# *1 YEAR INTO THE GDPR, AS SEEN FROM A CRO'S PERSPECTIVE*

2 April 2019

Uwe W Fiedler, Chief Privacy Officer

**DISCLAIMER:** **The views expressed in the workshop slides are purely those of the presenter and may not in any circumstances be regarded as providing legal advice or stating an official position of PAREXEL International Corporation**

PAREXEL®

YOUR JOURNEY. OUR MISSION.®

© 2019 PAREXEL INTERNATIONAL CORP.

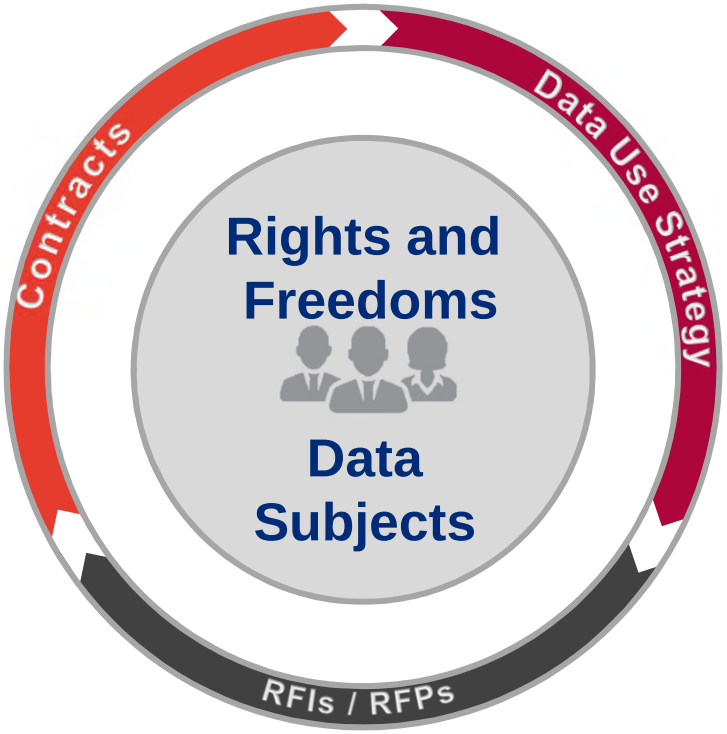
# AGENDA



PAREXEL

# CONTRACTS AND THE PERSONAL DATA PROCESSING LIFE CYCLE

- **Joint data controller arrangements**
- **“Classical” Data Processing Agreements**
- **Investigators**
- **Niche service providers**




- **Identifiability of clinical trial data**
- **Legal Grounds**
- **Data Protection Impact Assessments**

- **(Joint) data controller versus data processor**
- **Examples of pitfalls**

© 2019 PAREXEL INTERNATIONAL CORP. 

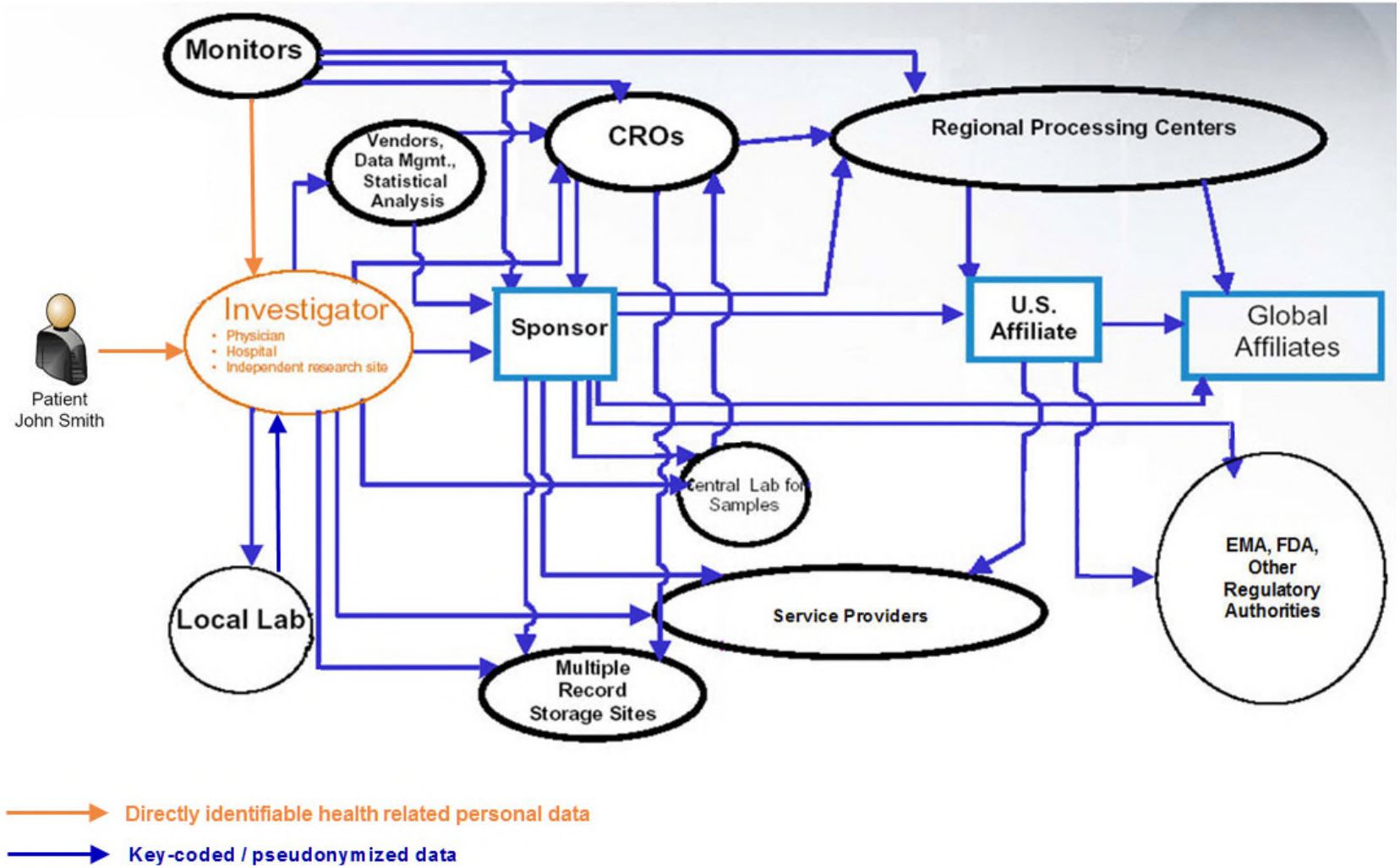
PAREXEL

# DATA USE STRATEGY



PAREXEL

# DATA FLOWS WITHIN CLINICAL TRIALS






PAREXEL

# *IDENTIFIABILITY OF CLINICAL TRIAL DATA*

- **Identifiability of clinical trial data**
  - Under the Declaration of Helsinki and ICH GCP guidelines, only investigators have the right to know the identity of study participants; study sponsors and CROs operating on behalf of the sponsor do not.
  - In November 2012, the UK Data Protection Authority ICO stated in "Anonymisation: managing data protection risk code of practice" that the disclosure of key-coded study data to a party that does not possess the key is not a disclosure of personal data.
  - On 19 October 2016 the European Court of Justice, in a decision concerning dynamic IP addresses (the Breyer case (C-582/14)), ruled that dynamic IP addresses are indirectly identifiable personal data **if** the recipient has legal means which enable the identification of the data subject with the assistance of other parties

➢ **It logically follows that clinical trial data are personal data for investigators, but no longer are personal data when passed to sponsors or CROs of sponsors in key-coded form.**



PAREXEL

# LEGAL GROUNDS FOR THE COLLECTION OF CLINICAL TRIAL DATA

- **Typically, ICFs are used as the legal ground to collect personal data from study participants and to share the data in key-coded form with sponsors**
- **Section 2.1 of EDPB opinion 03/2019 addresses the interplay between Clinical Trial Regulation (CTR) and GDPR:**

> *10. The EDPB is of the opinion that the processing operations expressly provided by the CTR and by relevant national provisions, and which are related to reliability and safety purposes, can be considered as falling within "legal obligation(s) to which the controller is subject" under Article 6(1)(c) of the GDPR.*
>
> *12. Therefore, the processing of personal data in the context of safety reporting …, have to be considered as necessary to comply with legal obligations to which the sponsor and/or the investigator are subject to.*
>
> *13. The corresponding appropriate condition for lawful processing of special categories of data in the context of these obligations shall be Article 9(2)(i) …*

- ➢ **<u>If</u> key-coded study data are defined as personal data, <u>and</u> pursuant to CTR are related to reliability and safety purposes, the** *"legal obligation(s) to which the controller is subject"* **applies, and no other legal grounds would be necessary for the collection of study data.**
- ➢ **Consequently study ICFs won´t contain any longer GDPR language**



PAREXEL

# DATA PROTECTION IMPACT ASSESSMENTS

- **Attention - Art 35 (1) states:**

> *Where a type of processing, particularly one using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*

- **Consequently, DPIAs should be performed prior to RFIs / RFPs or the negotiation of Data Processing Agreements**
- **Art 35 (1) also clarifies that DPIAs should only be performed "*where a type of processing <u>is likely to result in a high risk</u> to the rights and freedoms of natural persons*"**
- **The European Union Agency for Network and Information Security (ENISA) recently published two GDPR compliance related guidelines that clarify that both encryption and pseudonymization are appropriate security and privacy enhancing technologies and in particular stated that "*… in the GDPR context, pseudonymization can motivate the relaxation to a certain degree of data controllers' legal obligations if properly applied. …*"**



PAREXEL

# DATA PROTECTION IMPACT ASSESSMENTS

- **Regarding clinical trials:**
  - Investigators process the names of study participants together with health information
  - Both the sponsor and CROs operating on behalf of the sponsor only receive and process pseudonymized clinical trial data

➢ **Is it reasonable to think that the pseudonymization of clinical trial data is likely to result in a higher risk to the rights and freedoms of study participants than the processing of the names of study participants together with health information?**

➢ **If not – only investigators would have to perform DPIAs; sponsors and CROs operating on behalf of sponsors would not!**

➢ **Taking the EDPB opinion into account – if in the future the processing of clinical trial data is considered to be necessary to comply with legal obligations - is it reasonable to think that the processing of such data could result in a high risk to the rights and freedoms of study participants?**



PAREXEL

# REQUEST FOR INFORMATION
# REQUEST FOR PROPOSAL



PAREXEL

# DATA USE STRATEGY FIRST, RFI / RFP SECOND

- **Data controller versus joint data controller versus data processor**
  - Data controller(s) (jointly) determines the purposes and means of the processing of personal data
  - The purposes and means of the processing of personal data depend on the data use strategy of the data controller (not the other way around)
  - The GDPR does not clarify who “owns” personal data, so joint data controllership scenarios typically result in “joint data ownership”
  - Remember – a data processor processes personal data <u>only on documented instructions</u> from the data controller (including the transfer of personal data to a third country)
- **Please don´t comingle RFIs / RFPs with Data Processing Agreements**
  - Unclear data use / analysis strategy = unclear RFIs / RFPs
  - Unclear RFIs / RFPs = Data Processing Agreements that won´t support the data use / analysis strategy of the data controller!



PAREXEL

# EXAMPLES FOR PITFALLS

- **Legal grounds I – please don´t ask your data processor for the legal grounds that will justify the collection of personal data – this is the task of the data controller**
- **Legal grounds II - please don´t simply ask your data processor "how do you ensure GDPR compliance?"**
  - The legal ground for the processing of personal data by your data processor will be the Data Processing Agreement
  - If you already have a template that covers the intended outsourcing, just attach it to your RFI / RFP and obtain information that will verify the data processor is generally able to comply (this won´t be a legal review)
- **Data processing locations and international data transfer**
  - Please don´t just ask your data processer where your data will be processed
  - Instead articulate data transfer restrictions and ask for experience regarding alternatives



PAREXEL

# EXAMPLES FOR PITFALLS

- **Data classification – the data controller defines the sensitivity of the processed data, not the data processor**
- **Data classification II – the sensitivity of the processed data dictates the technical and organizational protection measures**
- **Data classification III – over-classification could also affect the data use / data analysis abilities of the data controller as data processors have no own legal grounds for the collection of personal data. For example, the classification of data elements as special categories of data will not "disappear" solely because the data will be forwarded to the data controller**
- **Protection measures already implemented because of the nature of the requested services – as clarified by the ENISA "*… pseudonymization is an established and accepted de-identification process that has gained additional attention following the adoption of the GDPR, where it is referenced as both a security and data protection by design mechanism. …*"**



PAREXEL

# EXAMPLES FOR PITFALLS

- **Information Security / IT Security**
  - Please remember Art 28 (1)*… the data controller shall use only data processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject*
  - Data controllers must define their technical and organizational protection requirements first, then obtain information verifying that the data processor is able to comply
  - Please remember - the sensitivity of the processed data dictates the technical and organizational protection measures needed
  - In case of discrepancies – data controllers should request information about alternative protection measures (data processors standardize their protection measures based on average customer requirements and your requirements may be typical)



PAREXEL

# CONTRACTS



PAREXEL

# *JOINT DATA CONTROLLER ARRANGEMENTS*

- **Art 26 does not require a contract; it instead refers to an *… arrangement that shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects***
- **In contrast to Art 28, Art 26 does not contain detailed requirements for joint data controller arrangements but**
  - Art 26 (2) … *the essence of the arrangement shall be made available to the data subject*
  - Art 26 (3) … *the data subject may exercise his or her rights under the GDPR in respect of and against each of the controllers*

➢ **Art 26 offers some flexibility to permit companies to define internal joint data controller relationships based on company policies**

➢ **Proving the legal validity of joint data controller arrangements could become complicated as currently neither best practices nor "real world" experiences exist (as opposed to "classic" Data Processing Agreements)**



PAREXEL

# “CLASSIC” DATA PROCESSING AGREEMENTS – GENERAL REQUIREMENTS

- **As clarified by Art 28 (3), a Data Processing Agreements should set out:**
  - the subject-matter of the processing,
  - the duration of the processing,
  - the nature and purpose of the processing,
  - the type of personal data
  - the categories of data subjects and
  - the obligations and rights of the controller

- **From a GCP point of view such requirements are not new and the EMA reminded sponsors in January 2017 that “*… due diligence should be exercised from the sponsor in order to ensure that the distribution of tasks is clearly documented and agreed by the vendor, and that each party has the control and access to the data and information that their legal responsibilities require. …*”**



PAREXEL

# “CLASSIC” DATA PROCESSING AGREEMENTS – GENERAL REQUIREMENTS

- **Art 28 (3) (a) requires “*that contract … shall stipulate, in particular, that the data processor processes the personal data only on <u>documented instructions</u> from the data controller*”:**
  - An increasing number of MSAs are being used as Data Processing Agreements but do not contain service-specific instructions
  - If a Statement of Work is used as documentation of instructions, notice of this should be provided in the Data Processing Agreement
  - In case emails or IMs will be used – the Data Processing Agreement should clarify how these instructions will be documented and, in particular, archived
- **It can be efficient and effective to also use the Data Processing Agreement to document the outsourced personal data processing activities (Art 30 (1)) – in particular, because Art 30 (4) clarifies that data protection authorities can request access to such records.**



PAREXEL

# “CLASSIC” DATA PROCESSING AGREEMENTS – GENERAL REQUIREMENTS

- **Art 28 (2); (3) (d) and (4) offer two options for the use of sub-processor(s):**
  1. General provisions for a first data processor sub-contracting certain activities to additional sub-processors include:
     - Verify if the CRO uses a standardized Data Processing Template for sub-contracting service related tasks
     - If the language is acceptable, note in the Data Processing Agreement that sub-contractors can be contracted based on the Data Processing Template
     - Provide instructions regarding notification of the use of sub-contracted sub-processors
  2. Specific authorization for each intended sub-contractor

- **International data transfer (Art 28 (3) (a)) -– It can be efficient and effective to incorporate a clear mandate for the first EEA data processor to add additional non-EEA sub-processor(s) in the name and on behalf of the EEA data controller** ***(WP 176 Section 3 (b), adopted by Art 29 Data Protection Working Party on 12 July 2010)***



PAREXEL

# “CLASSIC” DATA PROCESSING AGREEMENTS – GENERAL REQUIREMENTS

- **Data Breach reporting:**
  - Art 33 (2) states “*The data processor shall notify the data controller without undue delay after becoming aware of a personal data breach*”. Therefore the GDPR does not contain a fixed data breach reporting deadline for data processors, but the sensitivity of the processed data will dictate the timeliness of potential data breach reporting.
  - Please remember – the data controller data breach notification deadline of 72 hours (Art 33 (1)) starts to tick once the data processor has informed the data controller
  - Therefore, take into account the use of sub-processors if you request a fixed data breach reporting deadline in the Data Processing Agreement
  - Please also take the implemented protection measures (e.g. pseudonymization and/or encryption) into account as it may be beneficial to request the reporting of issues regarding such protected data as a Quality Issue instead of a Data Breach (remember - in accordance to Art 33 (1), the data controller solely decides if an incident becomes a Data Breach or not)



PAREXEL

# “CLASSIC” DATA PROCESSING AGREEMENTS – SPECIFIC SITUATIONS

- **Processing of personal data of data processor employees by the data controller**
  - Frequently, sponsors request disclosure of certain personal data of CRO staff (e.g. CVs, signed JDs, training compliance reports):
    - Caution – data protection authorities expressed concern when data controllers ask their employees for consent to the disclosure of personal data. Can sponsors ask employees of CROs for their consent for the disclosure of their personal data?
    - As an alternative, a data controller to data controller transfer could be used that includes appropriate data transfer and protection language in the MSA (including EU model clauses). This would allow CROs (as employers) to disclose the personal data of their employees
    - CROs can offer to disclosure pseudonymization training compliance reports with a privacy by default approach (which would allow a sponsor’s auditor to verify the validity of shared pseudonymization training compliance reports with pseudonyms substituted for CRO staff names during an audit). It would be difficult for sponsors to reject such an approach where sponsors agree to accept pseudonymized clinical trial data!



PAREXEL

# “CLASSIC” DATA PROCESSING AGREEMENTS – SPECIFIC SITUATIONS

- **Data Protection Impact Assessments – Art 28 (3) (f) only requires that data processors assist data controllers, not that data processors perform Data Protection Impact Assessments on client data**
- **Information Security / IT Security – Art 32**
  - As clarified by Art 28 (3) (c), Data Processing Agreements have to contain details regarding the required technical and organizational protection measures
  - As outlined by Art 32 (1) these protection measures should take into account “*the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*”
  - Art 32 (1) (a) also highlights the pseudonymization and encryption of personal data as appropriate technical and organizational measures
  - As mentioned previously, the ENISA also highlighted both encryption and pseudonymization as appropriate security and privacy enhancing technologies



PAREXEL

# "CLASSIC" DATA PROCESSING AGREEMENTS – SPECIFIC SITUATIONS

- **Data Subject Access Requests**
  - Quite often, Data Processing Agreements require that CROs should be able to answer questions received from study participants
  - Art 28 (3) (e) clarifies that data processor "*assists the data controller … insofar as this is possible, for the fulfilment of the controller's obligation to respond …* "
  - Art 11 further clarifies:

> *1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.*
>
> *2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.*

  - Regarding Art 11 (2) – under ICH GCP confidentiality obligations neither a sponsor not a CRO are allowed to know the identity of study participants.



PAREXEL

# CLINICAL SITE AGREEMENTS WITH INVESTIGATORS

- **Traditionally, sponsors defined Investigators as independent data controllers and used the study ICF as the legal ground for the disclosure of key-coded study data**
- **Consequences for study ICFs and Clinical Site Agreements where other models will be used:**
  - If Investigators are defined as joint data controllers, the study ICF must be clear about the joint-controller relationship, the Clinical Site Agreements would have to define the respective responsibilities for compliance with the GDPR and the Investigator would have to share the essence of the joint data controller arrangements with study participants
  - If Investigators are defined as data processors, the study ICF must clarify the controller-processor relationship, the Clinical Site Agreements have to become Data Processing Agreements in accordance to Art 28, the sponsor, as the data controller, would have to address data breaches at research sites and would have to decide if Data Protection Impact Assessments are necessary
- **Clinical Site Agreements should regulate the use of niche service providers**



PAREXEL

# AGREEMENTS WITH NICHE SERVICE PROVIDERS

- **As clarified in the EMA Q&A on Good clinical practice (GCP):**

> *… Niche subcontractors are used increasingly for carrying out specific tasks of the sponsor, such as monitoring, data management, Interactive voice response systems (IVRS), management of electronic patient diaries or CRFs etc. In addition there are contractors who undertake tasks that are partly or wholly related to the responsibilities of the investigator, even though the contractor may have their main contract with, and be paid by, the sponsor (such tasks may include specialised testing, source data retention (especially in the context of e-CRF or e-patient diary) or patient recruitment or follow-up contacts). … Great care is therefore needed in ensuring that the distribution of tasks is clearly documented and agreed, "*

- **It currently seems that the GDPR allows an Investigator to appoint niche service providers either as a joint data controller or as a data processor:**
  - If appointed as a joint data controller, Art 26 (2) requires the sharing of the essence of the joint data controller arrangement with the affected study participants
  - If appointed as a data processor, it would be necessary to execute an Art 28 Data Processing Agreement with the niche service provider (if applicable together with appropriate EU model clauses)



PAREXEL

# AGREEMENTS WITH NICHE SERVICE PROVIDERS

- **It seems to be necessary to execute at least:**
  - Third Party Beneficiary agreements between sponsors and niche service providers that also clarify that the niche service provider warrants not to share with the sponsor / CROs data elements that could violate ICH GCP confidentiality obligations
  - Art 28 Data Processing Agreements between the Investigator and niche service providers
  - Depending on the role of the Investigator as (joint) data controller, Clinical Site Agreements should contain clarifications about the GDPR compliance accountabilities regarding niche service providers (e.g. who performs data Protection Impact Assessments in case the niche service provider will get access to medical records containing patient names, who will deal with data breach reporting in case of incidents, who is accountable to audit the niche service provider and who documents the data processing activities of the niche service provider)

# SUMMARY



PAREXEL

# MISSING HARMONIZATION ACROSS OUR INDUSTRY AND POSSIBLE SOLUTIONS

- **From a CRO point of view it appears that sponsor companies often tackle GDPR compliance solely from a legal compliance point of view**
- **This could be a result of the legal uncertainty arising from missing harmonization across the pharmaceutical industry**
- **As a result, Data Processing Agreements are being used which contain "innovative" GDPR compliance requirements that may not go hand in hand with data use & analyses strategies articulated by project team members**

- **The following solutions may be able to improve the situation:**

  1. **Reclassify / down-classify the processing of key-coded study data processed by sponsor / CROs in accordance with the Clinical Trial Regulation / ICH GCP to the processing of "quasi" anonymized data***

* please see my presentation at the 1. meeting of the EMA TAG



PAREXEL

# MISSING HARMONIZATION ACROSS OUR INDUSTRY AND POSSIBLE SOLUTIONS

2. **Develop a Code of Conduct in accordance to Article 40 GDPR that covers the processing of personal data <u>under CTR / ICH GCP</u>** and is applicable to investigators, sponsor companies and service providers:
   - Cover medical records processed by investigators / research site staff and key-coded study data processed by investigators / research site staff, sponsors and CROs (Art 40 (2) (d) GDPR)
   - Justify international data transfer (Art 40 (2) (j) GDPR)
   - Cover the disclosure of contact data, CVs and training records from investigators and research site staff as well as from service provider staff (Art 40 (2) (b) GDPR)

   o Improve the transparency of processed study data for study participants (Art 40 (2) (e) GDPR

   o Clarify the data protection compliance requirements for the protocol (Annex I D. 17. (ak), (al) and (am) CTR)



PAREXEL

# MISSING HARMONIZATION ACROSS OUR INDUSTRY AND POSSIBLE SOLUTIONS

3. **Develop a Code of Conduct in accordance to Article 40 GDPR that covers the processing of personal data <u>outside of the CTR / ICH GCP</u>:**

   - Non-interventional studies (or observational studies) are not covered by the CTR
   - Therefore, it seems to be more likely that an imbalance of power could arise between the participant and the sponsor/investigator (comparable to section 2.2 (Processing operations purely related to research activities) of the EDPB Opinion 03/2019).
   - Consequently, a dedicated Code of Conduct that covers processing operations purely related to research activities outside of the CTR / ICH GCP could improve the protection of the rights and freedoms of study participants
   - Such a Code of Conduct could also distinguish the primary use from the secondary uses (comparable to section 3 of the EDPB Opinion 03/2019)



PAREXEL

# *THANK YOU*



PAREXEL

# SOURCES OF INFORMATION

- **Breyer decision - http://curia.europa.eu/juris/documents.jsf?num=C-582/14**
- **UK Data Protection Authority ICO "Anonymisation: managing data protection risk code of practice - https://ico.org.uk/media/1061/anonymisation-code.pdf**
- **European Data Protection Board (EDPB) Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) - https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers-interplay_en**
- **European Medicines Agency (EMA) Technical Anonymization Group (TAG) - https://www.ema.europa.eu/en/events/technical-anonymisation-group-tag-first-meeting**
- **ENISA, Recommendations on shaping technology according to GDPR provisions, An overview on data pseudonymization - https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions**
- **ENISA, Recommendations on shaping technology according to GDPR provisions, Exploring the notion of data protection by default - https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2**
- **Art 29 Data Protection Working Party, WP 176 - FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, Adopted on 12 July 2010 - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp176_en.pdf**



PAREXEL

# SOURCES OF INFORMATION

- **EMA Q&A on Good clinical practice (GCP) - https://www.ema.europa.eu/en/human-regulatory/research-development/compliance/good-clinical-practice/qa-good-clinical-practice-gcp:**

  2. GCP sets out responsibilities for the sponsor and the investigator, but tasks are increasingly undertaken by a range of contractors – how should this situation be addressed?

  8. What are the pitfalls to be aware of regarding contractual arrangements with vendors for electronic systems in connection with clinical trials? New January 2017

- **The ownership of Big Data, Christopher Rees - http://united-kingdom.taylorwessing.com/globaldatahub/article_big_data_ownership.html**



PAREXEL