07 December 2021
EMA/MB/422912/2020
Version 1.2

Joint Controllership Arrangement

With regard to the Clinical Trials Information System (CTIS)

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

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

the **Member States of the European Union** (hereinafter referred to as 'MS' or 'Member States'), and

commercial, non-commercial organisations and academia acting as **sponsors of clinical trials** (hereinafter referred to as 'sponsors') and **Marketing Authorisation Applicants/Holders** (hereafter referred to 'MAA/MAH' or 'marketing authorisation applicants/holders'),

Each of them a 'Party' and collectively referred to as 'Parties', to be considered as 'joint controllers' for the purpose of processing personal data captured in the Clinical Trial Information System administered by EMA (CTIS),

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 (hereinafter, CTR);

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 82, paragraph 1 of the CTR, consisting of:

i. Functional Specifications of the EU Portal and EU Database to be audited (EMA/42176/2014 Rev.1, Corr. *);

ii. Revision of section 6 of the 'Functional specifications for the EU Portal and EU Database to be audited – EMA/42176/2014' setting out features to support making information public;

iii. Appendix, on disclosure rules, to the 'Functional specifications for the EU Portal and EU Database to be audited - EMA/42176/2014' (EMA/228383/2015 Endorsed);

iv. Update of certain Functional Specifications/Non-Functional Requirements of the EU Portal and Database (EUPD) (EMA/MB/103780/2021) (endorsed by EMA Management Board on an ad-hoc meeting held on 23 February 2021).

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 rights of the Data Subjects 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) Whereas 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 Subjects 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) This Arrangement has been drawn up by the European Commission, the Agency, Member States in consultation with representatives of industry associations, academia and learned societies with the understanding that all commercial, non-commercial organisations and academia accessing CTIS in their capacity of sponsors and marketing authorisation applicants/holders, when accessing CTIS for the first time, will be reminded of the contents of this Arrangement and its Annexes before they can progress with the use of CTIS.

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 respective data protection obligations under Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, when carrying out processing operations of personal data of data subjects, collected as part of the use of CTIS.

Each Party may appoint authorised users (including assigning their roles and permissions) affiliated to that Party to access and use the CTIS on its behalf (including by way of example and without limitation: National Competent Authorities, Ethics Committees, Contract Research Organisation and other contractors), 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] Solely for the purposes of the implementation of this JCA, Member States may appoint relevant entities that would be representing them as joint controller(s) in accordance with their national rules. Upon their first access to CTIS such entities will be deemed to have accepted the JCA as a joint controller. A list identifying these entities will be made available, by the relevant Member State to the other Parties and the data subjects upon their request, via the e-mail address listed in Annex I.

1.3. This Arrangement governs the processing of personal data in the CTIS as necessary for the activities carried out in accordance with, amongst others, the principles set out in Article 81(2) of the CTR (hereafter, 'processing operation'). Description of categories of personal data processed in CTIS 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 **clinical trial sponsor** users, in the secure domain of CTIS, include uploading on the CTIS data and documents that may contain personal data, as needed, during the trial life cycle.

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

- clinical trials applications (CTAs) including initial and modifications[3];
- responses provided following request for information raised by the Member State Concerned[4];
- notifications for start of trial, start of recruitment, end of recruitment, temporary halt, restart of trial, end of trial (including early termination), third countries inspection reports, serious breaches, unexpected events, urgent safety measures and other tasks;
- information provided to the authorities following an inspection, an opinion requested as part of a corrective measures or an ad hoc request for information;
- summary of clinical trial results and lay person summary;
- annual safety reports (ASR);
- operation of searches and generation of reports based on data or documents in the CTIS.

b) Processing activity performed by the **marketing authorisation applicants/holders** users, in the secure domain of CTIS, includes uploading on the CTIS data and documents that may contain personal data, as needed, during the trial life cycle.

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

- submission of clinical study results provided as part of marketing authorisation applications in the EU, or variation or line extension to these, including all appendices except those listing individual patient data;
- operation of searches and generation of reports based on data or documents in the CTIS.

c) Processing activity performed by the Member States users, in the secure domain of CTIS, includes uploading on the CTIS data and documents that may contain personal data, as needed, during the trial life cycle.

[2] This is not an exhaustive list of processing activities but indicative of the main processing operation under consideration. Overall, data processing activities include the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.
[3] Modification of an initial application can be performed via the means of responses to RFI, Substantial and Non-Substantial modifications and addition of a new Member State Concerned
[4] Member State Concerned means the Member State where an application for authorisation of a clinical trial or of a substantial modification has been submitted under Chapters II or III of this Regulation respectively, Article 2(2)(12) of Regulation (EU) No 536/2014.

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

- preparation of considerations and request for information to be sent to the sponsors during the evaluation of a clinical trial application, initial and modifications;
- submission of the draft and final assessment reports for the assessment of part I and part II of the dossier;
- application of corrective measures, including requesting sponsor's opinion or consultation with other Member State/s Concerned[5];
- request additional information to the sponsors via the ad hoc assessment functionality;
- submission of inspection reports;
- submission of ASR evaluation reports and related requests for information;
- operation of searches and generation of reports based on data or documents in the CTIS.

d) Processing activity performed by the European Commission users, in the secure domain of CTIS, includes uploading on the CTIS data and documents that may contain personal data, as needed.

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

- submission of Union Controls plans/programmes;
- submission of Union Controls reports;
- operation of searches and generation of reports based on data or documents in the CTIS.

e) Processing activity performed by the European Medicines Agency users, in the secure domain of CTIS, includes:

- amending the uploaded data and documents on the CTIS, by means of removing from public website data and documents, or pushing publication forward in case of overriding public interest;
- user access management, via Identity Access Management (IAM) system used to generate users' credentials to access CTIS secure domain;
- maintenance of the CTIS database including responsibility for data storage;
- ensuring technical support to all users of CTIS in case of troubleshooting;
- 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 CTIS.

f) Processing activities for the users of all the above joint controllers 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 CTIS, and therefore out of scope of this Arrangement, and are carried

[5] The term 'Member State Concerned' means the Member State where an application for authorisation of a clinical trial or of a substantial modification has been submitted under Chapter II or III of Regulation (EU) No 536/2014.

out by the Parties separately in their role of 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, respectively, 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

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

Commercial, non-commercial organisation(s) and academia having roles in CTIS as **sponsors** or **marketing authorisation applicants/holders**, act separately as individual controllers in relation to the data processing activities carried out within their organisation, whether related to clinical trial or not, that are performed outside of CTIS, as applicable and based on their role.

This includes, by way of example and without limitation, activities carried out by the Parties, outside of CTIS for preparation of the content and maintenance of the following:

- clinical trial application dossier, responses to request for information (RFI) raised during the evaluation of an application, preparation of Annual Safety Reports, preparation of various types of notifications, compilation of trial summary of results and other documents for submission, including, when needed redaction or anonymisation of such document;
- Preparation of documents provided in reply to supervision activities carried out by the MS, such as: responses to inspection reports, opinion following consultation in the context of a corrective measure, responses to an ad hoc assessment, including, when needed redaction or anonymisation of such documents;
- Preparation of clinical study reports (CSR), including, when needed redaction or anonymisation of such documents;
- Preparation and maintenance of clinical trial master file, including, when needed redaction or anonymisation of such documents.

They also act as individual controllers when they extract from, and analyse outside of, the CTIS any data uploaded on the CTIS. It is the sole responsibility of the commercial, non-commercial organisation(s) and academia to ensure compliance with all obligations and conditions of Regulation (EU) 2016/679 regarding their activities performed as individual controllers.

2a.2. The **EU Member States, including where acting through authorised users such as National Competent Authorities and Ethics Committees**, act as individual controllers in relation to the data processing activities carried out within their organisation, whether related to clinical trial or not, that are performed outside of CTIS.

This includes, by way of example and without limitation, preparation of the content and maintenance of the following:

- considerations and requests for information to be sent to the sponsors during the evaluation of a clinical trial application, submission of the draft and final assessment reports for the assessment of part I and part II of the dossier, issuing conclusions and decisions on a clinical trial application;
- supervision of clinical trial to apply corrective measures, including the request for a sponsor opinion and the consultation with other Member State Concerned, the preparation of a request additional information to the sponsors via the ad hoc assessment functionality, preparation of inspection reports;
- evaluation of Annual Safety Reports;

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

2a.3. 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, or not, that are performed outside of CTIS, by way of example and without limitation related to the preparation of the content and maintenance of the following:

- Union controls plans, programmes and reports.

The European Commission also acts as individual controller when it extracts from, and analyses outside of, the CTIS any data uploaded on the CTIS. It is the sole responsibility of the European Commission to ensure compliance with all obligations and conditions of Regulation (EU) 2018/1725 regarding the activities performed as individual controller.

2a.4. The **European Medicines Agency** acts as individual controller in relation to the processing activities carried out within its organisation, related to clinical trial or not, that are performed outside of CTIS, by way of example and without limitation:

- User management via Identity Access Management (IAM)

The European Medicines Agency also acts as individual controller when it extracts from, and analyses outside of, the CTIS any data uploaded on the CTIS. It is the sole responsibility of the European Medicines Agency to ensure compliance with all obligations and conditions of Regulation (EU) 2018/1725 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 of CTIS, and within CTIS, to ensure that Data Subjects are informed of the details of the processing activity carried out in the CTIS.

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 CTIS, 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 a processing operation carried out by that Party in accordance with Section 1.4 above.**
a)	If the request falls under that Party's processing operation 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 a processing operation 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.)

I. **When a Party receives a Data Subject request, it must check whether the request concerns a processing operation carried out by that Party in accordance with Section 1.4 above.**

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

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 processing operations 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[6] 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

[6] Notification should include information about type of breach, possible consequences of the breach and measures already adopted to avoid possible damage.

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 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 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 CTIS 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 secure domain of the CTIS undergoing joint processing shall only be allowed to authorised staff/personnel/authorised users of the Parties, 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 appointing 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, as applicable.

3.6. Localisation of personal data

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

Where personal data is made available to the public in the public domain of CTIS 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 CTIS 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 under Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or national laws applicable to the Parties, 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 CTIS as outlined in Section 2.a above:

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

(ii) the Member States, the sponsors and marketing authorisation applicants/holders 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 CTIS users at the time of their first log in in CTIS. 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 CTIS.

7. Effective Date

This Arrangement has received the consent of the representatives of the Parties in September 2021 and has been endorsed by the EMA Management Board on the 7th October 2021, with the understanding that all users of the CTIS secure domain undertake to comply with it prior to, and as a condition to, using the CTIS from 31 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 3 of this Arrangement.

This Arrangement is effective as from the date above written and shall continue to be effective as long as the CTIS 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: datacontroller.clinicaltrials@ema.europa.eu

European Commission: SANTE-DATA-PROTECTION-COORDINATOR@ec.europa.eu

European Member States:

Member States	Contact Point
Austria	Datenschutz-BASG@basg.gv.at
Belgium	dpo@fagg.be
Bulgaria	*To be confirmed*
Croatia	*To be confirmed*
Cyprus	clinicaltrials@phs.moh.gov.cy
Czechia	ctis-dpo@sukl.cz
Denmark	dju@dkma.dk
Estonia	trials@ravimiamet.ee
Finland	clinicaltrials@fimea.fi
France	*To be confirmed*
Germany	ct@bfarm.de
Greece	trials@eof.gr
Hungary	ctrcontacthu@ogyei.gov.hu
Iceland	personuvernd@lyfjastofnun.is
Ireland	dataprotectionofficer@hpra.ie
Italy	responsabileprotezionedati@aifa.gov.it
Latvia	ct@zva.gov.lv
Liechtenstein	*To be confirmed*
Lithuania	*To be confirmed*
Luxembourg	info_donnees@ms.etat.lu
Malta	*To be confirmed*
Netherlands	datalek@minvws.nl
Norway	personvern@legemiddelverket.no
Poland	*To be confirmed*
Portugal	dpo@infarmed.pt
Romania	ro-ctis.datacontroller@anm.ro
Slovakia	CTIS@health.gov.sk
Slovenia	info@jazmp.si
Spain	delegado_protecciondatos@aemps.es
Sweden	kp.central@lakemedelsverket.se

Sponsors and marketing authorisation applicants/holders:

Contact points of the sponsors and marketing authorisation applicants/holders are indicated by the users within the CTIS or at the time of registration to get access to the CTIS.

A dedicated contact point for Data Subjects should also be available from the organisations' website.

Annex II

Data protection notice regarding personal data processing in the Clinical Trials Information System (CTIS)

This Data protection notice explains the most essential details of the processing of personal data in the context of the operation of the Clinical Trial Information System (CTIS), including the EU Portal and the EU Database established in accordance with the requirements of Article 80 and 81, respectively, of the Regulation (EU) No 536/2014[7], hereinafter the Clinical Trials Regulation.

The European Medicines Agency (hereafter referred to as 'the Agency'), in collaboration with Union Member States and the European Commission, has set up the CTIS database and it is responsible for its maintenance. CTIS enables the submission of clinical trials related information, from submission of clinical trials applications up to supervision during the clinical trial life cycle.

This Data protection notice explains the most essential details of the processing of personal data in CTIS, which includes:

the area of clinical trials applications and supervision during the trial lifecycle. This information is submitted through the EU Portal and stored in the EU Database;

the area of submission and evaluation of annual safety reports (ASRs).

The joint controllers ensure that processing of personal data in the context of the operation of the CTIS 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) are: European Commission, European Medicines Agency, Member States, commercial, non-commercial organisations and academia acting as sponsors of clinical trials and marketing authorisation applicants/holders.

The Parties of the Joint Controllership Arrangement act as joint controllers for the purpose of processing operations of personal data provided, in structure data and documents, in CTIS. The contact points of joint controllers are the following:

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

European Commission: SANTE-DATA-PROTECTION-COORDINATOR@ec.europa.eu

Member States: Annex I of the JCA

For sponsors or marketing authorisation applicants/holders contact points are identified at the time of their registration in CTIS.

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 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

7 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

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?

The Agency engages third parties to provide support for the:

development of CTIS functionalities;

maintenance of CTIS functionalities;

assurance of data quality in CTIS.

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 CTIS data processing activities can be summarised as follow:

Area of clinical trials: data and documents for a clinical trial submitted through the EU Portal to the EU Database in the context of:

The sponsor can submit through the EU Portal to the EU Database, Clinical Trials Applications (CTA) and subsequent modifications, responses to the request for information raised as part of the evaluation process, notifications, summary of results, opinions to corrective measures and response to an *ad hoc* assessment.

Following these submissions by the sponsors, there will be a corresponding evaluation carried out by the Member States concerned, responsible for the supervision of the clinical trials in their territory including inspections.

Marketing authorisation applicants/holders can submit clinical study reports with appendices, except those listing individual patient data.

Area of Annual Safety Reports (ASR):

Regarding investigational medicinal products other than placebo, the sponsor shall submit annually to the Agency a report on the safety of each investigational medicinal product used in a clinical trial for which it is the sponsor. This will be done via the submission of ASR to CTIS. Member States shall cooperate in assessing the information reported.

Personal data might be provided to enable compliance with the following:

For CTIS registered users:

To enable registration in CTIS and ensure user access management, via Identity Access Management (IAM) system, used to generate users' credentials to access CTIS secure domain;

To enable registered users uploading, viewing, changing the CTIS contents/documents in accordance with their access permissions;

To enable communication between the registered CTIS users and joint review of the CTIS contents;

To enable receiving technical support and secure interaction with the CTIS.

For sponsors, including sponsor's staff and sponsor's third party representatives:

e.g., to enable compliance with the obligation of CTR.

For investigators, principle investigators.

e.g., to enable compliance with the obligation of CTR.

2.1. Categories of Data Subject and personal data concerned

In the context of the use of CTIS, the submission of clinical trials applications, submission of ASR and during the clinical trials life cycle, examples of personal data that can be processed by Member States (also through National Competent Authorities and Ethics Committees), the Agency, the European Commission, the marketing authorisation applicants/holders and sponsors of clinical trials are presented below[8]:

Personal data of CTIS registered users having access to the CTIS sponsor's and authority's secure domain:

- Personal data such as name, surname, e-mail address, are captured at the time of creation of the accounts via Identity Access Management, to obtain credentials to access CTIS;
- These details are visible in the CTIS secure domain to the Administrator(s) within the user's organisation for the purpose of administering users' profiles;
- Name, surname and role of the user in CTIS are visible via the 'user' tab for each clinical trial;
- Users contact details will be visible only in the CTIS secure domain, and not disclosed in the public domain.

Personal data provided by the sponsors, including sponsor's staff:

- Contact point in the Union (i.e. first name, last name, telephone number and e-mail address: will be captured only in CTIS secure domains and will not be disclosed in the public domain);
- Legal Representative (i.e. first name, last name, telephone number and e-mail address: will be captured in CTIS secure domain and will be made public;
- Scientific and public contact point (i.e. Functional contact point name, telephone number, e-mail will be captured in CTIS secure domain and will be made public. These are expected to be functional contact points;
- Third parties contact point (i.e. telephone number and e-mail address) of the third-party organisation to whom tasks have been delegated will be in CTIS secure domain and will be made public. These are expected to be functional contact points;
- Sponsor's contact details for ASR submission (Full name, organisation details, telephone number and e-mail address) are captured in the ASR module of CTIS in relation to the submission of the Annual Safety Report. These details will be captured only in CTIS secure domains and will not be disclosed in the public domain;

Personal data in documents provided by the joint controllers in CTIS:

The joint controllers will be required to provide in the CTIS secure domain several documents possibly containing personal data for example:

[8] See also section 4.2. of the Appendix, on disclosure rules, to the "Functional specifications for the EU portal and EU database to be audited - EMA/42176/2014

- Sponsor documents: protocol, investigator brochure, GMP certification, cover letter which may contain personal data of sponsor staff, qualified person for GMP, summary of results, others; [9]
- Authorities users, including Member States' experts: assessment reports and inspection reports; [10]
- Marketing authorisation applicants/holders: clinical study report (CSR) with appendices, except those listing individual patient data. It is important to note that the names (not signatures) of the sponsor and coordinating investigator signatories of the clinical study report and the identities of the investigator(s) who conducted the trial should remain visible in the clinical study report loaded into the database and will be made public.

Should any of these documents contain personal data, as applicable and as required in light of Article 81(2) of Regulation (EU) No 536/2014, this can be provided in the version of the documents 'not for publication'. The version of the documents 'for publication' should not contain personal data.

Personal data of principal investigators' conducting the trial at the site and the person issuing suitability statement of the facilities:

Principal investigator details captured in the CTIS secure domain include name, surname, telephone number, e-mail address. These may be provided as functional contact points, but if they are provided as contact details of natural persons these will be made public.

- The following information will be made public from the database:
- The list of principal investigators' names, contact details and the names and addresses of the clinical trial sites;
- Investigator CV, including training on the principles of good clinical practice or other relevant experience, but in any case, containing only professional information relevant to the conduct of clinical trials;
- Any conditions, such as economic interests and institutional affiliations, that might influence the impartiality of the investigators;
- The written statement issued by the head of the clinic/institution or some responsible person testifying to the suitability of the facilities and human resources available for the trial is part of the application dossier, will include the name of the person issuing that statement.

Personal data of users creating records of new organisations / new locations in Organisation Management System (OMS)[11] for the purpose of use in CTIS:

- When creating a new organisation in OMS, or a new location for an existing organisation, the user is prompted to provide certain details. Requestors details provided at the time of registration via OMS will not be captured in the CTIS secure domain and therefore not be made public.

However, organisation details, like telephone number and e-mail address provided for the organisation/location registered in OMS, will be captured in CTIS secure domain and will be made public.

[9] With regard to ASR, in order to comply with Art 43.3 of the CTR and protect patients' rights, SARs in the line listing should be identified by case ID and study ID without including subject ID in the document. Similarly, the case ID and study ID when reporting the list of deceased and trial participants who dropped out in association with an AE, should not allow the identification of natural persons, see also https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-10/regulation5362014_qa_en.pdf

[10] There is no specific requirement in the Clinical Trials Regulation for the names of Member State experts to be included in the database.

[11] The OMS provides a single source of validated organisation data that can be used as a reference to support EU regulatory activities and business processes. It stores master data comprising organisation name and location address for organisations such as sponsors, regulatory authorities and manufacturers.

2.2. Legal basis of the processing

The processing of the personal data in CTIS, including collection, publication and archiving of clinical trial information in documents and structured data, is necessary for the management and functioning of the Agency and the performance of its tasks carried out in the public interest mandated by Union law, as controller of the CTIS, which includes the EU Portal and Database, for the effective materialisation of the objectives of the Clinical Trials Regulation. 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.

In addition, the Member States, the European Commission, the commercial, non-commercial organisation and academia acting as sponsors of clinical trials and marketing authorisation applicants/holders, are also joint controllers in the CTIS. They are legally obliged to collect and upload relevant documents in the CTIS. Therefore, the data processing by the Member States and the European Commission 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. In the case of sponsors and marketing authorisation applicants/holders their activities in CTIS and the related personal data processing is necessary for compliance with their legal obligations under the Clinical Trials Regulation in accordance with Article 6(1)(c) of the GDPR.

Since personal data processing by the Agency and the European Commission in the CTIS is based on the legal ground that this is necessary for the performance of a task carried out in the public interest, Data Subjects (i.e. those individuals whose data is processed in CTIS) **have the right to object against such processing**. See section 5 below.

2.3. Transfer of personal data outside of EU/EEA

The data centres used for CTIS 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 CTIS 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 CTIS 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 personal data in CTIS?

Clinical Trials data and documents and Annual Safety Reports provided in CTIS are going to be retained in CTIS for an initial period of 25 years[12] upon which the retention of the data will be subject to review.

The initial retention period starts from the date of the launch of CTIS, on 31 January 2022.

[12] Retention period of data and documents in CTIS has been set for an initial period of time of 25 years by analogy with the timing foreseen for the maintenance of a trial master file as defined in Article 58 of the CTR. The obligations for sponsors and investigators under Article 58 of Regulation (EU) No 536/2014 remain intact.

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

The provisions of access to the CTIS secure domains for authorities (the Agency, European Commission, National Competent Authorities and Ethics Committees on behalf of Member States) and sponsors, marketing authorisation applicants/holders, where data and documents are stored, are set in the 'Functional specifications for the EU portal and EU database to be audited', which foresees the implementation of a role based access and the assignment of roles and permissions to CTIS users.

CTIS users will have access to the clinical trials information based on their profile, therefore, not all the users in CTIS will have access to the same level of information or documentation that may contain personal data.

A public module of CTIS will ensure increased transparency and access to clinical trials data. Article 81(4) of Regulation (EU) No 536/2014 states that the EU database shall be publicly accessible unless, for all or part of the data and information contained therein, confidentiality is justified on the grounds: of protecting personal data. Accordingly, personal data is not expected to be published on the public module of the CTIS, unless otherwise specified, in accordance with data protection requirements.

5. Data subjects' data protection rights

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 CTIS, collect and use personal data. Requests for other information regarding the processing may also be directed to datacontroller.clinicaltrials@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.
- **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.
- **Right to object – Data subjects have the right to object at any time to this processing on grounds related to their particular situation**. In case of such objection against the processing, it must be stopped unless it is shown that the personal data is processed for compelling legitimate reasons which override the interest or rights raised by the data subject, or if it is needed for the establishment, **exercise** or defence of legal claims.

The rights of the data subjects can be exercised in accordance with the provisions of Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, as may be the case.

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)** via 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