EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Considerations on the international transfer of personal (health) data in ICSRs/SUSARs originating in the EU

Training Module EV-M8

EMA/10819/2025

30 January 2026

Content summary

- EudraVigilance
  - The different stakeholders, their applicable data protection frameworks and guidance and accountability
  - Core principles of the EU General Data Protection Regulation (GDPR) and the importance of data pseudonymisation
  - GVP Module VI Addendum II – Masking of personal data in individual case safety reports submitted to EudraVigilance
- Reporting of adverse drug reactions: interplay between pharmacovigilance legislation, GVP VI Addendum II and the EU GDPR
- International transfer of personal (health) data originating in the EU
  - Transfers on the basis of an adequacy decision
  - Transfers subject to appropriate safeguards
- Where to seek data protection advice?
- Sources of information

1. EudraVigilance

- The different stakeholders, their applicable data protection frameworks and guidance, accountability
- Core principles of the EU General Data Protection Regulation (GDPR) and the importance of data pseudonymisation
- GVP Module VI Addendum II – Masking of personal data in individual case safety reports submitted to EudraVigilance

EudraVigilance (EV)

Different stakeholders involved in the processing of health-related information in EV:

- National Competent Authorities (NCAs) in the EEA, European Commission (EC), EMA;
- Marketing authorisation holders (MAHs);
- Sponsors of Clinical Trials;
- Patients, healthcare professionals, academia, public.

Applicable data protection framework and guidance:

- Regulation (EU) 2018/1725 – EU Data Protection Regulation (EU DPR): applicable to EU Institutions.
- Regulation (EU) 2016/679 – EU General Data Protection Regulation (GDPR): applicable to MAHs & Sponsors;
- GVP Module VI Addendum II – Masking of personal data in individual case safety reports submitted to EudraVigilance: applicable to all senders of cases (ICSRs and SUSARs) to EV

Accountability:

- Joint controllers of EudraVigilance system: EC, EMA, NCAs;
- Controllers in their own rights: MAHs & Sponsors.

Regulation (EU) 2016/679 – the GDPR

The General Data Protection Regulation (GDPR) applies since 25 May 2018. It sets out detailed requirements for organisations collecting, storing and managing personal data.

When does the GDPR apply?

The GDPR applies if a company:

- processes **personal data** and **is based in the EU**, regardless of where the actual data processing takes place;
- is **established outside the EU but** offers goods or services to individuals in the EU, or monitors the behaviour of individuals within the EU, thereby **processing their personal data**.

Non-EU based businesses processing EU citizen's data have to appoint a **representative in the EU**.

When does the GDPR not apply?

The GDPR does **not** apply if:

- the data subject is a legal person (i.e., an organisation);
- the processing is done by a person acting for purposes which are outside his trade, business, or profession;
- the data subject is deceased; however national laws may apply.

Regulation (EU) 2016/679 – the GDPR

Article 4(1) of the GDPR defines **Personal data** as:

- 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 reference to an identifier such as a name, an identification number, location data, an online identifier or (…) factors specific to the physical, physiological, genetic (…) identity of that person;

Article 4(5) of the GDPR defines **Pseudonymisation** as:

- 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;

Regulation (EU) 2016/679 – the GDPR

Article 4(15) of the GDPR defines **Data concerning health** as:

- personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Article 4(15) of the GDPR states that **Personal Data concerning health**:

- should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services (…); a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Why is pseudonymisation important?

Fully identifiable personal data
Maximum utility
Maximum risk

Pseudonymised data

Reduced utility
Reduced risk

Anonymised data

Minimum utility
Minimum risk

Significant **risks** to the protection of data subjects.

- Potential risks may impact the **interests** and **rights of the data subject.**
- They could lead, inter alia, to **discriminatory effects on natural persons** on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, etc.

The application of **pseudonymisation** to personal data can **reduce the risks to data subjects**.

- It also helps controllers and processors to meet their data protection obligations;
- As the data utilisation is greater than the one obtained via an anonymisation technique, better decisions can be taken.

For data to be rendered truly anonymous, an anonymisation technique must be **irreversible**.

- However, as a result, **the utility of the data may be impaired, depending on the purpose for which it is used**.

Pseudonymisation through masking of personal data in ICSRs/SUSARs submitted to EudraVigilance: GVP Module VI Addendum II

The Agency adopted, together with the joint controllers (European Commission and competent authorities in Member States), a common masking policy that should be complied with by all entities (i.e., MAHs, Sponsors, NCAs and EMA) when reporting to EudraVigilance.

This guideline was developed by EMA together with NCAs and in consultation with the MAHs and was published in July 2025 as GVP Module VI - Addendum II: Masking of personal data in individual case safety reports submitted to EudraVigilance.

It provides instructions that complement Section ***VI.C.6.2.2.10. Data protection laws***, forming an integral part of the guidance in GVP Module VI and is **to be implemented by all senders** of individual case safety report (**ICSRs**) and suspected unexpected serious adverse reactions (**SUSARs**) to EV.

GVP Module VI – Addendum II

All ICH-E2B(R3) data elements were assessed to determine if their data was required in support of the pharmacovigilance (PV) and safety monitoring obligations set out in the EU pharmaceutical legislation.

The relevant obligations placed on the Agency, NCAs and the Pharmacovigilance Risk Assessment Committee (PRAC) were also taken into consideration.

The GVP VI Add. II instructions do **not** change the current EV Business Rules (there is no impact to the electronic submission process of ICSRs and safety messages).

The EU Individual Case Safety Report Implementation Guide does not require any changes and remains fully applicable.

Note # 1:
The instructions should be implemented as soon as possible and within a reasonable timeframe

Note # 2:
The timeframe should be documented to demonstrate when and how this will be achieved.

Note # 3:
The guidance applies to all cases: ICSRs (including Literature & non-EEA cases) and SUSARs.

GVP Module VI – Addendum II

Table of contents

VI.Add.II.4 Data elements to be left blank

The 11 data elements provided in **Table VI.Add.II.2.** are **not** necessary for signal management, duplicate detection or ICSR processing.

Since the use of nullFlavors is not supported by the ICH E2B(R3) guideline (see Annex IV ICH-E2B(R3)), the sender of the ICSRs should leave these 11 data elements **blank** when submitting ICSRs or SUSARs to EudraVigilance.

Table VI.Add.II.2.: 11 ICSR data elements to ALWAYS be left blank by the sender of ICSRs to EudraVigilance (provided that the data are available to the sender)

Field Identification ICH or EU E2B(R3) Data Elements in line with EU ICSR Implementation Guide		
Field ICH or EU	**ICH E2B(R3) data element reference**	**Data field name**
ICH	C.3.3.2	Sender's Title
ICH	C.3.3.3	Sender's Given Name
ICH	C.3.3.4	Sender's Middle Name
ICH	C.3.3.5	Sender's Family Name
ICH	C.3.4.1	Sender's Street Address
ICH	C.3.4.2	Sender's City
ICH	C.3.4.3	Sender's State or Province
ICH	C.3.4.4	Sender's Postcode
ICH	C.3.4.5	Sender's Country Code
ICH	C.3.4.6	Sender's Telephone
ICH	C.3.4.7	Sender's Fax

VI.Add.II.3 Data elements to be masked

The 13 data elements provided in **Table VI.Add.II.1.** are **not** required for signal management, duplicate detection or ICSR processing.

These data elements should therefore be set with the nullFlavour ***MSK***, provided that data are available to the sender of the ICSR to EudraVigilance.

Table VI.Add.II.1.: 13 ICSR data elements to ALWAYS be masked by the sender of ICSRs to EudraVigilance (provided that the data are available to the sender)

Field Identification ICH or EU E2B(R3) Data Elements in line with EU ICSR Implementation Guide		
Field ICH or EU	**ICH E2B(R3) data element reference**	**Data field name**
ICH	C.2.r.1.1	Reporter's Title
ICH	C.2.r.1.2	Reporter's Given Name
ICH	C.2.r.1.3	Reporter's Middle Name
ICH	C.2.r.1.4	Reporter's Family Name
ICH	C.2.r.2.1	Reporter's Organisation
ICH	C.2.r.2.2	Reporter's Department
ICH	C.2.r.2.3	Reporter's Street
ICH	C.2.r.2.6	Reporter's Postcode
ICH	C.2.r.2.7	Reporter's Telephone
ICH	D.1.1.1	Patient Medical Record Number(s) and Source(s) of the Record Number (GP Medical Record Number)
ICH	D.1.1.2	Patient Medical Record Number(s) and Source(s) of the Record Number (Specialist Record Number)
ICH	D.1.1.3	Patient Medical Record Number(s) and Source(s) of the Record Number (Hospital Record Number)
ICH	D.10.1	Parent Identification

VI.Add.II.5 and VI.Add.II.6

The data elements provided in **Table VI.Add.II.3.** and **Table VI.Add.II.4.** may contain or not personal identifiers or quasi-identifiers. In any case, they are **required for signal management, duplicate detection and ICSR processing**.

When available, these elements should **not be masked nor left blank** by the sender of the ICSR/SUSAR to EudraVigilance.

Some notable examples of the fields listed in those tables are shown below:

ICH	C.2.r.2.4	Reporter's City
ICH	C.2.r.2.5	Reporter's State or Province
ICH	C.2.r.3	Reporter's Country Code
ICH	C.3.2	Sender's Organisation
ICH	C.3.3.1	Sender's Department
ICH	C.3.4.8	Sender's E-mail Address
ICH	C.4.r.1	Literature Reference(s)
ICH	D.1	Patient (name or initials)
ICH	D.1.1.4	Patient Medical Record Number(s) and Source(s) of the Record Number (Investigation Number)
ICH	D.2.1	Date of Birth
ICH	D.2.2a	Age at Time of Onset of Reaction / Event (number)
ICH	D.2.2b	Age at Time of Onset of Reaction / Event (unit)
ICH	D.2.2.1a	Gestation Period When Reaction / Event Was Observed in the Foetus (number)
ICH	D.2.2.1b	Gestation Period When Reaction/Event Was Observed in the Foetus (unit)
ICH	D.2.3	Patient Age Group (as per reporter)
ICH	D.3	Body Weight (kg)
ICH	D.4	Height (cm)
ICH	D.5	Sex
ICH	D.6	Last Menstrual Period Date
ICH	D.7.1.r.1b	Medical History (disease / surgical procedure / etc.) (MedDRA code)
ICH	D.10.2.1	Date of Birth of Parent
ICH	D.10.2.2a	Age of Parent (number)
ICH	D.10.2.2b	Age of Parent (unit)
ICH	D.10.3	Last Menstrual Period Date of Parent
ICH	D.10.4	Body Weight (kg) of Parent
ICH	D.10.5	Height (cm) of Parent
ICH	D.10.6	Sex of Parent

Clarification

Does the EV data masking guideline (GVP Module VI Add. II) contradict the current GVP VI and EU ICSR Imp. Guide?

The ICSR implementation guide acknowledges that for certain data elements that can identify an individual (such as the *D.1 Patient (name or initials)* or the *D.2.1 Date of Birth)*, the use of the ***MSK*** flag *can* be appropriate.

In any case, the EMA would like to highlight that GVP Module VI was last revised in 2017 and the latest version of the EU ICSRs implementation guide dates to March 2021.

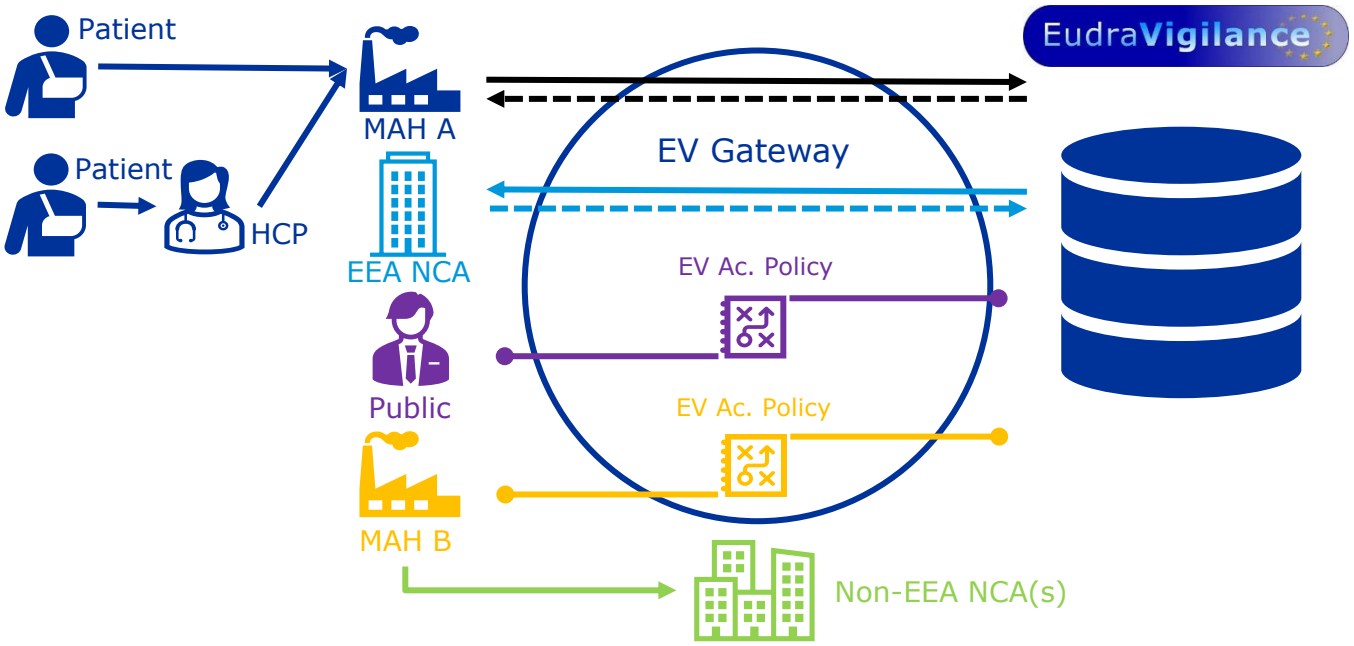
Despite the GDPR being published in 2016 and becoming effective in May 2018, there was no agreed common masking policy among EU Member States.

The EV data masking guideline published in 2025 supersedes the older guidance (provided in GVP Module VI and the EU ICSRs implementation guide).

2. Reporting of adverse drug reactions

- Interplay between pharmacovigilance legislation, GVP VI Addendum II and the EU GDPR

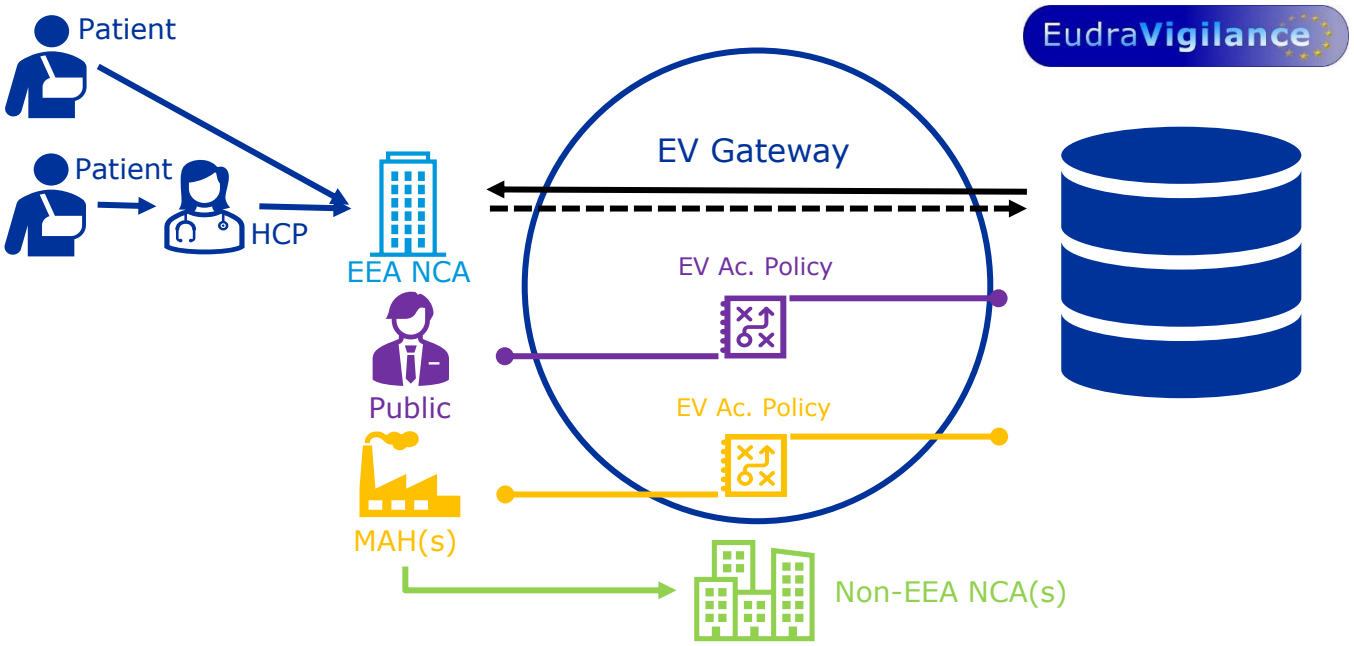
Most common ways for information exchange amongst multiple stakeholders in the EU/EEA – **MAHs (1/2)**



Key

- Exchange of information
- ICSR Submission
- ACK message
- Rerouted ICSR, if requested by NCA(s)
- ACK message
- Public access to EV database via the ADRReports.eu portal - **for Spontaneous PM reports only** (access in accordance with the EMA's EV Access Policy)
- ICSR Download by MAH (access in accordance with the EMA's EV Access Policy)
- ICSR Submission by EEA MAH B to Non-EEA NCA(s), if applicable

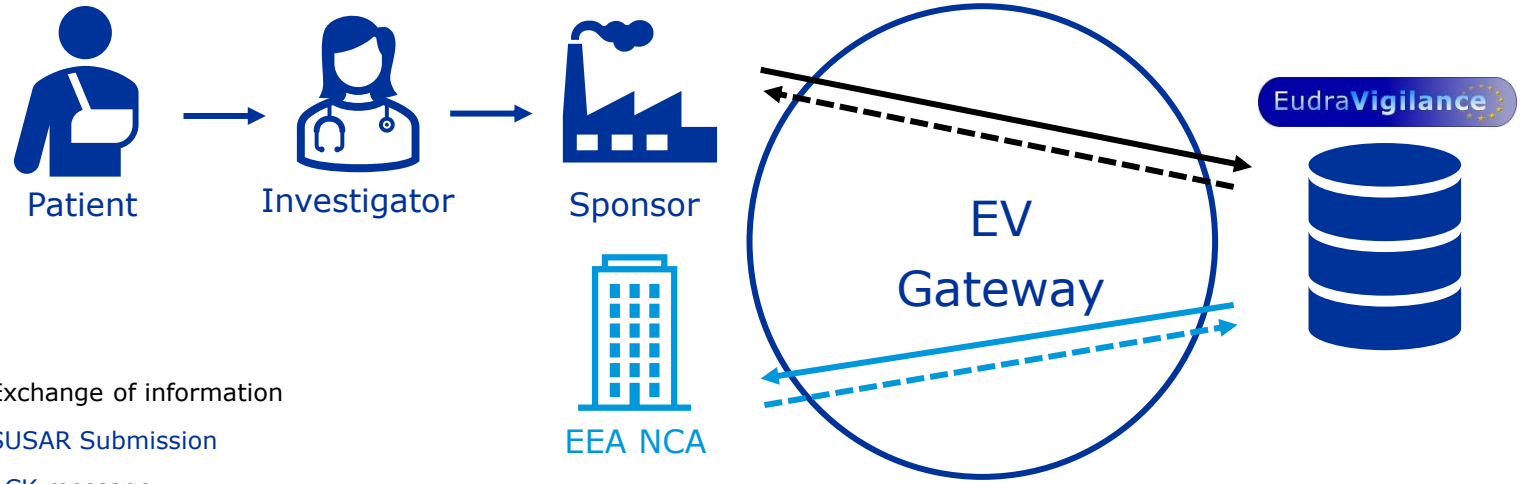
Most common ways for information exchange amongst multiple stakeholders in the EU/EEA – **MAHs (2/2)**



Key

- Exchange of information
- ICSR Submission
- ACK message
- Public access to EV database via the ADRReports.eu portal - **for Spontaneous PM reports only** (access in accordance with the EMA's EV Access Policy)
- ICSR Download by MAH(s) (access in accordance with the EMA's EV Access Policy)
- ICSR Submission by EEA MAH(s) to Non-EEA NCA(s), if applicable

Most common way for information exchange amongst multiple stakeholders - **Sponsors**



Reporting of adverse drug reactions: Legal Requirements/PV legislation and additional guidance

When an organisation receives a report directly from a Reporter (for MAHs and NCAs) or from the Investigator (for Sponsors), it has to process the data to meet the reporting requirements in line with local and, if applicable, international requirements.

In the EU, the requirements for the reporting of suspected adverse reactions (ICSRs and SUSARs) to EudraVigilance are set out in:

- **Sponsors:** Regulation (EU) No 536/2014; the format and content of ICSRs is further defined by the Commission Implementing Regulation (EU) No 520/2012; and GVP VI Addendum II.
- **MAHs:** Regulation (EC) No 726/2004 and Directive 2001/83/EC; the format and content of ICSRs is further defined by the Commission Implementing Regulation (EU) No 520/2012 and the applicable Good Pharmacovigilance Practices (GVPs), namely GVP Module VI and GVP VI Addendum II.

The guidance of GVP Module VI addendum II applies to **all senders** (i.e., MAHs, Sponsors, NCAs and EMA) of cases (**ICSRs** and **SUSARs**) to EV.

Reporting of adverse drug reactions

Application of the GDPR

In line with the provisions of the GDPR, **MAHs** and **Sponsors are data controllers** for the personal data processing activities carried out pursuant to the **clinical trials and pharmacovigilance (PhV) legislation**, including the access and **further processing** of ICSR data originating in from EudraVigilance.

- **A data controller** is a legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- "**Further processing**" **includes** access and **onward transfers** of ICSRs originating in the EU, independently of the origin (for example, a report from a Consumer/Investigator or case received from another sender), mode of access granted (for MAHs: EV, EVDAS) and level of access granted (e.g. granularity of the fields).

Reporting of adverse drug reactions

Application of the GDPR

PhV/Safety systems need to ensure compliance with the provisions set out in the GDPR.

- Those adaptations are subject to the **MAH's** and **Sponsor's own data protection assessment** regarding the risks to the rights and freedoms of natural persons;
- This includes the implementation of the **necessary technical and organisational measures,** for example:
  - protecting access to the systems with passwords
  - granting access rights to the PhV database only to certain authorized users and reviewing access rights at regular intervals
  - ensuring that, by default, only personal data which are necessary for fulfilling each specific legal requirement are processed

3. International transfer of personal (health) data originating in the EU

- Transfer tools for the international transfer of personal (health) data originating in the EU
  - Transfers on the basis of an adequacy decision
  - Transfers subject to appropriate safeguards

Access to data in EudraVigilance - **MAHs**

Article 24(2) of Regulation (EC) 726/2004 defines several level of access to EV:

- EV is fully accessible to the NCAs of the Member States and to EMA and the EC;
- EV is accessible to MAHs to the extent necessary for them to comply with their **PhV obligations**.

The EV Access Policy implements the varying access levels by determining which stakeholder groups have access to each data field.

As already explained in S11 of this training course, MAHs (Stakeholder group III) have access to:

- L1 ICSRs (Public subset of ICSR data elements)
- **L2A ICSRs (to fulfil their PhV obligations)**
- **L2B ICSRs (for signal evaluation and other PV activities – see slide 20)**
- L3 ICSRs (MAH's own cases and MLM cases)

International transfer of personal (health) data originating in the EU – **MAHs (1/2)**

Considering that EEA-based MAHs may have:

1) Affiliates/subsidiaries in third countries who are required to comply with local PhV legislation; and/or
2) Licensing partners in third countries with whom ICSR data may be required to be exchanged (if there is a Safety Data Exchange Agreement (SDEA) in place between the parties)

This may require MAHs to report personal data originating from the EEA (**including in reports obtained from EV** – see next slide) to third countries.

This transfer of data may qualify as an **international transfer of personal (health) data**.

The GDPR provides for mechanisms to do so which are further explained by the EDPB: International data transfers | European Data Protection Board.

International transfer of personal (health) data originating in the EU – **MAHs (2/2)**

L2A ICSR download: MAHs should note that if they are required to share ICSR data originating from EV, they are requested to **only** use the reports obtained via **L2A download**.

L2B ICSR download: Considering the provisions of Annex C of the EV Access Policy, L2B ICSR Downloads requests by MAHs are **only** applicable:

- Following the initial signal management steps as outlined in the GVP Module IX have been performed, including a reference to the corresponding e-RMR if applicable;
- Given a review of ICSR data in the context of a pharmacovigilance assessment procedure such as the PSUR as outlined in GVP Module VII or when required by the PRAC in a referral or signal assessment procedure.

International transfer of personal (health) data originating in the EU - **Sponsors**

Considering that Sponsors often run clinical trials in multiple countries, including in non-EEA countries, health data originating in the EEA may have to be sent to outside the EEA.

This transfer of data may qualify as an **international transfer of personal (health) data**.

The GDPR provides for mechanisms to do so which are further explained by the EDPB: International data transfers | European Data Protection Board.

International transfer of personal (health) data originating in the EU

Despite of these transfer requirements that EEA-based organisations may have, the GDPR imposes **limitations** on transfer of personal data outside the EEA:

- **The level of protection of individuals granted by the GDPR should remain essentially equivalent**, despite the transfer of health-information to third countries;
- Personal data may only be transferred outside of the EEA in compliance with the conditions laid down in **Chapter V of the GDPR**, for example, the organization shall:
  - Have an appropriate **legal basis** for transferring personal data to a third country;
  - Rely an appropriate **transfer tool** (as provided by articles 45 and 46 of the GDPR) - see EDPB guidance International data transfers | European Data Protection Board; and
  - Only transfer the personal data that are necessary to achieve the purpose of the transfer (**data minimization principle**).

International transfer of personal (health) data originating in the EU

MAHs and **Sponsors** are **accountable** for complying with the rules set out in Union data protection legislation when transfer personal data i.e., the GDPR and national data protection laws where applicable.

MAHs and Sponsors shall adhere to the rules applicable to the transfer of personal data to third countries as set out in Chapter V of the GDPR and the confidentiality undertaking of the EudraVigilance Access Policy (the last one is only applicable for MAHs).

International transfer of personal (health) data originating in the EU

Transfer tools

Article 45 of the GDPR – Transfers on the basis of an adequacy decision

The European Commission has the power to determine (Article 45 of the GDPR) whether a country outside the EU (i.e. third country) offers an adequate level of data protection by adopting an adequacy decision.

The effect of such an adequacy further safeguard being necessary. The list of countries which are currently recognized by the EC as providing an adequate level of data protection is available at:

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

International transfer of personal (health) data originating in the EU

Transfer tools

Article 46 of the GDPR – Transfers subject to appropriate safeguards

In the absence of a decision pursuant to Article 45 of the GDPR, an organization may transfer personal data to a third country or an international organisation only if it has provided **appropriate safeguards**, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Article 46 lists the transfer tools which may provide appropriate safeguards.

In the absence of adequacy decision and before transferring ICSRs containing personal data to third countries, MAHs and Sponsors rely on an **appropriate transfer tool**.

4. Where to seek data protection advice?

Where to seek data protection advice?

In case of question relation to personal data protection, **MAHs/Sponsors should first seek advice from their organisation's Data Protection Officer** and then, if still needed, **from their national data protection authority (DPA)**.

The competent data protection authority is the authority in the EU Member State where the company is based. The list of DPAs is available at:

https://edpb.europa.eu/about-edpb/about-edpb/members_en

If the MAH/Sponsor processes personal data in or across several EU member states or is part of a group of companies established in several EU member states, the competent DPA may be located in another EU Member State than the one in which the MAH/Sponsor is established.

5. Sources of Information

Sources of information

Regulation (EU) 2016/679 (EU GDPR): https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2018/1725 (EU DPR): https://eur-lex.europa.eu/eli/reg/2018/1725/oj

Regulation (EU) No 536/2014: https://eur-lex.europa.eu/eli/reg/2014/536/oj

Commission Implementing Regulation (EU) No 520/2012: https://eur-lex.europa.eu/eli/reg_impl/2012/520/oj

Regulation (EC) No 726/2004: https://eur-lex.europa.eu/eli/reg/2004/726/oj

Directive 2001/83/EC: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32001L0083

Commission Implementing Regulation (EU) No 520/2012: https://eur-lex.europa.eu/eli/reg_impl/2012/520/oj

GVPs: https://www.ema.europa.eu/en/human-regulatory-overview/post-authorisation/pharmacovigilance-post-authorisation/good-pharmacovigilance-practices-gvp

GVP VI (EMA/873138/2011): https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-good-pharmacovigilance-practices-gvp-module-vi-collection-management-and-submission-reports-suspected-adverse-reactions-medicinal-products-rev-2_en.pdf

Sources of information

GVP Module VI – Addendum II (EMA/178902/2025): https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-good-pharmacovigilance-practices-gvp-module-vi-addendum-ii-masking-personal-data-individual-case-safety-reports-submitted-eudravigilance_en.pdf

EMA EV Access Policy (EMA/759287/2009): https://www.ema.europa.eu/en/documents/other/european-medicines-agency-policy-access-eudravigilance-data-medicinal-products-human-use-revision-4_en.pdf

EMA EV Access Policy - Confidentiality undertaking for MAHs (EMA/337295/2016): https://www.ema.europa.eu/system/files/documents/other/wc500206426_en.pdf

International data transfers (European Data Protection Board): https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en

Adequacy decisions (European Commission): https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Data Protection Authorities in the EU: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

Sources of information

EU Individual Case Safety Report (ICSR) Implementation Guide (EMA/51938/2013): https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/european-union-individual-case-safety-report-icsr-implementation-guide_en.pdf

EV Business rules: https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/eu-individual-case-safety-report-icsr-implementation-guide-business-rules-spreadsheets_en.zip

Summary of EV-M8

We are now at the end of the training Module EV-M8, which provided you the basis for understanding:

- EudraVigilance
  - The different stakeholders, their applicable data protection frameworks and guidance and accountability
  - Core principles of the EU General Data Protection Regulation (GDPR) and the importance of data pseudonymisation
  - GVP Module VI Addendum II – Masking of personal data in individual case safety reports submitted to EudraVigilance
- Reporting of adverse drug reactions: interplay between pharmacovigilance legislation, GVP VI Addendum II and the EU GDPR
- International transfer of personal (health) data originating in the EU
  - Transfers on the basis of an adequacy decision
  - Transfers subject to appropriate safeguards
- Where to seek data protection advice?
- Sources of information