance database') to collate pharmacovigilance information regarding medicinal products authorised in the Union and to allow competent authorities to access that information simultaneously and to share it. The Eudravigilance database shall contain information on suspected adverse reactions in human beings arising from use of the medicinal product within the terms of the marketing authorisation as well as from uses outside the terms of the marketing authorisation, and on those occurring in the course of post-authorisation studies with the medicinal product or associated with occupational exposure.

maintains the EudraVigilance database and data processing network (the "EudraVigilance System") to collate and analyse pharmacovigilance information regarding medicinal products authorised in the EU and to allow NCAs to access and share that information simultaneously.

156. Chapter III of Commission Implementing Regulation (EU) 520/2012 on the performance of pharmacovigilance activities provided for in Regulation (EC) No 726/2004[66] and Directive 2001/83/EC[67] provide for the minimum requirements for the monitoring of data in EudraVigilance. The guideline on good pharmacovigilance practices (GVP): Module IX further outlines the signal management process and the roles and responsibilities of all stakeholders involved.

157. In accordance with Article 40 of Regulation (EC) No 536/2014[68] , EMA shall set up and maintain an electronic database for the reporting provided for in Articles 42 i.e. the reporting of Suspected Unexpected Serious Adverse Reactions (SUSARs) by the sponsor to EMA. That database shall be a module of the database referred to in Article 24 of Regulation (EC) No 726/2004 (the 'EudraVigilance database'). This module is referred to as EVCTM.

158. EVCTM is the pivotal point for SUSAR reporting for all clinical trials in the European Union.

159. Commission Implementing Regulation (EU) 2022/20[69] lays down the rules for the application of Regulation (EU) No 536/2014 and setting up the rules and procedures for the cooperation of the Member States in the safety assessment of clinical trials. In accordance with Article 5(1) of the IR, the safety assessing Member

[66] Commission Implementing Regulation (EU) No 520/2012 of 19 June 2012 on the performance of pharmacovigilance activities provided for in Regulation (EC) No 726/2004 of the European Parliament and of the Council and Directive 2001/83/EC of the European Parliament and of the Council Text with EEA relevance, OJ L 159, 20.6.2012, p. 5–25.

[67] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use, OJ L 311, 28.11.2001, p. 67–128.

[68] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance, OJ L 158, 27.5.2014, p. 1–76.

Article 40 (Electronic database for safety reporting)

1. The European Medicines Agency established by Regulation (EC) No 726/2004 (the 'Agency') shall set up and maintain an electronic database for the reporting provided for in Articles 42 and 43. That database shall be a module of the database referred to in Article 24 of Regulation (EC) No 726/2004 (the 'Eudravigilance database').

[69] Commission Implementing Regulation (EU) 2022/20 of 7 January 2022 laying down rules for the application of Regulation (EU) No 536/2014 of the European Parliament and of the Council as regards setting up the rules and procedures for the cooperation of the Member States in safety assessment of clinical trials (Text with EEA relevance), OJ L 5, 10.1.2022, p. 14–25.

State shall amongst other duties screen and assess information about all suspected unexpected serious adverse reactions reported in the EudraVigilance database in accordance with Article 42 of Regulation (EU) No 536/2014, regardless of whether they occurred in Member States or in third countries, as well as information contained in annual safety reports, in accordance with Articles 6 and 7 following a risk based approach.

160. In light of the above, EMA has a legal basis to perform the processing operations regarding Eudravigilance. The EDPS takes note that the replacement of the current EVDAS, which is an integral part of the EudraVigilance system by the EV SSAP does not change the legal basis for the data processing and the roles and responsibilities set out in the EudraVigilance Joint Controllership Arrangement, even though some adaptations may be required prior to the launch of the production phase[70].

161. Consequently, **EMA has a lawful ground to process personal data for pharmacovigilance and clinical trials,** including to set up and maintain an electronic database for the reporting SUSAR (EudraVigilance database)**, under Article 5(1)(a) EUDPR**.

162. Furthermore, regarding the processing of data concerning health, the EDPS considers that the **EMA meets the requirements foreseen in Article 10(2)(i) EUDPR**, since the processing of personal data related to the EV SSAP is necessary for reasons of public interest in the area of public health (e.g. pharmacovigilance), to ensure high standards of quality and safety of medicinal products, on the basis of Union Law which provides for suitable and specific measures to safeguard the rights and freedoms of data subjects.

163. Regarding the ground under Chapter V EUDPR for the transfers of personal data to third countries in the context of the EV SSAP, as already stated above in para. 8 and 33 of this Opinion, the assessment will be done separately by the EDPS in case file 2024-0532.

[70] A dedicated EV SSAP Data Protection Notice, which outlines the applicable legal bases for the data processing activities (see Annex IV of the DPIA) has been drafted.

4. CONCLUSION

164. As indicated above, in order to ensure compliance of the processing with the EUDPR, the EDPS **deems necessary** that EMA:

1. in light of the principles of lawfulness, fairness and transparency (Article 4(1)(a) EUDPR) and in light of Articles 14(1) and 16(1)(e) and (f) EUDPR, **either notify data subjects - whose personal data is already being processed - with the joint-controllers support, of the changes in EudraVigilance**, including the potential impact of the changes upon them (including stemming from new transfers of personal data outside the EEA), and the modality used to communicate the changes, and be able to demonstrate how the timeframe between notification of the changes and the change taking effect; **or EMA document the assessment and the reasons not to perform such notification of the changes to data subjects, under Articles 4(2) and 16(5) EUDPR (Recommendation 8). Otherwise, the EDPS considers that the EMA would violate the data subjects right to information under Articles 14(1), as well as 16(1)(e) and (f) EUDPR.**

2. in order to ensure the controller is implementing all the necessary technical and organisational security measures**, carefully select the trusted users receiving the** [redacted] **privileges on** [redacted] **policies in such a way as to implement the principle of least-privilege, in light of Article 33(1) EUDPR. Furthermore, the EDPS deems necessary that EMA verifies the proper implementation of the aforementioned policies (Recommendation 9).**

3. **and RxLogix develop a policy and procedure to transfer these log files to EMA for regular review. These logs should be in a readable format for EMA. On its side, EMA should implement a tool to sift through these log files in order to facilitate detecting unauthorised operations, which could lead to unauthorised access or modification of personal data in the database against the instructions of the controller. In case such unauthorised operations are detected, the security incident management process should be triggered. (Recommendation 11). Otherwise, the EDPS considers that the EMA would violate Articles 4(1)(f), 33(1)(b) and (d) and Article 33(3) EUDPR.**

4. **check which sub-processors are entailed in the use of AWS and properly assess the risks of all processors and sub-processors therein involved (Recommendation 15). Otherwise, the EDPS considers that the EMA would violate Article 29 EUDPR.**

165. Moreover, the EDPS also **recommends** that EMA:

1. following the outcome of the ongoing investigation, as well as in any future development of the EV SSAP or in any changes on how AWS provides IaaS and PaaS cloud services to EMA and its processor, **make additional assessments on whether the safeguards and measures EMA and its processor have in place for the AWS cloud services used for the EV SSAP are still effective (Recommendation 1)**;
2. following the outcome of the ongoing investigation, as well as in any future development of the EV SSAP or in any changes on how AWS provides IaaS and PaaS cloud services to EMA and its processor**, ensure additional measures are taken for the AWS cloud services used for the EV SSAP and for any new AWS or Microsoft cloud services envisaged for the EV SSAP, including changes to the contracts in order to ensure compliance with EUDPR and other EU law applicable to the data in the EudraVigilance and the EV SSAP (Recommendation 2)**;
3. **consider assessing if any measures similar to those imposed under the EDPS decision of 8 March 2024 (in particular measures under paragraphs 592.1., 592.2.1., 592.2.2., and 592.2.3. c), f) and g of that decision) need to be taken for the AWS cloud services used for the EV SSAP, including necessary changes to the contracts, and data flows to third countries (Recommendation 3);**
4. **assess not only the risks of unauthorised transfers, but also the risks of authorised transfers. Therefore, EMA has to assess potential remote access to support requests to prevent fraud and abuse and if the transfer is requested by RxLogix, including transfers by default, transfers that could be opted-out and transfers that cannot be stopped. (Recommendation 4);**
5. **mention in the DPIA specific examples of the communication channels that will be used to inform the data subjects (i.e. displayed as a data subject fills in an online form) (Recommendation 5);**
6. use a table of contents with hyperlinks to the respective sections of the data protection notice at the beginning, as well as a 'in a nutshell' initial section with the **information on the processing activity which has the most impact on the data subjects (i.e., safety monitoring activities), the purposes of the processing operations, the identification of the joint-controllers and a description of the data subject's rights**, in line with the principle of fairness (Article 4(1)(a) EUDPR) **(Recommendation 6);**

7. wherever possible, provide the information about the risks, rules, safeguards and data subjects rights regarding the processing of their personal data well in advance[71], namely with the support of the other joint-controllers. Therefore, **the EDPS recommends that EMA contact the other joint-controllers to provide the data protection notice to data subjects as soon as possible (Recommendation 7);**
8. **document the envisaged time limits for erasure of the different categories of data in the corresponding record of processing activity (EV SSAP ROPA), in accordance with Article 31(1)(f) EUDPR (Recommendation 10);**
9. **either apply [redacted] or ensure using the most up-to-date cryptographic settings for [redacted] (Recommendation 12);**
10. **either audit the source code of the upload application or ensures that the only upload destination is the RxLogix-owned [redacted] database (Recommendation 13);**
11. **systematically include, in any process which uses such [redacted], the obligation by EMA to check the activity (logs) of the [redacted] (Recommendation 14).**

166. The EDPS expects that EMA **implement recommendations Nos 8, 9, 11 and 15 and provides documentary evidence** of this implementation within **three months** of this Supervisory Opinion.

167. In light of the accountability principle, the EDPS expects that EMA **implement the other recommendations** (Nos 1, 2, 3, 4, 5, 6, 7, 10, 12, 13 and 14).

168. The EDPS expects to be consulted on any significant update of the DPIA as a result of a substantial modification of the personal data processing operations at stake.

Done in Brussels

Wojciech Wiewiórowski

Digitally signed by:
WOJCIECH RAFAŁ
WIEWIÓROWSKI (EUROPEAN
DATA PROTECTION SUPERVISOR)
Date: 2024-10-16 13:12:17 UTC

[71] Article 29 Working Party - Guidelines on transparency under Regulation 2016/679 (last revised and adopted on 11 April 2018), p. 16.