1 July 2022
EMA/137320/2022 – endorsed
Data Analytics and Methods

Joint Controllership Arrangement

With regard to EudraVigilance Human (EV)

Amongst the **European Commission** (hereinafter referred to as 'Commission' or 'European Commission'),

the **European Medicines Agency** (hereinafter also referred to as 'the Agency' or 'EMA'), and

the **Member States of the European Union (EU)/European Economic Area (EEA)** (hereinafter referred to as 'MS' or 'Member States') represented by **National Competent Authorities** (hereinafter referred to as 'NCAs').

Each of them a 'Party' and hereinafter collectively referred to as 'Parties', to be considered as 'joint controllers' for the purpose of processing personal data captured in EudraVigilance Human (EV) administered by EMA and covering the following system components:

1. EudraVigilance Gateway – the data processing network;
2. EudraVigilance Database Management system comprising the EudraVigilance Clinical Trials Module (EVCTM), the EV Post-Authorisation Module (EVPM) and data quality management functionalities (recoding and duplicate detection);
3. EudraVigilance web reporting application (EVWEB) including Individual Case Safety Report (ICSR) creation, submission, re-routing to NCAs of Member States, querying and for EVPM ICSR download by marketing authorisation holders;
4. EudraVigilance Data Warehouse and Analysis System (EVDAS) including signal detection, safety monitoring and data analysis functionalities;
5. Public Adverse Drug Reaction Reports portal (ADRReports.eu);
6. Extended Medicinal Products Dictionary (xEVMPD).

Having regard to 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;

Having regard to 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;

Having regard to 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;

Having regard to the 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;

Having regard to the Commision 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;

Having regard to 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 (hereinafter, Regulation (EU) 2018/1725), and in particular Article 28 thereof;

Having regard to 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 (hereinafter, Regulation (EU) 2016/679), and in particular Article 26 thereof;

Having regard to the functional specifications as referred to in Article 24, paragraph 2 of Regulation (EC) No 726/2004, as defined in the "EudraVigilance functionalities to be audited" (EMA/626168/2013).

Whereas:

(i) Article 28 of Regulation (EU) 2018/1725 establishes that where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers, who by means of an arrangement between them, shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the Data Subject and their respective duties to provide the information referred to in Articles 15 and 16 of Regulation (EU) 2018/1725;

(ii) Article 26 of Regulation (EU) 2016/679 establishes that where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers, who by means of an arrangement between them, shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the Data Subject and their respective duties to provide the information referred to in Articles 13 and 14 of Regulation (EU) 2016/679;

(iii) Article 24(1) of Regulation (EC) No 726/2004 stipulates that 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;

(iv) Article 57(2) of Regulation No 726/2004 establishes that the Agency, shall for the purposes of the database provided for in paragraph 1(l), set up and maintain a list of all medicinal products for human use authorised in the Union;

(v) Article 40(1) of Regulation (EU) No 536/2014 stipulates that 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');

(vi) Article 40(2) of Regulation (EU) No 536/2014 stipulates that the Agency shall, in collaboration with Member States, develop a standard web-based structured form for the reporting by sponsors to the database referred to in paragraph 1 of suspected unexpected serious adverse reactions;

(vii) Article 81(3) of Regulation (EU) No 536/2014 establishes that the EU database[1] shall support the recording and submission to the Medicinal Product Dictionary, contained in the Eudravigilance database, of all the data on medicinal products without a marketing authorisation in the Union and substances not authorised as part of a medicinal product in the Union, that are necessary for the maintenance of that dictionary;

(viii) This Joint Controllership Arrangement (JCA) has been drawn up by the Agency, in cooperation with the European Commission, and Member States, involved through their appointed NCA(s) representatives.

Have agreed as follows:

1. Scope of this arrangement

1.1 This Arrangement sets out the allocation of respective roles, responsibilities, and practical arrangements between the Parties for compliance with their data protection obligations under Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively, when carrying out processing operations of personal data of data subjects, collected as part of the use of EV.

Each Party may appoint authorised users (including assigning their roles and permissions) affiliated to that Party to access and use EV on its behalf (including by way of example and without limitation: NCAs, the Commission), each of them a 'user' for the purpose of this Arrangement[2].

1.2 For the purpose of this Arrangement, the definitions laid down in Article 3 of Regulation (EU) 2018/1725 and Article 4 of Regulation (EU) 2016/679, respectively shall apply.

1.3 This Arrangement governs the processing of personal data in EV as necessary for the activities carried out in accordance with, amongst others, the principles set out in Article 24 of Regulation (EC) No 726/2004 and Article 40 of Regulation (EU) No 536/2014 (hereafter, 'processing operation'). A description of categories of personal data processed in EV and categories of data subjects concerned is included in the Data Protection Notice enclosed as Annex II.

1.4 In support of the supervision of the safety of medicinal products studied in clinical trials and authorised in the EU, a data processing operation, which may include personal data, consists of the processing activities[3] performed by the Party responsible for that task:

a. Processing activity performed by the **European Commission** users, in the secure, access-controlled domain of EV includes the:

[1] The Clinical Trial Information System
[2] Following approval of this EV JCA and subsequent login to EV, authorised users will be requested to accept the EV JCA once and each time an updated version is available.
[3] This is not an exhaustive list of processing activities but indicative of the main processing operations under consideration

- registration and administration of users of the Commission and the members appointed by the Commission in accordance with Article 61a(1)(b) of Regulation (EC) No 726/2004;
- viewing information on the responsible person for pharmacovigilance/EV;
- operating of searches and generation of reports in EV;
- viewing and downloading of data, reports and outputs.

b. Processing activity performed by the **Member States** users, in the secure, access-controlled domain of EV includes the:
   - registration and administration of NCA users;
   - viewing information on the responsible person for pharmacovigilance/EV;
   - creation and/or submission of Individual Case Safety Reports (ICSRs);
   - receiving ICSRs rerouted by means of EV (clinical trials and post-authorisation phase);
   - operating of searches and generation of reports in EV;
   - receiving and assessing signal detection monitoring reports;
   - performing screening and assessment of suspected unexpected serious adverse reactions (SUSARs) originating from clinical trials;
   - viewing and downloading of data, reports and outputs.

c. Processing activity performed by the **European Medicines Agency** users, in the secure, access-controlled domain of EV include:
   - user registration to generate credentials for users;
   - recording of contact details of the Qualified Person Responsible for Pharmacovigilance;
   - maintenance of EV including responsibility for data storage;
   - ensuring technical support to all users of EV in case of troubleshooting;
   - In the area of pharmacovigilance:
     - recording and storing of ICSRs submitted by NCAs and marketing authorisation holders (MAHs) to EV;
     - user access management in accordance with Article 24(2) of Regulation (EC) No 726/2004 and the EV Access Policy (in the latest version);
     - re-routing of ICSRs to NCAs in Member States;
     - operating of searches and generation of reports in EV;
     - creating and distributing signal detection monitoring reports;
     - assessing signals and safety issues;
     - publishing information on reports of suspected adverse reactions on the adrreports.eu portal;
     - sharing of information on suspected adverse reactions with the World Health Organisation in accordance with Article 28c(1) of Regulation (EC) No 726/2004 and agreed modalities for the transfer of such information[4].
   - In the area of clinical trials:
     - recording and storage of ICSRs submitted by sponsors of clinical trials[5] to EVCTM;
     - re-routing of ICSRs to NCAs in Member States;
     - operating of searches and generation of reports in EV;
     - facilitating the creation of safety monitoring reports for SUSARs by NCAs in Member States.

[4] World Health Organization (WHO) | European Medicines Agency (europa.eu)
[5] It should be noted that Article 42(3) of Regulation (EU) 536/2014 states that where a sponsor, due to a lack of resources, does not have the possibility to report to the database referred to in Article 40(1) and the sponsor has the agreement of the Member State concerned, it may report to the Member State where the suspected unexpected serious adverse reaction occurred. That Member State shall report the suspected unexpected serious adverse reaction in accordance with paragraph 1 of this Article.

- Medical Literature Monitoring (MLM):
  - creating, submitting, recording and storage of ICSRs resulting from the selected medical literature monitoring obligations as set out in Article 27 of Regulation (EC) No 726/2004;
- Duplicate detection and data quality management:
  - detecting and managing duplicates of ICSRs submitted by multiple senders;
  - creating of master cases;
  - making available medicinal product information in the XEVMPD and recoding of information reported in ICSRs against the XEVMPD;
  - reviewing of data quality of ICSRs submitted to EV.

1.5 **Section 2a** below provides further details on activities carried out by the Parties that are **out of the scope of the use** of EV, and therefore out of scope of this Arrangement, and are carried out by the Parties separately as individual and independent data controller for such activities.

2. Controllers and Joint Controllers

2.1. For the purpose of this Arrangement, the Parties are considered as 'controllers' within the meaning of point (8) of Article 3 of Regulation (EU) 2018/1725 and point (7) of Article 4 of Regulation (EU) 2016/679, respectively.

2.2. The Parties act collectively as Joint Controllers, and each of them as a Joint Controller, pursuant to Article 28 of Regulation (EU) 2018/1725 and Article 26 of Regulation (EU) 2016/679, in relation to the processing activities as described in point 1.4 above.

Section 2a – Processing activities which fall out of scope of the Joint Controllership Arrangement

2a.1. The processing activities explained in this Section 2a performed by the Joint Controllers, as part of their remit and out of the scope of the use of EV, fall outside the scope of this Arrangement.

2a.2. The **European Commission** acts as individual controller in relation to the processing activities carried out within its organisation, whether related to the supervision activities in relation to the implementation of the Regulation (EU) No 536/2014 and Regulation (EC) No 726/2004, or not, that are performed outside of EV. The Commission also acts as individual controller when it extracts from, and analyses outside of EV any data submitted to EV. It is the sole responsibility of the Commission to ensure compliance with all obligations and conditions of Regulation (EU) 2018/1725 regarding the activities performed as individual controller.

2a.3. The **EU Member States**, **represented by National Competent Authorities**, act as individual controllers in relation to the data processing activities carried out within their organisation, that are performed outside of EV. They also act as individual controllers when they extract from and analyse outside of EV any data submitted to EV. It is the sole responsibility of the Member States, represented by NCAs, to ensure compliance with all obligations and conditions of Regulation (EU) 2016/679 regarding the activities performed as individual controllers.

2a.4. The **European Medicines Agency** acts as individual controller in relation to the processing activities carried out within their organisation, performed outside of EV, for example:

- Initial user registration in the EMA Account Management (EAM) system[6].

[6] Please see the EMA Privacy statement regarding such user registration: https://www.ema.europa.eu/en/documents/other/european-medicines-agencys-privacy-statement-ema-account-management-system_en.pdf

The Agency also acts as individual controller when they extract from and analyse outside of EV any data submitted to EV. It is the sole responsibility of the European Medicines Agency to ensure compliance with all obligations and conditions of Regulation (EU) 2018/725 regarding the activities performed as individual controller.

3. Responsibilities, roles and relationship towards Data Subjects

In order to guarantee compliance with applicable data protection rules, each of the Parties shall comply with the general principles of data protection, as laid down in Article 4 of Regulation (EU) 2018/1725 and Article 5 of Regulation (EU) 2016/679, respectively.

3.1. Provision of information to Data Subjects

A Data Protection Notice is published on the public domain portal of EV to ensure that data subjects are informed of the details of the processing activity carried out in EV.

As regards the activities listed in Section 2a, each Party is solely responsible to comply with its obligations as an individual controller to inform data subjects about the processing of their personal data.

3.2. Handling of Data Subject requests

The data subjects may exercise their rights under Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively, in respect of and against each of the Parties.

Each Party shall handle data subject requests raised in connection with the information that they provide to EV in accordance with their internal process and applicable data protection requirements. Reference to the relevant contact points for every Party can be found in Annex I.

The Parties shall cooperate and, when so requested, provide each other with swift and efficient assistance in handling any data subject requests in accordance with the following steps:

I. When a Party receives a data subject request, it must check whether the request concerns activities carried out by that Party in accordance with Section 1.4 above.
a. If the request falls under that Party's activities as listed in Section 1.4, then the receiving Party will be responsible to handle the request. It shall send an acknowledgment of receipt to the data subject without undue delay and shall handle the request in accordance with applicable data protection legislation *(in this case, go to step V).*
b. If it appears that more Parties are concerned by the handling of the request then the receiving Party shall, without undue delay, liaise with parties and if necessary, call a meeting with the Parties concerned at the latest within three working days of its receipt *(in this case, go to step IV, otherwise go to step II).*
II. If the receiving Party finds that the request concerns activities which belong to another Party in accordance with Section 1.4 above, it shall forward the request to that other Party.

a. The request shall be forwarded by using secure means of transmission (e.g., Eudralink) and without undue delay, at the latest within five working days of its receipt. Within the same deadline, the receiving Party shall inform the data subject about forwarding the request and also clearly state to which Party the request has been forwarded *(go to step III).*

III. The Party to whom the request has been forwarded must check whether it agrees to be responsible to handle the request.

a. If the Party accepts being the responsible Party to handle the request, then it shall send an acknowledgment of receipt to the data subject without undue delay, at the latest within ten working days and shall handle the request in accordance with applicable data protection legislation *(in this case, go to step V).*

b. If the Party does not accept being the responsible Party to handle the request or it considers that more Parties should be involved, then it shall, without undue delay, call a meeting with the receiving Party and with any other Party or Parties concerned, at the latest within three working days of its receipt (*in this case, go to step IV).*

IV. The Parties involved shall agree on a process to handle the request together (or to be handled solely by one Party) in accordance with applicable data protection legislation. They shall provide any information and assistance required to address the request.

a. Unless the Parties agree otherwise, the final reply to the request shall be sent by the receiving Party. In any case, a confirmation should be sent to the data subject as soon as possible, at the latest within ten working days from the original receipt of the reply, about which Party will send the final reply to the request *(go to step V).*

V. The Party (or Parties) handling a data subject request shall provide information on action taken on a request to the data subject without undue delay and at the latest within one month of receipt of the request. That period may be extended by two further months where necessary[7], taking into account the complexity and number of the requests pursuant to Article 14(3) of Regulation (EU) 2018/1725 and Article 12(3) of Regulation (EU) 2016/679, respectively.

Exchanges with the data subject(s) shall be handled solely by the Party(ies) receiving a data subject request, whilst all other Parties shall cooperate upon request of the Party(ies) directly involved. Data can be corrected by the relevant Parties with an update done directly in EV - as regards ICSRs by means of an amendment report in accordance with the ICH E2B(R3) standard-, while where the handling of the request requires removal of data stored within EV, EMA will be responsible for such removal and will liaise to that effect with the Party originally providing the data in EV. In such cases, the responses and the final reply to the data subject shall be sent by the Party who received the request or the Party who originally submitted the data concerned.

[7] It is to note that the controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

As regards the activities listed in Section 2a, each Party is responsible alone to reply to data subject requests and allow data subjects to exercise their rights under Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively.

3.3. Management of security incidents, including personal data breaches

The Parties shall handle security incidents, including personal data breaches, in accordance with their internal procedures and applicable legislation.

The Parties shall, in particular, provide each other with swift and efficient assistance as required to facilitate the identification and handling of any security incidents, including personal data breaches, linked to the joint processing.

The Parties shall notify each other of the following within the scope of this Arrangement in accordance with Annex I:

a. Any risks that are reasonably likely to result in damage to the availability, confidentiality and/or integrity of the personal data undergoing joint processing;

b. Any security incidents actually or potentially affecting personal data that are linked to the joint processing operation;

c. Any personal data breach (i.e., any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data undergoing joint processing), the likely consequences of the personal data breach and the assessment of the risk to the rights and freedoms of natural persons, and any measures taken to address the personal data breach and mitigate the risk to the rights and freedoms of natural persons;

d. Any breach of the technical and/or organisational safeguards of the joint processing operation.

Each Party is responsible for managing all security incidents, including personal data breaches, that occur as a result of an infringement of that Party's obligations under this Arrangement and Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively.

The responsible Party(ies) shall document the security incident (including personal data breaches) and notify the other Parties without undue delay and at the latest within 48 hours after becoming aware of a security incident (including a personal data breach).

The Party responsible for managing a personal data breach incident shall create and maintain appropriate records of the incident and notify it to the European Data Protection Supervisor or the competent national supervisory authority in accordance with Article 34 of Regulation (EU) 2018/1725 and Article 33 of Regulation (EU) 2016/679, respectively.

It shall do so without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The Party responsible shall inform the other Parties of such notification.

The Party responsible for the personal data breach shall communicate that personal data breach to the data subjects concerned if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The Party responsible shall inform the other Parties of such communication.

The communication to the data subjects referred to in the previous paragraph shall not be necessary if any of the conditions listed in Article 35(3) of Regulation (EU) 2018/1725 and Article 34(3) of Regulation (EU) 2016/679, respectively, are met.

3.4. Responsibility for the security of processing

The Agency shall implement appropriate technical and organisational measures to ensure the security of processing personal data in EV pursuant to Article 33 of Regulation (EU) 2018/1725.

Each Party shall implement appropriate organisational measures to ensure the security of processing pursuant to Article 33 of Regulation (EU) 2018/1725 and Article 32 of Regulation (EU) 2016/679, respectively.

Access to personal data stored in the in the secure, access-controlled domain of EV undergoing joint processing shall only be allowed to authorised staff/personnel/authorised users of the Parties acting as data processors, for the purposes of administering, operating and using the IT system which facilitates the processing operation. This access shall be subject to ID and password requirements.

3.5. Processors

When using a processor, each Party shall ensure the compliance of such processing pursuant to Article 29 of Regulation (EU) 2018/1725 and Article 28 of Regulation (EU) 2016/679, respectively.

3.6. Localisation of personal data

The data centres used for EV are stored in the following EU countries: Netherlands, Ireland, and Germany.

Where personal data is made available to the public on the adrreports.eu portal and is accessed from outside the EU/EEA, this is based on Article 50(1)(g) of Regulation (EU) 2018/1725, or Article 49(1)(g) of Regulation (EU) 2016/679, i.e. the transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case.

If a Party authorises a user to access the secure domain of EV from outside the EU/EEA, that Party shall ensure that an appropriate data transfer mechanism is established prior to any access by that user, and that such international data transfers comply with the rules of Chapter V of Regulation (EU) 2018/1725 or Regulation (EU) 2016/679, respectively.

3.7. Other responsibilities of the Joint Controllers:

Without prejudice to obligations of Joint Controllers that may be applicable based on national laws, the Joint Controllers shall be responsible for the following:

a. Recording of the processing operation;

b. Ensuring that the personal data undergoing processing are adequate, accurate, relevant, and limited to what is necessary for the purpose;

c. Ensuring a transparent information and communication to data subjects of their rights;

d. Facilitating the timely exercise of the rights of data subjects;

e. Handling of data subjects' requests in accordance with the procedure adopted;

f. Deciding to restrict the application of, or derogate from data subject rights, where necessary and proportionate, in accordance with internal rules adopted by the Party in compliance with Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively;

g. Ensuring privacy by design and privacy by default;

h. Identifying and assessing the lawfulness, necessity and proportionality of transmissions and transfers of personal data;

i. Carrying out a data protection impact assessment;

j. Carrying out a prior consultation with the European Data Protection Supervisor, or other competent national supervisory authority, where needed;

k. Ensuring that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

l. Cooperating with the European Data Protection Supervisor or other competent national supervisory authority, on request, in the performance of his or her tasks.

4. Liability for non-compliance

Without prejudice to the liability stemming from processing activities performed outside of EV as outlined in Section 2.a above:

(i) the Agency and the Commission shall be liable for non-compliance with the provisions of Regulation (EU) 2018/1725, for the role and activities performed in accordance with Sections 1 and 3 of this Arrangement.

(ii) the Member States shall be liable for non-compliance with the provisions of Regulation (EU) 2016/679, each for the role and activities performed in accordance with Sections 1 and 3 of this Arrangement.

5. Cooperation between the Parties of this Arrangement

Each Party, when so requested, shall provide a swift and efficient assistance to the other Parties in execution of this Arrangement, while complying with all applicable requirements of Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively, and other applicable national rules on data protection.

6. Acknowledgement of this Arrangement by the users

A hyperlink to this Arrangement will be displayed to EV users at the time of the log in, in EV. By accessing the system, the users will acknowledge that they are familiar with the contents of the JCA and that they have received and understood the Data Protection Notice attached to the JCA as Annex II. They will be required to do so once and thereafter when a new or amended version of this Agreement will become applicable.

Should a new, or amended version of this Arrangement be available, a hyperlink to the revised text will be displayed to the users before they can further progress with the use of EV.

7. Effective Date

This Arrangement has received the consent of the representatives of the Parties in June 2022 and has been submitted for endorsement to the EMA Management Board meeting on June 2022, with the understanding that all users of the EV access-controlled domain undertake to comply with as a condition to using EV system from Q4 2022 onwards.

Should any amendments to this Arrangement become necessary, this will follow the adoption procedure involving representatives of the Joint Controllers as referred to in Recital 3 of this Arrangement.

This Arrangement is effective as from the date above written and shall continue to be effective as long as the EV system will be in use.

Annex I

Contact points:

Contact points for cooperation between the Parties and for Data Subjects

Each Party nominates a single point of contact, whom other Parties can contact in respect of queries, complaints, and provision of information within the scope of this Arrangement.

European Medicines Agency:
Functional email: datacontroller.analytics@ema.europa.eu

European Commission: sante-consult-b5@ec.europa.eu

European Member States:

Member State	Contact Point
Austria	Datenschutz-BASG@basg.gv.at
Belgium	dpo@fagg.be
Bulgaria	dpo@bda.bg
Croatia	osobnipodaci@halmed.hr
Cyprus	phv@phs.moh.gov.cy
Czech Republic	poverenec@sukl.cz
Denmark	dju@dkma.dk
Estonia	
Finland	tietosuojavastaava@fimea.fi
France	Evelyne.PIERRON@ansm.sante.fr Corinne.KIGER@ansm.sante.fr Frederic.DITTENIT@ansm.sante.fr
Germany (BfArM)	Clinical Trials related matters: ct@bfarm.de Pharmacovigilance related matters: uaw@bfarm.de
Germany (PEI)	Datenschutz@pei.de
Greece	dpo@eof.gr
Hungary	adatvedelem@ogyei.gov.hu
Iceland	personuvernd@lyfjastofnun.is
Ireland	dataprotectionofficer@hpra.ie
Italy	responsabileprotezionedati@aifa.gov.it
Latvia	personas.dati@zva.gov.lv
Liechtenstein	Vlasta.Zavadova@llv.li
Lithuania	NepageidaujamaR@vvkt.lt

Member State	Contact Point
Luxembourg	info_donnees@ms.etat.lu
Malta	
Netherlands	privacy@cbg-meb.nl and privacy@igj.nl
Norway	personvern@legemiddelverket.no
Poland	iod@urpl.gov.pl
Portugal	dpo@infarmed.pt
Romania	
Slovakia	zodpovednaosoba@sukl.sk
Slovenia	dpo@jazmp.si
Spain	delegado_protecciondatos@aemps.es
Sweden	kp.central@lakemedelsverket.se

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Annex II:

European Medicines Agency's Data Protection Notice for EudraVigilance Human (EV)

This Data protection notice explains the most essential details of the processing of personal data in the context of the operation of EudraVigilance Human (EV) established in accordance with the requirements of Article 24(1) of Regulation (EU) No 726/2004[8]. The European Medicines Agency (hereafter referred to as "the Agency"), in collaboration with Union Member States and the European Commission, has set up and maintains the EudraVigilance database and data processing network[9] to collate and analyse information on suspected adverse reactions regarding investigational medicinal products (IMPs) studied in clinical trials and medicinal products authorised in the EU. This is to allow national Competent Authorities (NCAs), the Agency and the Commission to access and share that information simultaneously. Whilst EV is operated by the Agency, its content originates from NCAs, marketing authorisation holders (MAHs) and sponsors of clinical trials.

This Data Protection Notice explains the most essential details of the processing of personal data by the Agency, which includes:

- the area of **pharmacovigilance**[10] and information on suspected adverse drug reactions (ADRs) originating from patients, health care professionals and other sources, which is reported to EV by NCAs and MAHs, thus supporting the continuous safety of medicines[11];
- the area of **clinical trials**[12] and information on suspected unexpected serious adverse reactions (SUSARs) reported by sponsors[13] to EV thus allowing NCAs to evaluate whether an IMP poses an unknown risk to the trial subject and to take measures to protect the safety of trial subjects, if necessary[14].

[8] CL2004R0726EN0080010.0001.3bi_cp 1..1 (europa.eu)
[9] EudraVigilance | European Medicines Agency (europa.eu)
[10] Pharmacovigilance: Overview
[11] Title IX, Chapter 3 of Directive 2001/83/EC, Title II, Chapter 3 of Regulation (EC) 726/2004 and Chapters III, IV and V of the Commission Implementing Regulation (EU) 520/2012
[12] CHAPTER VII SAFETY REPORTING IN THE CONTEXT OF A CLINICAL TRIAL of Regulation 536/2014
[13] It should be noted that Article 42(3) of Regulation (EU) 536/2014 states that where a sponsor, due to a lack of resources, does not have the possibility to report to the database referred to in Article 40(1) and the sponsor has the agreement of the Member State concerned, it may report to the Member State where the suspected unexpected serious adverse reaction occurred. That Member State shall report the suspected unexpected serious adverse reaction in accordance with paragraph 1 of this Article.
[14] Regulation (EU) No 536/2014

Official address Domenico Scarlattilaan 6 ● 1083 HS Amsterdam ● The Netherlands
Address for visits and deliveries Refer to www.ema.europa.eu/how-to-find-us
Send us a question Go to www.ema.europa.eu/contact **Telephone** +31 (0)88 781 6000 An agency of the European Union

The joint controllers ensure that processing of personal data in the context of the operation of EV complies with all applicable requirements of Regulation (EU) 2018/1725[15] (EUDPR) and Regulation (EU) 2016/679[16] (GDPR), respectively, and other applicable national rules on data protection.

1. Who is responsible for your data?

1.1. Who are the joint controllers?

The joint controllers under the Joint Controllership Arrangement (JCA) are the European Medicines Agency, the European Commission and National Competent Authorities in Member States of the EU/EEA.

The Parties of the Joint Controllership Arrangement act as joint controllers for the purpose of processing operations in EV of personal data provided in structure data and supporting documents.

The contact points of the joint controllers are the following:

- **European Medicines Agency:** datacontroller.analytics@ema.europa.eu
- **European Commission:** sante-consult-b5@ec.europa.eu
- **Member States:** Annex I of the JCA

The respective roles and relationship vis-à-vis data subjects are explained in the JCA. In accordance with the applicable rules of the EUDPR and GDPR, data subjects may exercise their rights under the Regulations in respect of, and against each of, the joint controllers. In order to ensure that any request can be handled as swiftly as possible, it is recommended that data subject contacts the joint controller who, in line with the activities allocated in the JCA, collected, and mainly processes the personal data concerned.

It should be noted that marketing authorisation holders and sponsors of clinical trials are separate controllers for their personal data processing activities carried out pursuant to the pharmacovigilance and clinical trials legislation, as applicable.

1.2. Who is the data processor?

The Agency engages third parties to provide support for the:

- maintenance of EV functionalities,
- development of EV functionalities,
- monitoring of a number of substances and selected medical literature to identify suspected adverse reactions with medicines authorised in the EU, and for entering the relevant information into EV[17],
- management of duplicated ADR reports submitted to EV[18],
- assurance of data quality in EV,

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[17] Monitoring of medical literature and entry of adverse reaction reports into EudraVigilance
[18] Guideline on good pharmacovigilance practices (GVP) Module VI Addendum I – Duplicate management of suspected adverse reaction reports (EMA/405655/2016)

- provision of system support to EV users.

Contact details of the EMA processors (and, if necessary, of other Parties' processors), can be made available to the data subjects upon request.

2. Purpose of this data processing

The purpose of the EV data processing activities can be summarised as follows:

- User registration and access management;
- Maintenance of EV including responsibility for data storage;
- Ensuring technical support to all users of EV in case of troubleshooting;

a. In the area of pharmacovigilance:

- Electronic submission of Individual Case Safety Reports (ICSRs) by NCAs and MAHs containing information on suspected adverse reactions related to medicines as initially reported by patients[19], healthcare professionals or other sources;
- Rerouting of ICSRs reported by MAHs to NCAs in Member States where the suspected adverse reactions occurred;
- Conduct of searches and generation of reports (e.g., safety monitoring and signal detection), based on data held in EV, including extraction and analysis of this data outside of the system by authorised users (see section 4);
- Publishing information on reports of suspected adverse reactions on the adrreports.eu portal;
- Sharing of information on suspected adverse reactions with the World Health Organisation in accordance with Article 28c(1) of Regulation (EC) No 726/2004 and agreed modalities for the transfer of such information[20].

b. In the area of clinical trials:

- Electronic submission of ICSRs by sponsors and/or NCAs containing information on suspected unexpected serious adverse reactions (SUSARs) related to investigational medicinal products (IMPs) studied in clinical trials;
- Rerouting of SUSARs reported by Sponsors to NCAs in Member States in accordance to the SUSAR rerouting criteria previously defined by the NCAs;
- Conduct of searches by NCAs and generation of reports (e.g., safety monitoring) based on data held in EV, including extraction and analysis of this data outside of the system by authorised users (see section 4).

c. In the area of Medical Literature Monitoring (MLM):

- Creating, submitting, recording and storing of ICSRs by the Agency resulting from the selected medical literature monitoring obligations as set out in Article 27 of Regulation (EC) No 726/2004;

d. In the area of duplicate detection and data quality management

- Detecting and managing duplicates of ICSRs submitted by multiple senders by the Agency;

[19] Did you know? You can report side effects yourself
[20] World Health Organization (WHO) | European Medicines Agency (europa.eu)

- Creating master cases based on confirmed duplicates by the Agency;
- Making available medicinal product information in Extended Medicinal Product Dictionary (XEVMPD) and recoding of medicinal product information reported in ICSRs against the XEVMPD by the Agency;
- Reviewing of data quality of ICSRs by the Agency.

2.1. Categories of personal data concerned

Personal data refer to any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by an identifier such as name, an identification number or others[21].

The content of ICSRs is defined by legislation[22] with the minimum reporting criteria further set out in good pharmacovigilance practice guidance (GVP) Module VI[23] and Regulation 536/2014.
Examples of personal data that can be processed by NCAs, MAHs and sponsors of clinical trials for the reporting of suspected adverse reactions are name, address or phone number of a healthcare professional/investigator, a patient's email address (name.surname@xxxx.com) or details regarding an identified or identifiable patient's health or personal characteristics (e.g., age, gender).

NCAs, MAHs and sponsors of clinical trials pseudonymise such information before submission to EV, while ensuring that reports still contain sufficient information to allow for the safety monitoring and assessment of medicines. Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person[24].

NCAs, MAHs and sponsors of clinical trials assign a unique identifier to each ICSR so they can follow-up reports and when submitted to EV, the ICSRs can be adequately processed, and duplicates detected and managed. Rules are in place prohibiting re-identification of data subjects with the exception where NCAs, MAHs or sponsors of clinical trials need to follow-up with the initial reporter of the suspected adverse reaction(s).

GVP Module VI[25] also sets out the obligations as regards the monitoring of public sources such as medical literature, internet or digital media including social media. This may involve the processing of personal data as part of ADR reports originating from such public sources, which are important to support the monitoring of the safety and the risk-benefit balance of medicinal products, particularly in relation to the detection of new safety signals or emerging safety issues.

2.2. Legal Basis

EV related personal data processing operations are expressly provided for in the pharmaceutical legislation[26] and in relevant national provisions and are necessary for the performance of tasks carried

[21] Definition in accordance with Article 3(1) of 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)
[22] Article 28 of the Commission Implementing Regulation (EU) 520/2012 and Regulation No (EU) 536/2014
[23] Guideline on good pharmacovigilance practices (GVP) Module VI – Collection, management and submission of reports of suspected adverse reactions to medicinal products (Rev 2)
[24] Article 3(6) of Regulation (EU) 2018/1725.
[25] Guideline on good pharmacovigilance practices (GVP) Module VI – Collection, management and submission of reports of suspected adverse reactions to medicinal products (Rev 2)
[26] EudraLex - Volume 1 - Pharmaceutical legislation for medicinal products for human use

out in the public interest. They refer the purpose of the protection of health by setting standards of quality and safety for medicinal products. In particular, the processing of data is provided for under:

- Title II, Chapter 3 of Regulation (EC) No 726/2004[27] as regards the pharmacovigilance obligations for centrally authorised medicinal products;
- Title IX, Chapter 3 of Directive 2001/83/EC[28] and the obligations for the recording, reporting and assessment of pharmacovigilance data relating to non-centrally authorised medicinal products;
- Chapter VII of Regulation (EU) No 536/2014 and the obligations relating to the performance of safety reporting and assessment;
- Chapter IV[29] of the Commission Implementing Regulation (EC) No 520/2012, which sets out the rules on the format and content for the submission of reports of suspected adverse reactions and Chapter V[30] lays down the principles for the transmission of reports of suspected adverse reactions including the content of such reports;
- Chapter III[31] of the Commission Implementing Regulation (EC) No 520/2012, which defines the minimum requirements for the monitoring of data in the EV database with further details on the signal management process provided for in GVP Module IX[32]
- Chapter II of the Commission Implementing Regulation (EU) 2022/20, which describes the rules and procedures for the cooperation of the Member States in safety assessment of clinical trials

The processing operations which are necessary for compliance with a legal obligation to which the joint controllers are subject to can therefore be justified under Article 5(1)(b) of the EUDPR and Article 6(1)(c) of the GDPR and the corresponding appropriate condition for lawful processing of special categories of data in the context of these obligations is Article 10(2)(i) of the EUDPR and Article 9(2)(i) of the GDPR.

2.3. Transfer of personal data outside of EU

The data centres used for EV are stored in the following EU countries: Netherlands, Ireland, and Germany. Where personal data is made available to the public via the adrreports.eu portal and is accessed from outside the EU/EEA, this is based on Article 50(1)(g) of Regulation (EU) 2018/1725, or Article 49(1)(g) of Regulation (EU) 2016/679, i.e. the transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case.

[27] Title II "Authorisation and supervision of medicinal products for human use", Chapter 3 "Pharmacovigilance" of 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
[28] Title IX "Pharmacovigilance", Chapter 3 "Recording, reporting and assessment of pharmacovigilance data" of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2 DIRECTIVE 2001/83/EC on the Community code relating to medicinal products for human use.
[29] CHAPTER IV "Use of terminology, formats and standards" Commission Implementing Regulation (EU) 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.
[30] CHAPTER V "Transmission of reports of suspected adverse reactions" Commission Implementing Regulation (EU) 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.
[31] CHAPTER III "Minimum requirements for the monitoring of data in the Eudravigilance database", Commission Implementing Regulation (EU) 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.
[32] Guideline on good pharmacovigilance practices (GVP) Module IX – Signal management (Rev 1).

If a Party authorises a user to access the secure, access-controlled domain of EV from outside the EU/EEA, that Party shall ensure that an appropriate data transfer mechanism is established prior to any access by that user, and that such international data transfers comply with the rules of Chapter V of Regulation (EU) 2018/1725 or Regulation (EU) 2016/679, respectively.

3. How long do we keep your data?

Pseudonymised reports of suspected adverse reactions are maintained for as long as EV is in operation in accordance with Article 24(1) of Regulation No 726/2004. This is to provide for a large and coherent data pool covering a wide range of medicinal products and ICSRs, which is necessary to ensure that statistical methods and algorithms for signal detection and data analysis operate consistently and a full and complete scientific evaluation across different medicinal products and therapeutic areas is provided for over time.

4. Who has access to your information and to whom is it disclosed?

The provisions of access to EV data and the actors, to whom access should be granted, are set out in the pharmaceutical legislation[33]. The EV Access Policy[34] further details the different levels of access provided to these actors taking into account the need to protect personal data as well as their pharmacovigilance obligations or interests. These actors refer to NCAs in Union Member States, the European Commission, the Agency, healthcare professionals, the public, MAHs, academia, the WHO and medicines and regulatory authorities in third countries.

Information on spontaneous reports from patients and healthcare professionals held in EV can be accessed publicly as follows: adrreports.eu.

In accordance with Regulation (EU) No 536/2014, access to SUSARs reported to EVCTM is provided to NCAs in Member States of the EU/EEA, the Agency and the Commission.

5. What are your rights under personal data protection?

Data subjects (i.e., the individual whose personal data is processed) have a number of rights:

- **Right to be informed** – This data protection notice provides information on how the joint controllers, via EV, collect and use personal data. Requests for other information regarding the processing may also be directed to datacontroller.analytics @ema.europa.eu
- **Right to access** – Data subjects have the right to access their personal data. Data subjects have the right to request and obtain a copy of the personal data processed regarding them.
- **Right to rectification** – Data subjects have the right to obtain - without undue delay - the rectification or completion of their personal data if it is incorrect or incomplete.
- **Right to erasure** – Data subjects have the right to require the Agency to delete or stop processing their personal data, for example where the data is no longer necessary for the purposes of processing. In certain cases, the data may be kept to the extent it is necessary, for example, to comply with a legal obligation or if it is necessary for reasons of public interest in the area of public health.

[33] Article 24(2) of Regulation (EC) No 726/2004
[34] European Medicines Agency policy on access to EudraVigilance data for medicinal products for human use (EudraVigilance Access Policy) (EMA/759287/2009 Revision 3*)

In cases where the right to erasure is requested and granted to a data subject, data may be kept if it has undergone an appropriate process of anonymisation.

- **Right to restrict processing** – In a few, codified cases, Data subjects have the right to obtain the restriction of the processing, meaning that their data will only be stored, but not actively processed for a limited period of time. For more information about this right and its limitations, see the EMA General Data protection notice, hosted at www.ema.europa.eu/en/about-us/legal/privacy-statement

In the context of the right to access and the right to rectification, you should note that there may be instances where a requestor contacts the Agency as regards their personal data being processed in EV, but it may not be possible for the Agency to confirm whether personal data concerning the requestor are being processed. This is based on the principle that generally personal data in ICSRs are pseudonymised before being submitted by an NCA, a MAH or a sponsor to EV (as outlined in section 3.1). In such instances, the Agency will refer the requestor to the NCA, MAH or sponsor that submitted the ICSR to EV, who may in turn refer them to their healthcare professional/investigator, who submitted the report.

The rights of the data subject can be exercised in accordance with the provisions of Regulation (EU) 2018/1725[35].

6. Recourse

In case data subjects have any questions regarding the processing of their personal data, or they think that the processing is unlawful, or it is not in compliance with this Data Protection Notice or the general EMA Data Protection Notice, the joint controllers can be contacted via the contact points listed in Section 1.1.

Data subjects also have the right to lodge a complaint with the European Data Protection Supervisor (EDPS) at any time at the following address: edps@edps.europa.eu
or with a competent Data Protection Authority whose contact details you may find here:
https://edpb.europa.eu/about-edpb/board/members_en

[35] 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)