25 January 2022
EMA/616933/2021

Questions and Answers on the Joint Controllership Arrangement and data protection matters related to the use of the Clinical Trials Information System

Version 1.0

This document has been prepared to address questions received in the context of the Joint Controllership Arrangement (JCA) and data protection matters related to the use of the Clinical Trials Information System (CTIS).

The EMA Management Board endorsed the CTIS JCA at their meeting on 7 October 2021. The current version of the CTIS JCA dated 7 December 2021 includes an update to Annex II thereof, i.e. the Data Protection Notice by the European Medicines Agency.

The present document is intended to complement and clarify the CTIS JCA and the CTIS Data Protection Notice (Annex II of the CTIS JCA) and does not replace it.

Updates to this Questions and Answers document will be performed as required taking into account the experience gained with the operation of CTIS, which will go-live on 31 January 2022, and in case any amendments to the JCA will become necessary.

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

Table of Contents

Acronyms

Acronym	Description
CSR	Clinical Study Report
CTIS	Clinical Trials Information System
CTR	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 (Clinical Trial Regulation)
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor
EMA	European Medicines Agency
EUDPR	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 (European Union Data Protection Regulation)
GDPR	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
JCA	Joint Controllership Arrangement
MSs	Member States of the European Union
Sponsors	Sponsors of clinical trials
MAAs	Marketing Authorisation Applicants
MAHs	Marketing Authorisation Holders

Questions and Answers on the Joint Controllership Arrangement and data protection matters related to the use of the Clinical Trials Information System

1. What is meaning of data subject in the context of the CTIS?

Regulation (EU) 2016/1679 (the "GDPR") and Regulation (EU) 2018/1725 (the "EUDPR") define a data subject as "*an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number or to one or more factors specific to the physical, physiological, genetic or mental identity of that natural person*[1]."

In the context of CTIS, "data subject" means authorised CTIS users, sponsors contacts, principal investigators and clinical trial participants. Their personal data processed in CTIS refers to:

- names and contact details of authorised CTIS users having access to the respective CTIS secure domains,
- administrative trial information such as the name and email address of the contact points of sponsors,
- name and surname of principal investigators; and
- pseudonymised information as regards clinical trial participants such as the participant's clinical trial identification number, age or gender.

It bears reminding that the principles of data protection shall not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable[2].

For further details, please refer to chapter 2.1 "Categories of Data Subject and personal data concerned" of EMA data protection notice (Annex II to the CTIS JCA).

2. How can personal data be protected in CTIS?

The principles of data protection apply to any information concerning an identified or identifiable natural person. The application of pseudonymisation to personal data of clinical trial participants can reduce the risks to the data subjects concerned and help a controller to meet their data protection obligations[3].

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable natural person[4] without the cooperation of the holder of the additional information needed (e.g. the key code linking trial participant number to the identified trial participant, which is held separately by the investigator).

[1] In this respect, see: Article 4(1) and recital 26 of the GDPR; Article 3(1) and recital 16 of the EUDPR.
[2] Recital 26 of the GDPR and recital 16 of the EUDPR.
[3] In this respect, see: recital 28 of the GDPR and recital 17 of the EUDPR.
[4] Article 3(6) of the EUDPR and Article 4(5) of the GDPR

For the processing concerned, e.g., when a user uploads pseudonymised data in the respective secure domain of CTIS, the controller is responsible to take technical and organisational measures to ensure that additional information for attributing the personal data to a specific data subject is kept separately and secure to mitigate data protection risks when processing personal data.
For example, the inclusion of a trial participant's number and details of information related to a trial participant (i.e. key coded data of the trial participant) is allowed in the '*not for publication*' version of documents.
Versions of the documents '*for publication*' should not contain personal data of trial participants i.e., personal data are to be anonymised (see Question 7.).

3. Is the content of the CTIS JCA based on a defined structure?

In the context of the CTIS JCA, joint controllers enter into a specific arrangement laying down their roles and responsibilities, in particular towards the data subjects. In practice, such a written arrangement is the legal instrument establishing the relationship between the different Parties involved in the joint controllership. The structure of a joint controllership arrangement is outlined in the EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/17255. That structure has been used as a model in the preparation of the CTIS JCA, which also includes two Annexes.
Annex I to the CTIS JCA includes a list of contact points for cooperation between the different Parties[6] subject to the CTIS JCA and having access to the CTIS secure domain as applicable, and for data subjects in respect of queries, complaints and provision of information within the scope of the Arrangement.
Annex II thereof provides a Data Protection Notice regarding personal data processing in the CTIS.

4. How was the CTIS JCA endorsed and how is it accepted by CTIS users?

Following consultation by EMA, the EDPS confirmed[7] that the following Parties are joint controllers of the CTIS: European Commission, EMA, the EU/EEA MSs, commercial and non-commercial organisations including academia acting as sponsors and MAAs/MAHs while having access to the CTIS secure domain. The concept of "joint controllers" is enshrined in Article 26 of the GDPR and Article 28 of the EUDPR.
The text of the CTIS JCA sets out the roles and responsibilities of the joint controllers in relation to the processing of personal data while using and interacting with CTIS (for details see chapter 1 of the CTIS JCA). Representatives of the Parties acting as joint controllers of CTIS were engaged in the drafting of the JCA and endorsed the final text at dedicated meetings on 23 and 24 September 2021.
The EMA Management Board endorsed the CTIS JCA at their meeting on 7 October 2021.

[5] https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf
[6] Parties mentioned in the CTIS JCA are: the European Medicines Agency, the European Commission, the EU/EEA Member States and commercial and non-commercial organisations, SME and academia having access to the secure domains of CTIS
[7] EDPS Case Number C 2018-0642

The current version dated 7 December 2021 includes an update to Annex II thereof, the Data Protection Notice by the European Medicines Agency, and can be accessed at the EMA webpage as follows: Joint Controllership Arrangement (JCA) for CTIS (europa.eu)

The endorsed CTIS JCA is also made available to all users in the secure domain of the CTIS. When accessing the system for the first time, each CTIS user is required to confirm acceptance of the terms set out in the JCA.

5. Who is responsible to comply with the data protection obligations set out in the CTIS JCA?

The CTIS JCA defines the allocation of respective roles, responsibilities and practical arrangements between the Parties (see question 4.) for compliance with their data protection obligations under the EUDPR and GDPR, when carrying out processing operations of personal data of data subjects, collected as part of the use of CTIS. For the purpose of the JCA, the Parties are considered as 'joint controllers' within the meaning of Article 26 of the GDPR and Article 28 of the EUDPR.
An authorised administrator of a Party (entity) will assign to a CTIS user roles and permissions in accordance with defined categories before the user can perform any activity in CTIS. Each CTIS user, when accessing CTIS for the first time, needs to be familiar with and accept the content of the CTIS JCA and thereafter comply with the obligations in accordance with the JCA itself and the GDPR and/or EUDPR, as applicable.
In case of non-compliance with the obligations set out in the CTIS JCA, it is the joint controller who is held responsible for the non-compliance stemming from the processing activities performed in CTIS i.e., the Party to which, or on behalf of whom, the individual user (which may include the Party's partners or contractors) has been granted access to CTIS. . For details, please refer to chapter 4 "Liability for non-compliance" of the CTIS JCA.
It is important to note that each of the joint controllers can act as an independent controller at its end for the processing activities that can be performed without the cooperation of the other Parties. The general concept of "controller" is enshrined in point (7) of Article 4 of the GDPR and point (8) of Article 3 of the EUDPR , respectively i.e., the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
For example, sponsors or MAA/MAHs are independent data controllers in relation to the data processing activities performed outside of CTIS and carried out within their organisation, whether related to clinical trials or not.

6. What is the role of the DPO in an organisation and related CTIS JCA responsibilities?

The role of a Data Protection Officer is clearly defined in section 4 of the GDPR and section 6 of the EUDPR. That officer should be a person with expert knowledge of data protection law and practices, which should be determined according to the data processing operations carried out by the controller, or the processor, and the protection required for the personal data involved. Such data protection officers should be in a position to perform their duties and tasks in an independent manner.
Amongst others, a DPO performs the following tasks:

- to inform and advise the (joint) controller and the employees who carry out processing of their obligations pursuant to the GDPR/EUDPR and to other Union or Member State data protection provisions including those set out in the CTIS JCA;
- to monitor compliance with the GDPR/EUDPR, with other Union or Member State data protection provisions and with the policies of the (joint) controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations including CTIS, and the related audits.

The responsibility for potential non-compliance with the obligations set out in the CTIS JCA rests with the legal entity which is the data controller.

7. To which extent do users need to protect personal data in the version of clinical documents for regulatory use and the version intended for publication?

The purpose of a clinical trial is to gather reliable and robust data on an investigational medicinal product. This fundamental principle is confirmed by Article 3(b) of the Clinical trials Regulation (CTR). To this extent the sponsor or investigator, as applicable, shall record, process, handle, and store all clinical trial information in such a way that it can be accurately reported, interpreted and verified while the confidentiality of records and the personal data of the subjects remain protected in accordance with the applicable law on personal data protection[8].

Furthermore, the sponsor is required to implement appropriate technical and organisational measures to protect information and personal data processed against unauthorised or unlawful access, disclosure, dissemination, alteration, or destruction or accidental loss, in particular where the processing involves the transmission over a network (Article 56(2) of the CTR) e.g., to the CTIS.

One of these measures include the application of pseudonymisation to personal data, which can reduce the risks to the data subjects concerned (see Question 2.).

The CTIS has been established to enable cooperation between the competent authorities of the Member States concerned to the extent that it is necessary for the application of the CTR, to facilitate the communication between sponsors and Member States concerned and to enable sponsors to refer to previous submissions of an application for authorisation of a clinical trial or a substantial modification (Article 81(2) of the CTR). Both Member States concerned, and sponsors are responsible for the continuous supervision of the benefit/risk balance of the trial.

To this end, CTIS shall contain personal data only insofar as this is necessary for such purposes (Article 81(6) of the CTR). From a data protection perspective, this meets the principle of purpose limitation and data minimisation i.e., personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed[9].

In the context of transparency of clinical trials in CTIS and to protect the right of trial participants to private life and the right to the protection of personal data, Article 81(7) of the CTR sets out that no personal data of subjects shall be publicly accessible, which is further reinforced by Article 81(4) of the CTR that states that the CTIS shall be publicly accessible except where justified to protect the confidentiality of personal data.

[8] Article 56(2) of the CTR.

[9] Article 5(c) of the GDPR and Article 4(c) of the EUDPR.

Chapter 2.1 "Categories of Data Subject and personal data" of the Data Protection Notice (Annex II of the CTIS JCA), which applies to all Parties therefore states the following:
"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." Exceptions apply where such data is required to be in the public domain (such as the name of the clinical investigator and address of their site).

8. Why has the title of the privacy statement been changed to data protection notice?

The European Data Protection Supervisor (EDPS) recently informed all European Union Institutions and bodies that the term "Privacy Statement" used in all previously published documents should be replaced by "Data Protection Notice". This change has been reflected accordingly in the CTIS Privacy Statement, which is also contained in Annex II to the CTIS JCA.

9. What is the purpose and structure of the Data Protection Notice (Annex II to CTIS JCA)?

The Data Protection Notice is addressed to data subjects and explains the reason for the processing of personal data, the way CTIS collects, handles and ensures protection of all personal data provided, how that information is used and what rights data subjects (e.g., CTIS users, sponsors, investigators, trial participants) have in relation to their personal data. It also specifies the contact details of the responsible Joint Controllers with whom data subjects may exercise their rights, the EMA Data Protection Officer and the EDPS.
The structure of the Data Protection Notice is based on the template provided by the EDPS[10].
The Data Protection Notice is authored by EMA and as a document is not endorsed or accepted *per se* (see Question 4.). The Data Protection Notice is an annex to the CTIS JCA (Annex II), is subject to publication on the CTIS public domain and is also made available to registered users within the CTIS secure domain. In addition, as an independent controller, the other Parties to the CTIS JCA may have published their own Data Protection Notice(s) as regards the processing at their end of personal data relevant in the context of clinical trials.

10. Can a Party authorise a user to access the secure domain of CTIS from outside the EU/EEA?

The terms for a Party to authorise a user to access the secure domain of CTIS from outside the EU/EEA are set out in chapter 3.6 "Localisation of personal data" of the CTIS JCA.

11. Who should report security incidents, including those involving personal data breaches?

The process of managing security incidents in the context of CTIS, including those involving personal data breaches, is set out in chapter 3.3. of the CTIS JCA. Whichever Party/joint controller first detects a security incident, including when such incident involves a personal data breach within the scope of

[10] https://edps.europa.eu/data-protection/our-work/publications/other-documents/privacy-statements-template_en

the CTIS JCA[11]) or receives a report/information from another entity/person identifying such occurrence, should immediately notify all other Parties. This is irrespective of whether the Party reporting the security incident, including such that involve a personal data breach, is responsible. The notification should be addressed to the contact points set out in Annex I of the CTIS JCA. Further investigation may be required by the Parties as the route cause at the time of notification might not be clear.

The Parties are responsible to handle security incidents, including those involving personal data breaches, in accordance with their internal procedures and applicable legislation. Furthermore, the Parties should provide each other with swift and efficient assistance as required to facilitate the identification and handling of any security incidents, including those involving personal data breaches, linked to the joint processing.

Each Party is responsible for managing all security incidents, including those involving personal data breaches, that occur as a result of an infringement of their (that Party's) obligations as set out in the CTIS JCA and in accordance with the EUDPR and GDPR, respectively.

Examples of personal data breach notifications are provided in the European Data Protection Board guideline 01/2021[12]. Further useful instructions in dealing with data breaches are provided by the European Data Protection Supervisor in the "Guidelines on personal data breach notification for the European Union Institutions and Bodies"[13].

12. In what circumstances would EMA expect another Party to assume responsibility for the management and reporting of a personal data breach caused by a failure of technical security measures?

The roles and responsibilities are set out in chapter 3.3 "Management of security incidents, including personal data breaches" of the CTIS JCA. Examples where a Party, other than EMA, would need to assume responsibility for the management and reporting of a personal data breach related to a failure of technical security measures in the context of CTIS are the following:

	Example 1	Example 2
Example	Data have been exfiltrated from a compromised end user device due to a malicious code placed within the device.	Data have been exfiltrated from CTIS by an ex-employee.
Assumption	This device is used for processing activities within the CTIS application. The malicious code may give the attacker full control over the device.	The employer left the organisation and maintained the CTIS user-ID and password.
Data Breach Notification	Notify Parties within the scope of the CTIs JCA in accordance with Annex I.	Notify Parties within the scope of the CTIs JCA in accordance with Annex I.

[11] See chapter 1 of the CTIS JCA, "Scope of this arrangement".
[12] https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf
[13] https://edps.europa.eu/sites/default/files/publication/18-12-14_edps_guidelines_data_breach_en.pdf

	Example 1	Example 2
Mitigation Action	Joint controller concerned is responsible to implement adequate security measures for end user devices and to remedy the breach identified.	Joint controller concerned is responsible to implement adequate security measure for leavers (offboarding) e.g., disable account and access and to remedy the breach identified.