European Union General Data Protection Regulation – Effects on Research

Mark Barnes

Partner, Ropes & Gray LLP
Co-Director, Multi-Regional Clinical Trials Center of Brigham and Women's Hospital and Harvard

ROPES & GRAY

AGENDA

- Introduction and Jurisdictional Scope
- Bases for Processing Personal Data
- Consent under the GDPR
- Controller vs. Processor and Contract Requirements
- Bases for Transferring Personal Data
- Bottom Lines

AGENDA

- **Introduction and Jurisdictional Scope**
- Bases for Processing Personal Data
- Consent under the GDPR
- Controller vs. Processor and Consent Requirements
- Bases for Transferring Personal Data
- Bottom Lines

Map of EEA Member States

EEA Members

EEA Member

Provisional EEA Member

European Free Trade Association ("EFTA") Members

EFTA Member

EFTA Signatory, But Has Not Ratified

Introduction and Jurisdictional Scope

- Prior to the GDPR, the 1995 EU Data Protection Directive was in effect. (Directive 95/46/EC) (the "**Directive**").
- The Directive and GDPR apply in the 28 member states of the EU and the three additional countries (Iceland, Liechtenstein and Norway) that together with the EU make up the EEA.
  - The United Kingdom is preparing for GDPR implementation despite "Brexit."
- Typically, **the Directive had applied to U.S.-based companies only in those scenarios in which the company was "established in" the EEA**.
  - A company could be deemed to be "established in" the EEA by virtue of:
    - Operating a subsidiary or campus in the EEA; or
    - Operating an office in the EEA.

Introduction and Jurisdictional Scope

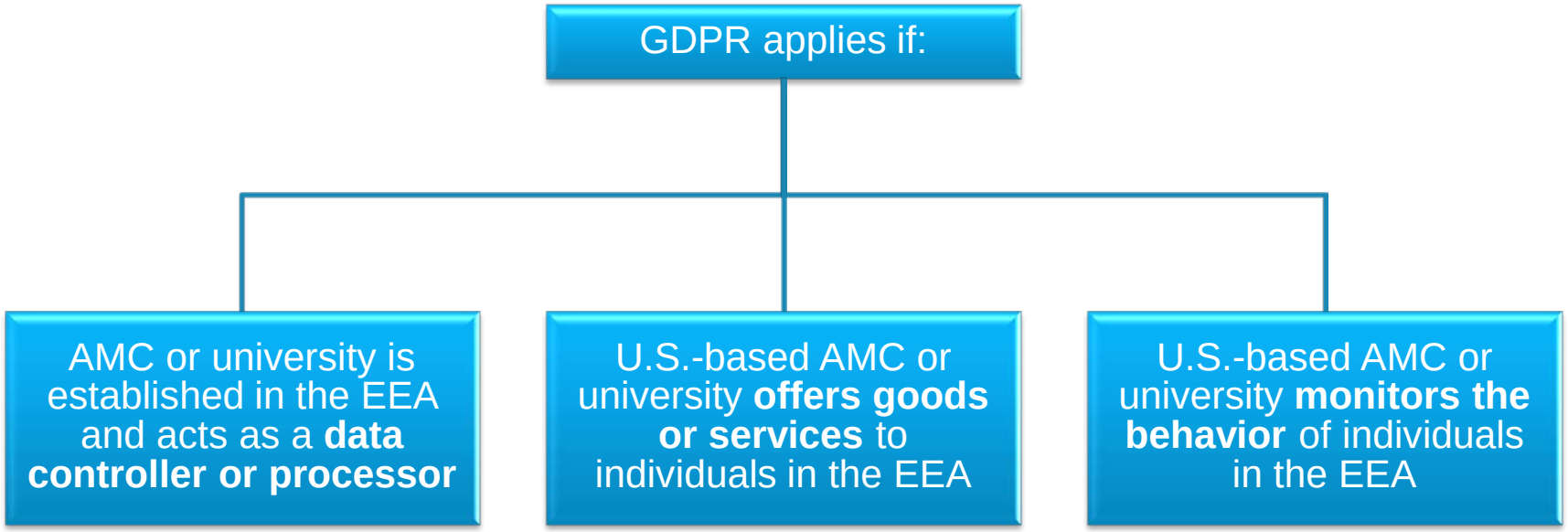
- Effective May 25, 2018, the European Union's General Data Protection Regulation (the "**GDPR**") has implemented a number of changes to privacy law in the European Economic Area ("**EEA**").

Introduction and Jurisdictional Scope

- GDPR also applies to the processing of personal data of data subjects by a controller or processor not established in the EEA, when processing activities are related to:
  - Offering of goods or services, irrespective of whether payment of the data subject is required, to such data subjects in the EEA, or
  - Monitoring of data subjects' behavior as far as their behavior takes place within the EEA.

  See GDPR, Art. 3(2).

GDPR Application to U.S.-Based Universities and AMCs



Offering Goods or Services

- GDPR provides that, "[i]n order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor **envisages offering services to data subjects** in one or more Member States in the Union." GDPR, Recital 23.
  - GDPR notes that the goods or services offered should be considered "**irrespective of whether connected to payment**." GDPR, Recital 23.
- Little guidance has been offered on the meaning of "offering goods or services" to persons located in the EEA.

Offering Goods or Services

- GDPR clarifies that "**mere accessibility of the controller's, processor's or an intermediary's website**" in the EEA is **insufficient to ascertain an intention to offer goods or services in the EEA**. GDPR, Recital 23.
  - GDPR jurisdiction therefore requires that a website be somehow **directed to EEA data subjects**, such as translating the website into an EEA member state language, using an EEA member state currency, or mentioning customers or users in the EEA. *See* GDPR, Recital 23.

U.S. Organizations Offering Goods or Services

- Arrangements in which a U.S.-based entity may be determined to "envisage" offering services to EEA data subjects:
  - Clinical Trial Agreement between U.S.-based sponsor and an EEA study site;
  - U.S.-based sponsor's translation of informed consent documents, FAQs and its webpage into one or more EEA languages.
  - U.S.-based sponsor provides investigational product to an EEA study site as part of a multi-site clinical trial;
  - U.S.-based entity provides mobile application to EEA residents for collection of research data; or
  - Collaboration agreements with universities in EEA member states to develop educational platforms and share data.

U.S. Organizations Offering Goods or Services

- Terms of research arrangements involving **European governmental grants or contracts** may require compliance with GDPR.
  - U.S. universities or AMCs may be direct awardees or sub-recipients through EEA institutions of European governmental grants or contracts to perform research services.
  - Data flows with EEA direct grant awardees should be scrutinized to see if they involve offering services to EEA data subjects.

GDPR Recitals on “Monitoring Behavior”

- GDPR’s recitals provide that “[i]n order to determine whether a processing activity can be considered to monitor the behavior of data subjects, it should be ascertained **whether natural persons are tracked on the internet** including potential subsequent use of personal data processing techniques which consist of profiling a natural person, **particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviors and attitudes.**” GDPR, Recital 24.

"Monitoring Behavior" and Clinical Trials/ Human Subjects Research

- Conducting clinical research with **research sites or research subjects located in the EEA** could involve activities that may constitute ''monitoring of the behavior of data subjects.''
  - **Multi-Site Research**: A U.S.-based sponsor, or a U.S. university or AMC that serves as a lead site, of a clinical trial with sites located in the EEA **could be seen as monitoring the behavior of data subjects** in the EEA, for example, by reviewing data regarding subjects' adherence to trial requirements or monitoring data collection and adverse events.
  - **Mobile Application Research**: Mobile applications (or "**apps**") may be used by a site that enrolls subjects in a study remotely, with the app collecting data on subjects' physical condition or geographic location through subjects' mobile phones. If such arrangements **transmit data to the study site or to the sponsor or its vendors**, this activity **could be seen as the data recipient's "monitoring behavior"** of data subjects in the EEA.

Regulatory Bodies

- **European Data Protection Supervisor** – EU-level independent data protection authority that advises EU institutions on legislation and policies that may affect privacy, intervenes before the Court of Justice of the EU regarding interpretations of data protection law, and cooperates with Member States' data protection authorities to improve consistency in application of data protection law.
- **Article 29 Working Party** – EU body that issued non-binding guidance on EU data protection law. Upon the May 25, 2018 implementation of the GDPR, replaced by the European Data Protection Board.
- **European Data Protection Board** – EU body that will issue guidelines on the interpretation of core data protection concepts and will issue binding decisions on disputes regarding cross-border data processing to ensure uniform GDPR application.

Regulatory Bodies

- **Supervisory Authorities/Data Protection Authorities** - the GDPR requires each Member State to "provide for one or more independent public authorities to be responsible for monitoring the application of [the GDPR], in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union." GDPR, Art. 51(1).
  - United Kingdom: Information Commissioner's Office ("ICO")
  - Germany: The Federal Commissioner for Data Protection and Freedom of Information ("BfDI")
  - France: National Commission of Informatics and Liberties ("CNIL")

“Personal Data” under the GDPR

- “Personal data” are defined broadly to include:
  - “**[A]ny information relating to an identified or identifiable natural person** (“data subject”).” GDPR, Art. 4(1).
- “An identifiable person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, **genetic**, mental, economic, cultural, or **social identity** of that person.” GDPR, Art. 4(1).

“Personal Data” under the GDPR

- Set of data to which GDPR applies is broader than that covered under the Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”).
  - Applies to **all “personal data” across all sectors** of the economy, not only health care; no concept of “covered entity.”
  - Personal data under GDPR include, for example, identifying information on EEA health care providers (“**HCPs**”), such as principal investigators, and other persons who are not patients.

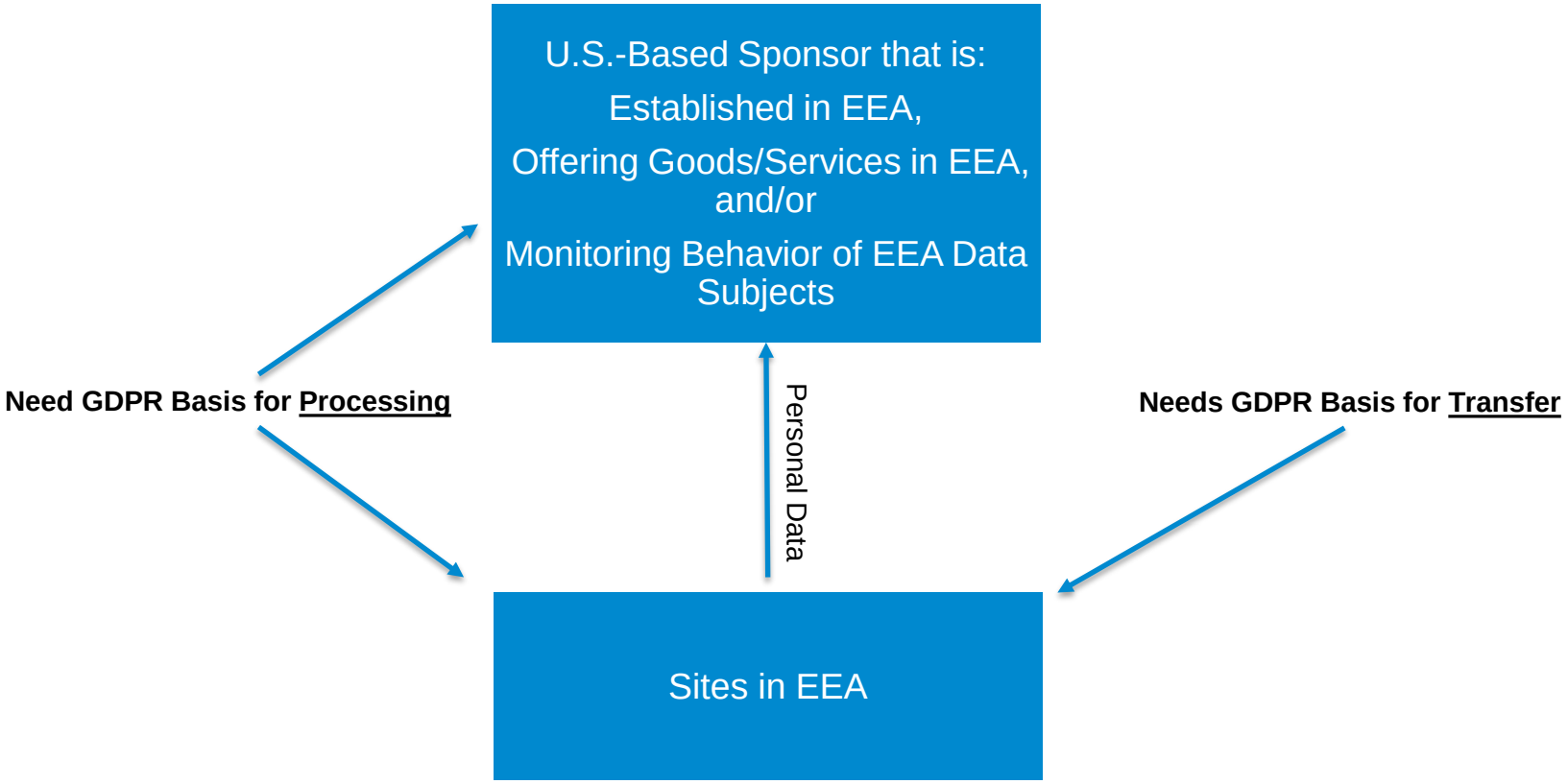
“Personal Data” under the GDPR

- Under GDPR, **no anonymisation “safe harbor”** akin to HIPAA removal of identifiers.
  - Whether data are anonymized such that they are no longer identifiable is judged on a **facts and circumstances test**, taking into account “all the means reasonably likely to be used . . . [e]ither by the controller **or by another person** to identify the natural person directly or indirectly.” GDPR, Recital 26.
- **“Pseudonymised” data (*e.g.*, key-coded data) remain “personal data.”**

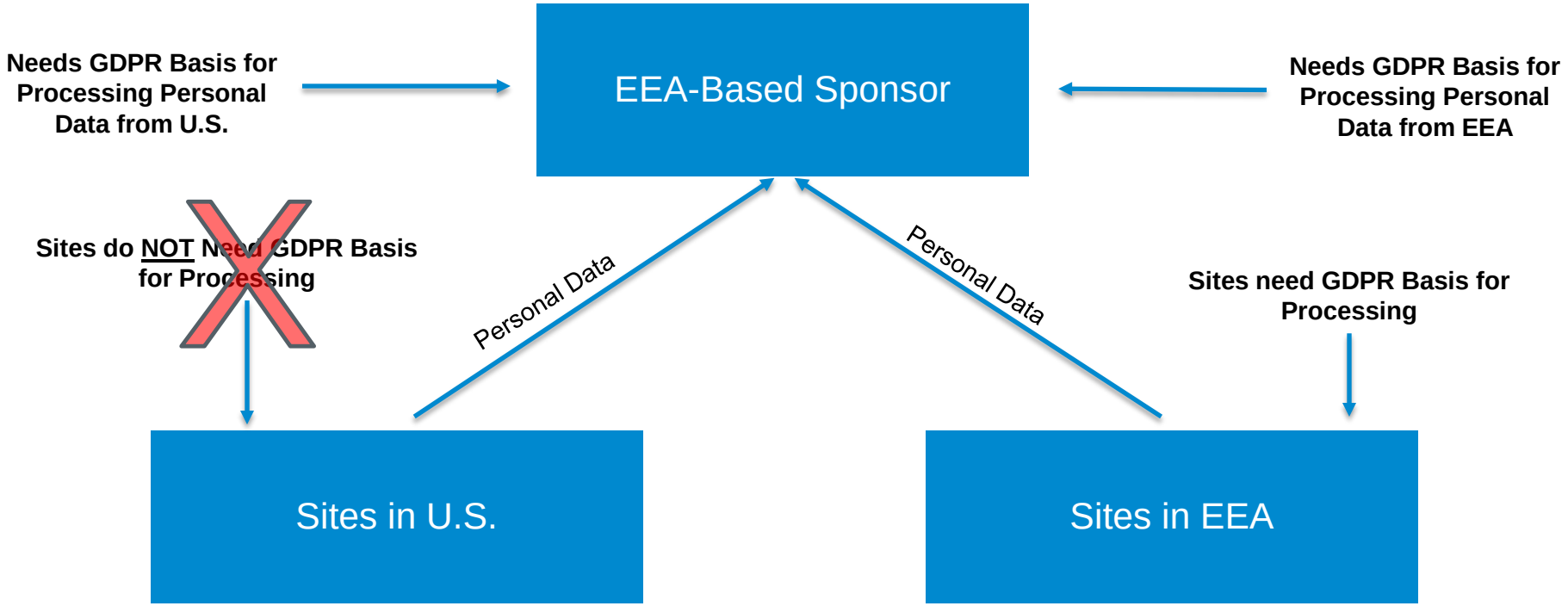
“Special Categories of Personal Data” under the GDPR

- Prohibition on processing “**special categories**” of personal data absent an applicable exception.
- “Special categories” of personal data include:
  - Racial or ethnic origin
  - Data concerning health
  - Data concerning a natural person’s sex life or sexual orientation
  - Genetic data
  - Biometric data used for the purpose of uniquely identifying an individual
  - Political opinions, religious or philosophical beliefs or trade union membership. *See* GDPR, Art. 9.

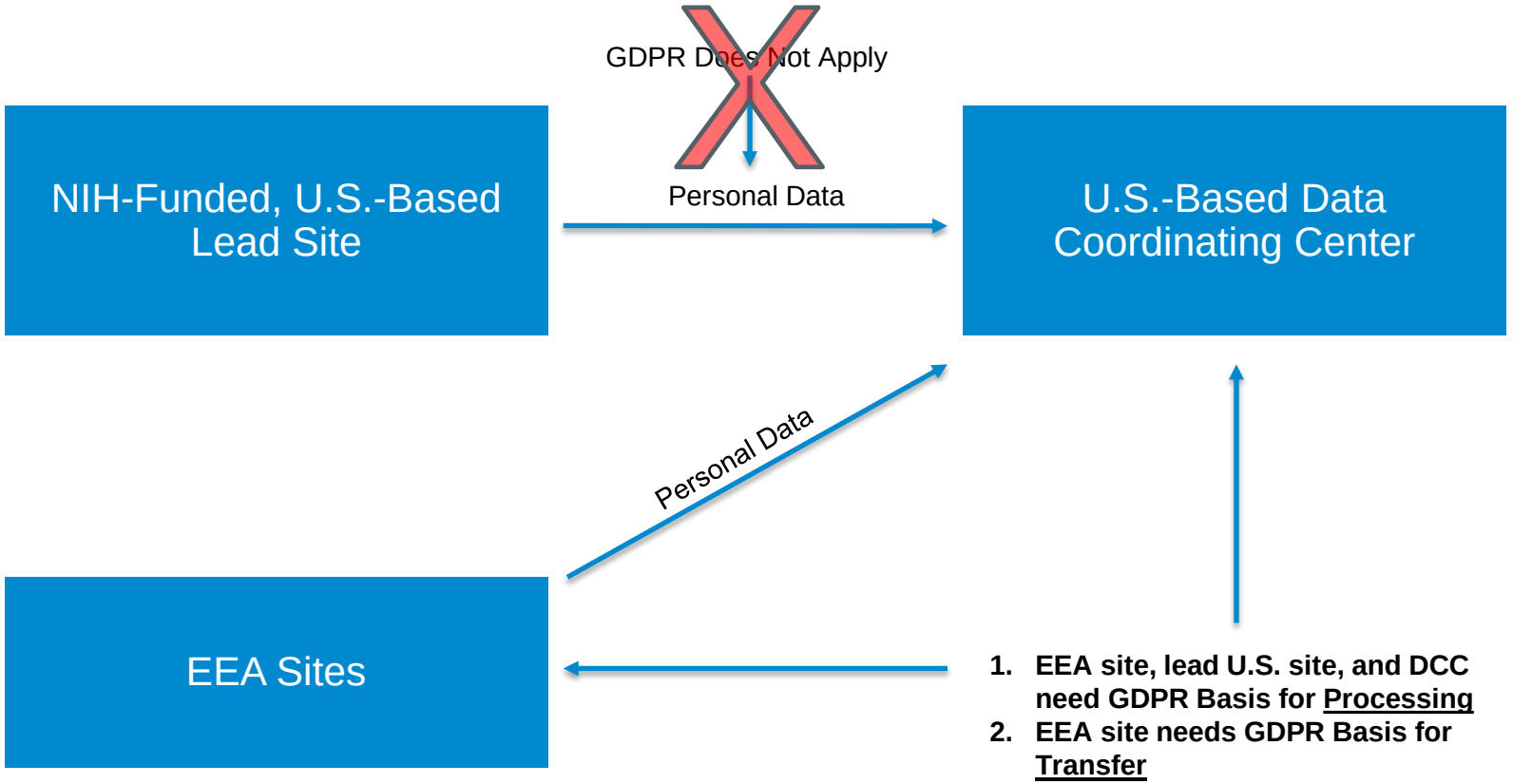
GDPR Application to Sponsor with Sites in EEA



GDPR Application to Multi-Site Trial



NIH-Funded Lead Site in U.S.



AGENDA

- Introduction and Jurisdictional Scope
- **Bases for Processing Personal Data**
- Consent under the GDPR
- Controller vs. Processor and Contract Requirements
- Bases for Transferring Personal Data
- Bottom Lines
- Hypotheticals

Authority for Processing Personal Data

- Processing of personal data that is subject to GDPR **requires a legal basis**.
  - *cf.* HIPAA and need for legal basis to use or disclose PHI.
- Different legal bases are available for processing of regular personal data as opposed to "special categories" of personal data.
- Consent of data subject is basis for processing both regular personal data and special categories of personal data.
- Consent will often prove useful in the research context.

Bases for Processing Personal Data

- Bases for processing personal data include:
  - Data subject has given **consent** to processing.
  - Processing necessary for the **performance of a contract** to which the data subject is a party.
  - Processing necessary for **compliance with a legal obligation**.
  - Processing necessary to protect **vital interests** of the data subject or a natural person.
  - Processing necessary for a **task carried out in the public interest**.
  - Processing necessary for the **legitimate interests of the controller** or a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject.

    GDPR, Art. 6(1).

Bases for Processing Special Categories of Personal Data

- Bases for processing special categories of personal data include:
  - **Explicit consent**
    - GDPR notes that more restrictive laws of the EU or an individual EEA member state may provide that **the data subject may <u>not</u> lift, even by consent, the general prohibition on processing special categories of personal data**. *See* GDPR Art. 9(2)(a). Thus, disparities could emerge across EEA member states.
    - The Article 29 Data Protection Working Party (the "**Working Party**"), a body that provides non-binding guidance on EU data protection law, has advised that "'explicit consent' is understood as having the same meaning as **express consent**" and that "[u]sually, **explicit or express consent is given in writing with a hand-written signature**." Opinion No. 15/2011 (WP197) of the Article 29 Data Protection Working Party.

Bases for Processing Special Categories of Personal Data

(continued)

- Necessary for **scientific or historical research** purposes
  - However, GDPR provides that EEA member states should provide for appropriate safeguards for the processing of personal data for research purposes, which could lead to disparate requirements across EEA member states.
  - Unclear if member states must take affirmative action to permit reliance on this basis.
- **Public interest** in the area of public health
  - Most directly relates to processing by health professionals to protect public health in the event of epidemics or pandemics, or reporting of adverse events by life sciences companies to regulatory authorities.
  - It is not clear that the life sciences community could/should rely on this basis without a direct link between the research and public health.

See GDPR Art. 9(2).

AGENDA

- Introduction and Jurisdictional Scope
- Bases for Processing Personal Data
- **Consent under the GDPR**
- Controller vs. Processor and Contract Requirements
- Bases for Transferring Personal Data
- Bottom Lines
- Hypotheticals

Consent

- GDPR recognizes that consent will already be required for scientific research under parallel EU regulatory regimes.
  - "The processing of personal data for scientific research purposes should also comply with other relevant legislation such as on clinical trials." GDPR, Recital 156.
  - "For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council should apply." GDPR, Recital 161.

Consent to Future Uses of Personal Data

- GDPR text addresses processing personal data for future uses:
  - GDPR provides that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; **further processing for** archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), **not be considered to be incompatible with the initial purposes** ('purpose limitation')." GDPR, Art. 5(1)(b).
  - "**It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research**. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose." GDPR, Recital 33.

Future Uses of Personal Data

- Also relevant to future research, the GDPR permits the processing of personal data (***but not special categories of personal data***) on the basis of the controller or a third party's "legitimate interests," that is if:
  - "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." GDPR, Art. 6(1)(f).

Working Party Guidance on Consent

- However, Working Party guidance appears to provide more limited advice regarding consent to future research uses.
- On December 12, 2017, the Working Party issued draft guidelines on consent under GDPR, with final guidelines issued on April 16, 2018.
  - Final guidelines retain many of the provisions that made the draft guidelines problematic.
- The guidance highlights several key consent principles:
  - Consent has four elements:
    - Freely given
    - Specific
    - Informed
    - Unambiguous indication by a statement or a clear affirmative action
  - Consent should be as easy to withdraw as to give.

Working Party Guidance on Consent

- **Breadth of Consent (continued)**
  - Special categories of data will be subject to a stricter interpretation of Recital 33 and require a high degree of scrutiny.
  - Obtain additional consent as research advances and more details are known about future research activities.
  - If details of research are not known with specificity at outset, updates regarding details of the research should be provided to subjects as the information becomes known so that subject can determine whether to exercise right to withdraw.
  - Suggests making available a “comprehensive research plan” to subjects at the outset of the research.

Working Party Guidance on Consent

- Withdrawal of Consent
  - Guidance recognizes that "**withdrawal of consent could undermine types of scientific research** that require data that can be linked to individuals."
  - Nonetheless, guidance continues as follows:
    - "[T]he GDPR is clear that consent can be withdrawn and controllers must act upon this – there is **no exemption to this requirement for scientific research**. If a controller receives a withdrawal request, it must in principle **delete the personal data straight away** if it wishes to continue to use the data for the purposes of the research."

Working Party Guidance on Consent

- Possible reconciliation of withdrawal of consent and legal requirements to maintain data:
  - "Controllers have an obligation to delete data that was processed on the basis of consent once that consent is withdrawn, **assuming that there is no other purpose justifying the continued retention. . . . In that case, the other purpose justifying the processing must have its own separate legal basis**. This does not mean the controller can swap from consent to another lawful basis."
    - "Controllers should therefore be clear from the outset about which purpose applies to each element of data and which lawful basis is being relied upon."
    - Once personal data have been collected for research, maintenance of data to meet adverse event monitoring and trial integrity requirements relies on basis that processing is "necessary for reasons of public interest in the area of public health, such as . . . **ensuring high standards of quality and safety of health care and of medicinal products or medical devices** . . . ."

    See GDPR, Art. 9(i).

Working Party Guidance on Consent

- Working Party notes that, even if the controller relies on another basis to retain data, the **controller must still respect data subjects' requests for erasure**, which is a separate right of data subjects under the GDPR.
  - Requests for erasure under the GDPR are subject to an exception that **permits controllers to retain data for compliance with legal obligations or for scientific research purposes** if deletion would be likely to render impossible or seriously impair the achievement of the objectives of such processing. *See* GDPR, Art. 17(3).

AGENDA

- Introduction and Jurisdictional Scope
- Bases for Processing Personal Data
- Consent under the GDPR
- **Controller vs. Processor and Contract Requirements**
- Bases for Transferring Personal Data
- Bottom Lines
- Hypotheticals

Controller vs. Processor

- Controller
  - Alone or jointly with others determines the **purposes and means** of processing personal data.
- Processor
  - Processes personal data **on behalf of the controller**.
- Both controllers and processors regulated directly under GDPR.
- Controllers have more responsibilities, for example:
  - Providing notices to data subjects, responding to exercise of subject rights, appointing representative in EEA, notifying supervisory authorities and data subjects of data breaches, maintaining records of processing.

Processing Agreement

- GDPR requires that processing by a processor shall be **governed by a contract** or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and **sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller, and that stipulates that the processor:**
  - Processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject…;
  - Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
  - Takes all measures required pursuant to Article 32 (security of personal data);
  - Respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

Vendor Contract Requirements

(continued)

- Taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights…;
- Assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (i.e., security; Data Protection Impact Assessments), taking into account the nature of processing and the information available to the processor;
- At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; and
- Makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

GDPR Article 28(3).

Subprocessor Agreements

- GDPR requires that the processor **shall not engage another processor without prior specific or general written authorisation** of the controller.
- In the case of general written authorisation, the processor **shall inform the controller of any intended changes** concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
- Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, **the same data protection obligations** as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 **shall be imposed on that other processor by way of a contract** or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation.
- Where that other processor fails to fulfil its data protection obligations, the **initial processor shall remain fully liable to the controller** for the performance of that other processor's obligations.

GDPR Art. 28(2) & (4).

AGENDA

- Introduction and Jurisdictional Scope
- Bases for Processing Personal Data
- Consent under the GDPR
- Controller vs. Processor and Contract Requirements
- **Bases for Transferring Personal Data**
- Bottom Lines
- Hypotheticals

Requirements for Transfer of Personal Data to U.S.

- GDPR **requires that a legal basis be in place to permit the transfer of personal data from the EEA to jurisdictions lacking adequate data protection legislation (*e.g.*, the United States)**. *See* Directive Ch. IV; GDPR Ch. V.
- Transfer requirements apply even if GDPR does not apply directly to receiving entity.
- The intent is to ensure that GDPR-level protections are extended to personal data notwithstanding their transfer.

“White Listed” Jurisdictions

- Certain countries have been “white listed” as offering adequate data protection, including:
  - Argentina
  - Canada
  - Israel
  - New Zealand
  - Switzerland
  - Uruguay
  - Andorra, Faeroe Islands, British Crown Dependencies (Guernsey, Jersey, Isle of Man)
  - Post-Brexit United Kingdom?????

Legal Bases for Data Transfer

- Obtaining the **explicit consent** of the data subject to the transfer of personal data to the U.S. for processing.
  - Requires **advising the data subject of the risks** of the transfer resulting from the absence of adequate data protection legislation in the recipient jurisdiction. *See* GDPR, Art. 49(1)(a).
- Entering into **model contractual clauses** approved by the European Commission with the EEA entity transferring personal data.
  - Two sets of controller-controller clauses.
  - One set of controller-processor clauses.
  - No processor-controller clauses.

    See GDPR, Art. 46(2).

Legal Bases for Data Transfer

- Transfer **necessary for performance of a contract between the data subject and the controller**, implementation of pre-contractual measures taken a data subject's request, or contract concluded in the interest of the data subject.
- Transfer necessary for **important reasons of public interest**.
- Transfer necessary for **establishment, exercise or defense of legal claims**.
- Data transfers necessary to protect the "**vital interests**" of the data subject.
  - Generally considered to be "life and death" situations.

    See GDPR, Art. 49(1).

Legal Bases for Data Transfer

- U.S.-based companies that are **for-profit entities** may have an additional option of applying for certification under the **EU-U.S. Privacy Shield**, a program administered by the U.S. Department of Commerce.
  - Permits personal data to be transferred from the EEA to U.S. for-profit entities that self-certify for the program after implementing various data protection measures consistent with EU privacy law.
- Associations may create **codes of conduct** setting forth rules on data processing. Such codes must be approved by the supervisory authority in the relevant EEA jurisdiction or the European Data Protection Board, if operable in multiple jurisdictions.

  See GDPR, Art. 46(2)(e).

AGENDA

- Introduction and Jurisdictional Scope
- Bases for Processing Personal Data
- Consent under the GDPR
- Controller vs. Processor and Contract Requirements
- Bases for Transferring Personal Data
- **Bottom Lines**
- Hypotheticals

Bottom Lines

- Consent as basis for processing data for interventional research
- Legitimate interests and contracts as bases for processing personal data
- Contracts as basis to transfer personal data outside EEA to countries lacking adequate protections
- Research uses to be included in notices of privacy practices
- Anonymization not generally feasible for secondary uses

Bottom Lines

- Controller vs. processor to be identified; processors to be bound by contract if processing personal data as a vendor or subawardee
- Transnational personal data transfers should be identified
- Transfers of personal data from EU to U.S. require a legal basis, such as model clauses
- Use of cookies should be evaluated – the ePrivacy Directive requires consent to cookies, and the Working Party's guidelines on the conditions for consent apply (*i.e.*, should be informed, specific, freely given, and unambiguous). Per Working Party, consent must be opt-in, not opt-out.

AGENDA

- Introduction and Jurisdictional Scope
- Bases for Processing Personal Data
- Consent under the GDPR
- Controller vs. Processor and Contract Requirements
- Bases for Transferring Personal Data
- Bottom Lines
- **Hypotheticals**

Hypothetical 1

- If a clinical trial initiated before May 25, 2018 is ongoing as of and/or after May 25 and the trial relied on the subjects' consent to process their personal data, does the GDPR require that the subjects be reconsented?

Hypothetical 1

- Re-consent is not likely necessary.
- The GDPR permits controllers who consented subjects under the Directive to continue to rely on the consents obtained thereunder. *See* GDPR, Recital 171.
- However, data controllers relying on pre-GDPR consents should ensure that such consents were "in line" with the conditions of the GDPR.
  - For example, any consents for the processing of special categories of personal data must have been "express," typically meaning that the consent is in writing.
  - In the context of clinical trials, express consents to the processing of personal data were usually already being obtained prior to the implementation of the GDPR.

Hypothetical 2

- Is a clinical trial site in the EU considered a processor or joint controller?

Hypothetical 2

- Likely a joint controller, if the EU site, together with the U.S. based entity, determine the purposes and means of processing.
- GDPR provides that "[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers." GDPR, Art. 26(1).
- Joint controllers should "in a transparent manner **determine their respective responsibilities for compliance** with the obligations under" the GDPR "in particular as regards the exercising of the rights of the data subject and their respective duties to provide" notices to the data subject. *See id.*
  - The "essence of the arrangement" must be made available to the data subjects.

Hypothetical 3

- May personal data collected for the standard of care be used secondarily for research purposes? If so, how?

Hypothetical 3

- **Consent** to processing in connection with the research would permit such processing, both as an Article 6 basis for processing and an Article 9 condition for processing special categories of personal information.
- If consent has not been obtained, a basis (Art. 6) and condition (Art. 9) that may permit the processing for research purposes include:
  - **Legitimate Interests (Art. 6)**
    - "Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." GDPR, Art. 6(f).
  - **Scientific Research Purposes (Art. 9)**
    - "Processing is necessary for . . . scientific . . . research purposes . . . in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject." GDPR, Art. 9(2)(j).
    - Article 89(1) requires that safeguards "shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization," particularly pseudonymisation, if the data processing can be completed with pseudonymized data.
- Also, processing for additional purposes must be **compatible with** processing for the initial purposes. The GDPR provides that processing for scientific research purposes "shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes. *See* GDPR, Art. 5(1)(b).

Hypothetical 4

- May data used in a previous study be used for secondary research purposes?

Hypothetical 4

- Likely yes.
- If consent was the basis for processing the data in the prior study, then the consent should be evaluated to determine whether it authorizes the use of the data for the future research in question.
  - As noted, consent may authorize use of personal data for some specified future research projects.
- Also, the processing for the future research must be **compatible** with the purposes of the processing for the initial research. This test presumably can be met:
  - The GDPR provides that processing for scientific research purposes "shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes. See GDPR, Art. 5(1)(b).
  - Could rely on Article 6 basis of legitimate interests and Article 9 condition of scientific research.

Hypothetical 5

- Can personal data be shared among separate entities for research? If so, how?

Hypothetical 5

- Personal data could be shared with other entities to carry out research. Some common reasons for sharing could include:
  - **Processing/analysis by another entity.** For example, a controller might engage a third-party data coordinating center to assist with collecting and analyzing data collected in a study.
    - A controller-processor agreement should be entered.
  - **Research collaborators.** A consortium could sponsor a clinical trial, with each consortium member receiving the data.
    - The consortium members would likely be joint controllers, in which case a joint controller side letter, or similar agreement, should be entered.
  - **Researchers engaged in additional research.** The data controller might wish to share the collected data with other researchers to conduct their own, separate research.
    - The additional research would need to be compatible with the purposes of the initial research. *See* GDPR, Art. 5(1)(b).
    - The additional research would need a basis for processing personal data and a condition for processing special categories of personal data. These could be, respectively, legitimate interests (GDPR, Art. 6(1)(f)) and scientific research (GDPR, Art. 9(2)(j)).

Hypothetical 6

- How may the GDPR affect biospecimen banking and research?

Hypothetical 6

- On its face, the GDPR's Recital 33 is best read to permit researchers to obtain a general consent for future processing in connection with "areas of scientific research."
- However, guidance would limit the ability of the research community to collect biospecimens for biobanks that can be accessed for future research purposes when those purposes are not known at the time of initial collection.
  - Phenotypic data associated with biospecimens are likely "personal data" under the GDPR.
    - Further, key-coded (pseudonymized) data remain personal data under the GDPR.
- Working Party guidance proposes "rolling consent" process as the research advances.
  - This would impose a burden on researchers continually, and perhaps frequently, to re-contact research subjects to obtain additional consent.
  - Biobanks may lose contact with data subjects in multi-year studies, making re-contact and additional consent impossible.