28 January 2022
EMA/366104/2021

Joint Controllership Arrangement

With regard to the Union product database (UPD)

Amongst

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

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

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 the Union product database administered by EMA ("UPD");

Having regard to Regulation (EU) 2019/6 of the European Parliament and of the Council of 11 December 2018 on veterinary medicinal products and repealing Directive 2001/82/EC;

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 Commission Implementing Regulation (EU) 2021/16 of 8 January 2021 laying down the necessary measures and practical arrangements for the Union database on veterinary medicinal products (Union product database) (hereinafter 'UPD Regulation');

Whereas:

(1) 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

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

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, by means of an arrangement between them;

(2) 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, 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, by means of an arrangement between them;

(3) Article 55(1) of Regulation (EU) 2019/6 stipulates that the Agency shall establish and, in collaboration with the Member States, maintain, a Union database on veterinary medicinal products;

(4) In accordance with Article 55(3) of Regulation (EU) 2019/6, the European Commission has adopted the UPD Regulation;

(5) This Arrangement has been drawn up by the Agency (in cooperation with the European Commission) and Member States (involved through their appointed NCA 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 Agency and the Member States 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 UPD. Each Party may appoint authorised users (including assigning their roles and permissions) affiliated to that Party to access and use the UPD on its behalf, each of them a 'user' for the purpose of this Arrangement[1].

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 the UPD as necessary for the activities carried out in accordance with the principles set out in Regulation (EU) 2019/6 and in the UPD Regulation. A description of categories of personal data processed in UPD and categories of Data Subjects concerned is included in the Data Protection Notice enclosed as Annex II.

1.4 A data processing operation consists of the processing activities[2], performed by the Party responsible for that task:

a) Processing activity performed by the **Member States** users, in the user secure domain (via NCA user interface or Application programming interface), include uploading on the UPD data and documents that may contain personal data, as needed, during the product life cycle.

This processing operation includes activities to populate structured data, upload documents and submit and update these, as applicable, in the context of:

- Creation of new product or update of dataset for an existing product following a positive outcome;

[1] Upon their first access to UPD, authorised users will be deemed to have accepted the JCA.
[2] This is not an exhaustive list of processing activities but indicative of the main processing operations under consideration

- User access management for users within their organisation (after initial registration of organisation super user, the registration of subsequent users is performed by said super user for the organisation)[3];
- Operation of searches and generation of reports based on data or documents in the system;
- Ensure data quality of submission in accordance with the UPD Access Policy.[4]

b) Processing activity performed by the **European Medicines Agency** users, in the user domain, include:

- Creation of a new product or update of a dataset for an existing product following a positive outcome;
- Super-users access management within UPD in accordance with Articles 7(a) and 13 of the UPD Regulation, via the EMA Account Management (EAM) system used to generate users' credentials to access UPD secure domain;
- User access management for users within EMA, (after initial registration of an organisation super user, the registration of subsequent users is performed by said super user for the organisation)[3];
- Maintenance of the UPD database including responsibility for data storage and security in accordance with Article 12 of the UPD Regulation;
- Operation of searches and generation of reports based on data or documents in the system, including extraction and analysis of this data outside of the system;
- Ensure data quality of submission in accordance with UPD Access Policy[4].

c) Processing activities for the **users of all the above joint controllers** and the marketing authorisation holders of all products included in the UPD (the latter acting as 'data processors', as this term is defined in Regulation (EU) 2016/679 and Regulation (EU) 2018/1725) include, in addition to submission of data and documents (where applicable), also the possibility to view and download data and documents that might contain personal data.

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 UPD, and therefore out of scope of this arrangement, that 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 Agency and the Member States, 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 Agency and the Member States 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.

[3] Registration details processed via EMA Account Management (EAM) are subject to 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
[4] https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/union-product-database-upd-access-policy-veterinary-medicinal-products-policy-no-0082_en.pdf

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 fall outside the scope of this Arrangement.

2a.2. 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 UPD. They also act as individual controllers when they extract from, and analyse outside of, the system any data uploaded on the UPD. It is the sole responsibility of the Member States, represented by National Competent Authorities, to ensure compliance with all obligations and conditions of Regulation (EU) 2016/679 regarding the activities performed as individual controllers.

2a.3. The **European Medicines Agency** acts as individual controller in relation to the processing activities carried out within their organisation, performed outside of UPD, for example:

- Initial user registration in the EMA Account Management (EAM) system[5]

The European Medicines Agency also acts as individual controller when they extract from, and analyse outside of, the system any data uploaded on the UPD. 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.

2a.4. For the sake of clarity, the parties also confirm that processing activities performed by **marketing authorisation holder** users outside of UPD are out of scope of this joint controllership arrangement, as these actors are not joint controllers and act as data processors within UPD. Marketing authorisation holders act as individual and independent controllers for data processing operations at their end and it is their sole responsibility to ensure compliance with all obligations and conditions of Regulation (EU) 2016/679 regarding their activities performed in relation to UPD, for example, the following:

a) uploading into the UPD data and documents that may contain personal data, as needed, during the product life cycle;

b) operation of searches and generation of reports based on data or documents in the system;

c) extracting from, and analysing outside of, the system any data uploaded on the UPD.

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 the UPD to ensure that Data Subjects are informed of the details of the processing activity carried out in the UPD.

[5] 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

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 UPD, 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 has the request 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 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 UPD, while where the handling of the request requires removal of data stored within UPD, EMA will be responsible for such removal and will liaise to that effect with the Party originally providing the data in UPD. 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.

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 the last two paragraphs of this Article 3.3.

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 measures to ensure the security of processing personal data in UPD pursuant to Article 33 of Regulation (EU) 2018/1725 and Article 12 of UPD Regulation.

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 secure user domain of the UPD undergoing joint processing shall only be allowed to authorised staff/personnel/authorised users of the Parties and to marketing authorisation holders 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. Marketing authorisation holders acting as data processors have to comply with the obligations set forth in Regulation (EU) 2016/679.

3.6 Localisation of personal data

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

Where personal data is made available to the public in the public domain of UPD 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 UPD 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:

- Recording of the processing operation;
- Ensuring that the personal data undergoing processing are adequate, accurate, relevant and limited to what is necessary for the purpose;
- Ensuring a transparent information and communication to Data Subjects of their rights;
- Facilitating the timely exercise of the rights of Data Subjects;
- Handling of Data Subjects' requests in accordance with the procedure adopted;
- 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;
- Ensuring privacy by design and privacy by default;
- Identifying and assessing the lawfulness, necessity and proportionality of transmissions and transfers of personal data;
- Carrying out a data protection impact assessment, where necessary;
- Carrying out a prior consultation with the European Data Protection Supervisor, or other competent national supervisory authority, where needed;
- Ensuring that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- 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 the UPD as outlined in Section 2.a above:

(i) the Agency 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. Acknowledgement of this Arrangement by the users

A hyperlink to this Arrangement will be displayed to UPD users at the time of their first log in in UPD. 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.

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 UPD.

6. Effective Date

This Arrangement has received the consent of the representatives of the Parties in November 2021 and has been submitted for endorsement to the EMA Management Board meeting on 27 January 2022, with the understanding that all users of the UPD secure domain undertake to comply with it prior to, and as a condition to, using the UPD from 28 January 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 5 of this Arrangement.

This Arrangement is effective as from the date above written and shall continue to be effective as long as the UPD 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.veterinary@ema.europa.eu

European Member States:

Member State	Contact Point
Austria	recht@basg.gv.at
Belgium	*To be confirmed*
Bulgaria	a_kolova78@itp.bg
Croatia	*To be confirmed*
Cyprus	mgenakritis@vs.moa.gov.cy
Czech Republic	*To be confirmed*
Denmark	ahol@dkma.dk
Estonia	*To be confirmed*
Finland	kirjaamo@fimea.fi
France	anmv-controllerUPD@anses.fr
Germany (BVL)	datenschutz@bvl.bund.de
Germany (PEI)	datenschutz@pei.de
Greece	dpo@eof.gr
Hungary	ati@nebih.gov.hu
Iceland	personuvernd@lyfjastofnun.is
Ireland	dataprotectionofficer@hpra.ie
Italy	*To be confirmed*
Latvia	ITsupport@pvd.gov.lv
Liechtenstein	recht@basg.gv.at
Lithuania	dap@vmvt.lt
Luxembourg	*To be confirmed*
Malta	*To be confirmed*
Netherlands	*To be confirmed*
Norway	personvern@legemiddelverket.no
Poland	iod@urpl.gov.pl
Portugal	epd@dgav.pt
Romania	*To be confirmed*
Slovakia	*To be confirmed*
Slovenia	info@jazmp.si
Spain	delegado_protecciondatos@aemps.es
Sweden	esubmission@mpa.se

Annex II:

Data Protection Notice regarding personal data processing in the Union product database (UPD)

Regulation (EU) 2019/6 mandates that the European Medicines Agency (the "Agency") establish and, in collaboration with the Member States and European Commission, maintain, a Union Product Database ("UPD"), containing information on authorised veterinary medicinal products, registered homeopathic veterinary medicinal products, veterinary medicinal products exempted from the marketing authorisation requirements, and approved parallel traded veterinary medicinal products, within the Union.

This Data Protection Notice explains the most essential details of the processing of personal data by the Agency. This specifically relates to the name and address of a qualified person for pharmacovigilance (QPPV), as well as the name and organisation of an authorised user whose actions and changes to the data sets in the restricted areas of the UPD database are recorded, to provide the audit trail and traceability of data changes.

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

1. Who is responsible for processing your data?

1.1 Who are the joint controllers?

The joint controllers under the Joint Controllership Arrangement ("JCA") for the UPD are:

European Medicines Agency and Member States.

The Parties to the JCA act as joint controllers for the purpose of processing operations of personal data provided, in structure data and documents, in UPD.

The contact points of joint controllers are the following:

European Medicines Agency: datacontroller.veterinary@ema.europa.eu

Member States: Annex I of the JCA

Marketing authorisation holders contact points are identified at the time of their registration in UPD.

The respective roles and relationship vis-à-vis Data Subjects are explained in the JCA. In accordance with the applicable rules of EUDPR and GDPR, Data Subjects may exercise their rights 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.

1.2 Who is the data processor?

Marketing authorisation holders act as data processors when they upload/download documents in/from UPD, containing personal data.

2. Purpose of this data processing

The purpose of this data processing activity is to collect and maintain information on veterinary medicinal products authorised in the Union as mandated by Regulation (EU) 2019/6. In this context, the QPPV personal data is processed while creating new veterinary medicinal product entries and maintaining the QQPV information via variations not requiring assessment, as well as providing audit trail and traceability of actions and changes to the datasets performed by registered users in the restricted areas of the UPD.

2.1 Personal data concerned

The QPPV personal data is processed when registered users in UPD create new veterinary medicinal products entries in the UPD or update existing data via variations not requiring assessment. Such data includes the following:

- First name and last name of qualified person for pharmacovigilance (QPPV)
- Location (address) where QPPV operates

In addition, the personal data of the UPD authorised and registered users is also processed when their actions in the restricted areas of the UPD are logged for the purpose of the audit trail and traceability of data changes. During the registration process to access the UPD, EMA collects personal data to open a user account and request a user role in the EMA Account Management system. The EMA Privacy Statement for the Account Management system outlines how EMA collects and uses personal data for the aforementioned purpose.

Such personal data includes the following:

- Name, surname and email address of a registered user

These details are visible in the UPD secure domain to the Administrator(s) within the user's organisation for the purpose of administering users' profiles.

Name, surname and role of the users in UPD are visible to the other people within the organisation which originated the personal data at stake.

Users' names, surnames, roles and contact details will be visible only in the UPD secure domain, and not disclosed in the public domain.

2.2 Legal basis of the data processing

The processing of personal data in the context of the Union Product Database is necessary in view of Regulation (EU) 2019/6 implementation and for the performance of the related tasks carried out in the public interest, namely the processing of personal data in the Union Product Database necessary in accordance with Article 55 (3b) of Regulation (EU) 2019/6 as well as Commission Implementing Regulation (EU) 2021/16. Therefore, this data processing by the Agency is lawful under Article 5(1)(a) of the EUDPR and justified on the grounds of public interest.

The data processing by Member States also relies on the lawful ground of public interest under Article 6(1)(e) of the GDPR [and Article 5(1)(a) of the EUDPR, respectively].

Data processing by marketing authorisation holders in UPD is necessary for compliance with their legal obligations under Regulation (EU) 2019/6, in accordance with Article 6(1)(c) of the GDPR.

In this regard, please note that you have the **right to object** against the processing as explained in Section 5 below.

2.3 Transfer of personal data outside of EU/EEA

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

Where personal data is made available to the public in the public domain of UPD 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 UPD 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?

Information on veterinary medicinal products and, as such, personal data related to QPPV as well as data history which relates to the audit trail and traceability of data changes performed by registered users are kept for 30 years in the Union Product database, upon which the retention of the data will be subject to review and may be extended if justified based on the purposes of the processing.

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

The provisions on access to the UPD and the actors to whom access should be granted are set out in Article 56 of Regulation (EU) 2019/6. The Union Product Database Access Policy further details the different levels of access provided to these actors, taking into account the need to protect personal data as well as their obligations or interests. As far as the handling of the personal data concerns, these actors refer to [the Commission (as one of the users),] national competent authorities within the EU Member States and the Agency, including contractors and external service providers working for them on UPD-related matter.

History of actions and changes to the data sets performed by the registered users in the restricted areas of the UPD can only be accessed by the EMA administrators (technical staff).

Reports on the history of changes to the data sets already existing in the UPD can be obtained by competent authorities (i.e., NCAs, EC and EMA) and marketing authorisation holders only for their veterinary medicinal products.

5. Your data protection rights

As data subject (i.e. the individual whose personal data is processed), you have a number of rights:

- **Right to be informed** – This Data Protection Notice provides information on how EMA collects and uses your personal data. Requests for other information regarding the processing may also be directed to datacontroller.veterinary@ema.europa.eu.
- **Right to access** – You have the right to access your personal data. You have the right to request and obtain a copy of the personal data processed by EMA.

- **Right to rectification** – You have the right to obtain - without undue delay - the rectification or completion of your personal if it is incorrect or incomplete.
- **Right to erasure** – You have the right to require EMA to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing. In certain cases your data may be kept to the extent it is necessary, for example, to comply with a legal obligation of the Agency or if it is necessary for reasons of public interest in the area of public health.
- **Right to restrict processing** – In a few, codified cases, you have the right to obtain the restriction of the processing, meaning that your 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 Privacy Statement, hosted at www.ema.europa.eu/en/about-us/legal/privacy-statement.
- **Right to object** – You have the right to object at any time to this processing on grounds related to your particular situation. If you do so, EMA may only continue processing your personal data if it demonstrates overriding legitimate grounds to do so or if this is necessary for the establishment, exercise or defence of legal claims.

The rights of the data subject can be exercised in accordance with the provisions of Regulation (EU) 2018/1725. For anything that is not specifically provided for in this data protection notice, please refer to the contents of the general EMA Privacy Statement: www.ema.europa.eu/en/about-us/legal/privacy-statement

6. Recourse

In case you have any questions regarding the processing of your personal data, or you think that the processing is unlawful or it is not in compliance with this Data Protection Notice or the general EMA Privacy Statement, please contact our functional mailbox datacontroller.veterinary@ema.europa.eu or the **EMA Data Protection Officer** at dataprotection@ema.europa.eu.

You also have the right to lodge a complaint with the **European Data Protection Supervisor (EDPS)** at any time at the following address:

- Email: edps@edps.europa.eu
- Website: www.edps.europa.eu
- Further contact information: www.edps.europa.eu/about-edps/contact_en