Title: European Union General Data Protection Regulation
Date of Last Revision: 07/25/18
Audience: Researchers

Background

Data protection in Europe has been in existence for over 20 years (1995 European Union Data Protection Directive). The basic premise of the EU Data Protection Directive was to safeguard the fundamental rights of the individual - to protect the privacy, and to provide protection, of all personal data collected for or about citizens in the European Union (EU), with regard to processing, using, or exchanging such data. The EU Data Protection Directive was based on seven principles:

- Subjects whose data is being collected should be given notice of such collection
- Subjects whose personal data is being collected should be informed as to the party or parties collecting such data
- Once collected, personal data should be kept safe and secure from potential abuse, theft, or loss
- Personal data should not be disclosed or shared with third parties without consent from its subject(s)
- Subjects should be granted access to their personal data and allowed to correct any inaccuracies
- Data collected should be used only for stated purpose(s) and for no other purposes
- Subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles

European Union General Data Protection Regulation

The 1995 EU Data Protection Directive was replaced with the European Union General Data Protection Regulation (EU GDPR), which became effective on May 25, 2018.

The EU GDPR updates and harmonizes data privacy laws across the EU, and establishes protections for the privacy and security of personal data about individuals in the EU single market countries. The EU single market countries [European Economic Area (EEA)] include: the EU member states, Norway, Iceland, Liechtenstein and Switzerland. This regulation potentially affects clinical and scientific research activities if the research involves personal data about individuals located in those countries regardless of the individuals' citizenship status in the countries.

The EU GDPR:

- Defines the circumstances under which it is lawful to collect, use, disclose, destroy, and process personal data
- Specifies certain (data) rights of individuals in the EU, including rights to access, amendment, and erasure
- Requires that personal data controllers and processors implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk to personal data
- Requires notification to data protection authorities and affected individuals following the discovery of a personal data breach

Applicability to Human Subjects Research Activities

<table>
<thead>
<tr>
<th>Scope of the EU GDPR</th>
<th>Jurisdiction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The regulation has direct extraterritorial reach to a controller or processor organization located in the United States if the organization:</td>
<td></td>
</tr>
<tr>
<td>1) Creates an establishment in the EU:</td>
<td></td>
</tr>
<tr>
<td>a) Operating an office or a subsidiary</td>
<td></td>
</tr>
<tr>
<td>b) Sponsoring clinical research occurring in the EEA</td>
<td></td>
</tr>
</tbody>
</table>
c) Acting as a core data facility or lead site for a multi-national clinical trial with EEA-based sites
d) Conducting clinical trials in which participant data are transmitted to sponsors, servers, or data core facilities based in the EEA

2) **Offers goods or services (including free offers of goods or services) to individuals in the EU:**
   a) Includes recruitment of individuals in the EU to participate in a research study
   b) Must establish whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union (Recital 23);
      examples include:
      i) CTA between US-based sponsor and EEA study site
      ii) US-based sponsor's translation of consent documents, FAQs, and its webpage into one or more EEA languages
      iii) US-based sponsor's provision of investigational product to an EEA study site as part of a multi-site clinical trial
      iv) US-based entity's provision of a mobile application to EEA residents for collection of research data
      v) Collaboration agreements with universities in EEA member states to develop educational platforms and share data
   c) Terms of research agreements involving European governmental grants or contracts may require compliance with the regulation
      i) US universities or academic medical centers may be direct awardees or sub-recipients through EEA institutions of European governmental grants or contracts to perform research services
         (1) Data flows with EEA direct grant awardees should be scrutinized to see if they involve offering services to EEA data subjects
   d) Must ascertain whether the offer of goods or services is **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)

3) **Monitors the behavior of individuals in the EU (Recital 24)** - examples include:
   a) Monitoring patients after they return to the EU as part of post-discharge care
   b) Monitoring of behavior includes tracking individuals on the internet by techniques that apply a profile to enable decisions to be made, or predict personal preferences, behaviors, attitudes, etc
   c) US-based sponsor (or university or academic medical center) that serves as a lead site, of a clinical trial with sites located in the EEA that reviews data regarding subjects’ adherence to trial requirements or monitoring data collection and adverse events
   d) Transmission of data to the study site or to the sponsor or its vendors when mobile applications are 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
      i) Includes US-based clinical research subjects during the period of travelling to the EEA, including for vacation or work

Article 24
Article 29 Working Party

4) **Transfer of personal data from a European Economic Area (EEA) country, to the US (outside of the EEA)**

5) **Has a contractual relationship with research vendors or other third parties who are subject to the regulation**
<table>
<thead>
<tr>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Personal Data:</td>
</tr>
<tr>
<td>a) any information relating to an identified or identifiable natural person who is in the EU, regardless of the individual’s EU citizenship status</td>
</tr>
<tr>
<td>i) EU citizens who obtain employment and reside in the US are generally not covered by the regulation</td>
</tr>
<tr>
<td>ii) US citizens who work at an EU branch of the US entity and reside in the EU are generally covered by the regulation</td>
</tr>
<tr>
<td>b) an individual is identified or identifiable if the individual can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person</td>
</tr>
<tr>
<td>c) includes identifying information on EEA healthcare providers, such as principal investigators, and other persons who are not patients, such as those conducting the study</td>
</tr>
<tr>
<td>d) includes key-coded data</td>
</tr>
<tr>
<td>e) regulation does not apply to decedent data (the regulation applies only to living individuals)</td>
</tr>
<tr>
<td>f) there is no specific list of what is “identifiable” [would require a facts and circumstances test (Recital 26)]</td>
</tr>
<tr>
<td>g) special categories of personal data requires explicit consent:</td>
</tr>
<tr>
<td>i) racial/ethnic origin</td>
</tr>
<tr>
<td>ii) data concerning health</td>
</tr>
<tr>
<td>iii) data concerning a natural person’s sex life or sexual orientation</td>
</tr>
<tr>
<td>iv) genetic data</td>
</tr>
<tr>
<td>v) biometric data used for the purpose of uniquely identifying an individual</td>
</tr>
<tr>
<td>vi) political opinions, religious or philosophical beliefs, trade union membership</td>
</tr>
<tr>
<td>2) Processing:</td>
</tr>
<tr>
<td>a) any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction</td>
</tr>
<tr>
<td>3) Data Controller:</td>
</tr>
<tr>
<td>a) a 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</td>
</tr>
<tr>
<td>i) an organization would take on a controller role if it participates in the design, direction or control of the research study (i.e., as a sponsor, lead researcher or primary research site) or directly recruits research subjects in the EU</td>
</tr>
<tr>
<td>ii) responsibilities include providing notices to data subjects, responding to exercise of subject rights, appointing representative in the EEA, notifying supervisory authorities and data subjects of data breaches, maintaining records of processing</td>
</tr>
<tr>
<td>4) Data Processor:</td>
</tr>
<tr>
<td>a) a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller</td>
</tr>
</tbody>
</table>
i) an organization will take on a processor role if it collects and/or processes personal data only on behalf of and at the direction of the controller (i.e., as a clinical research organization)

Other definitions

5) Biometric data:
   a) personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data

6) Data concerning health:
   a) personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status

7) Genetic data:
   a) personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

8) Pseudonymisation:
   a) 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

Impact on Human Subjects Research Activities

Processing of Personal Data

1) Processing of personal data requires a legal basis:
   a) Consent has been provided
   b) Necessary for the performance of a contract to which the data subject is a party
   c) Necessary for compliance with a legal obligation
   d) Necessary to protect vital interests of the data subject or a natural person
   e) Necessary for a task carried out in the public interest
   f) 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

2) Conditions for processing special categories of personal data:
   a) Requires explicit consent
   b) Necessary for scientific or historical research purposes
   c) Necessary for the public interest
   d) Necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent

University of California - Research under the EU GDPR

1) Scientific research (including registry studies) as defined by HIPAA and the US DHHS Common Rule
2) **Historical research** performed for genealogical purposes

3) **Statistical research**, in which statistical results may be used further for different purposes, including scientific research purposes

4) **Archiving purposes in the public interest**, in which public authorities (or, public or private bodies) that hold records of public interests and pursuant to the EU or a Member State Law, have a legal obligation to acquire, preserve, appraise, describe, communicate, promote, disseminate and provide access to records of ensuring value for general public interest

5) **Secondary Research**:  
   a. Obtain the consent of the data subject to conduct secondary research using his/her personal data (and explicit consent to use special categories of personal data for secondary research)  
   b. Document the compatibility of the secondary purpose with the initial purpose, where possible  
      i. Considerations:  
         1. Any link between those first purposes and the purposes of the intended further processing  
         2. The context in which the personal data was collected, and in particular, the reasonable expectations of data subjects based upon their relationship with the controller as to their further use  
         3. The nature of the personal data (i.e., types of personal data being processed)  
         4. The consequences of the intended further processing for data subjects (i.e., how the secondary use would impact the individual)  
         5. The existence of appropriate safeguards in both the original and intended further processing operations  
   c. Consent to Secondary Research:  
      i. Researchers should allow data subjects to explicitly consent to categories of secondary research uses, with each separate consent identifying:  
         1. Whether the specific consent covers the storage or sharing of personal data for the future research  
         2. The specific categories of research covered by the specific secondary research consent  
         3. The type(s) of researcher or research institution who may conduct the secondary research or have access to the personal data  
         4. Whether the personal data available for the secondary research use will be identifiable on its own, identifiable through the use of specimens, or identifiable by other means

*not explicitly defined in the EU GDPR*

Non-EU data controllers and processors need to appoint an EU representative (**Article 27**)

---

**Transferring Personal Data from the EEA to the US**

1) Transferring of personal data requires a **legal basis**:  
   a) Obtaining an **explicit consent** and **advising the data subject of the risks** associated with the transfer  
   b) Entering into a **model contractual clauses** approved by the European Commission with the EEA entity transferring the personal data  
      i) The underlying agreements should disclose the University of California’s obligations to comply with federal and state laws, including but not limited to public disclosure
laws (i.e., California Public Records Act) and requirements to comply with federal and state regulatory authorities (i.e., FDA); requests for exceptions to the Standing Order 100.4(dd)(9) are not required

c) Necessary for **performance of a contract between the data subject and the controller**
   i) Implementation of pre-contractual measures taken at the subject's request, or contract concluded in the interest of the data subject

d) Necessary for **important reasons of public interest**

e) Necessary for **establishment, exercise, or defense of legal claims**

f) Necessary to protect the **vital interests** of the data subject (life and death situations)

g) **Binding Corporate rules**
   i) Allow multi-national corporations to make intracompany transfers of personal data
   ii) May be used to transfer data from one subsidiary to another
   iii) Must be approved by cognizant data protection authority

**Model contracts for the transfer of personal data to third countries**
- 2001 Standard Controller-to-Controller Contract
- 2004 Standard Controller-to-Controller Contract
- Standard Controller-to-Processor Contract

**Personal Data Transferred from US to EEA**

1) A US-based entity may need to transfer its employees' data to the EEA if the entity is serving as a clinical trial site for an EEA-based clinical research sponsor (EEA-based pharma company or academic medical center)
   a. The EEA-based research sponsor may request that the US entity's employees sign a consent form to allow processing of their data in the EEA
   b. The EEA-based research sponsor may need to provide a notice regarding data processing activities to the US entity's employees whose data are being transferred to EEA sponsor

2) A US-based entity may need to transfer clinical trial data of research subjects to the EEA when the trial is sponsored by an EEA-based entity or EEA-based entity serves as the lead site
   a. The EEA-based sponsor may need the US entity to obtain trial subjects' consent that meets the notice requirements of the EU GDPR and allows processing of their data in the EEA
      i. Consent will need to include the following information:
         1. Their personal data will be transferred to the EEA for analysis
         2. The identity of the data controller/Data Protection Officer
         3. The contact information for data subject to file complaints with applicable data protection authority

**Controller-Processor Agreement Requirements**

Processing by a processor shall be **governed by a contract** or other legal act under the Union or a 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 the personal data and categories of data subjects and the obligations and rights of the controller, and that stipulates that the processor**:

1) 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 organization,
un}less required to do so by the Union or a Member State Law to which the processor is subject to

2) Ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality

3) Takes all measures in the security of personal data (pursuant to Article 32)

4) Respects the conditions for engaging another processor (paragraphs 2 and 4)

5) Taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights

6) Assists the controller in ensuring compliance with the obligations to perform Data Protection Impact Assessments, taking into account the nature of processing and the information available to the processor

7) 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 the Union or a Member State Law requires storage of the personal data

8) Makes available to the controller all information necessary to demonstrate compliance with the obligations specified in the regulation 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.

Sub-processor Agreement

1) The processor shall not engage another processor without prior specific or general written authorization of the controller

2) In the case of general written authorization, 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

3) Where the 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 (paragraph 3) shall be imposed on that other processor by way of contract or other legal act under the Union or Member State Law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this regulation

4) Where that other processor fails to fulfill its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor’s obligations

For existing studies

1) If the sponsor and its research sites determine that they are joint controllers together determine the purposes and means of processing the personal data, then they should enter into an additional agreement delineating their respective responsibilities with regard to processing and the exercise of the data subjects’ rights.
2) Alternatively, if the sponsor is the controller and research sites (or other entities such as data coordinating centers) are processors, then the sponsor should enter into controller-processor agreements with the sites.

Agreements should set 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 bind the processor to certain conditions specified by the regulation.

Articles 28 and 32

Informed Consent

1) Requires 4 elements:
   a) Freely given
      i) Considerations:
         (1) Power imbalance
            (a) For consent to be valid when there is an imbalance of power, the data subject must be able to exercise a real choice with no risk of deception, intimidation, coercion, or significant negative consequences if consent is not provided
         (2) Conditionality
            (a) Consent, when tied to the provision of a contract or service, is not freely given; two lawful bases of processing (consent and contract) cannot be merged and blurred such that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract
         (3) Granularity
            (a) Consent should only address a single, specific purpose of processing; if there is more than one purpose of processing, a separate consent is required for each individual purpose of processing
         (4) Detriment
            (a) The controller must be able to demonstrate that it is possible for a data subject to refuse or withdraw consent without detriment (i.e., deception, intimidation, coercion, significant negative consequences) if a data subject withdraws consent
   b) Specific
      i) Considerations:
         (1) Data subjects must give consent to each specific processing purpose
         (2) A controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow individuals to give specific consent for specific purposes
         (3) Controllers should provide specific information with each separate consent request about the data processed for each purpose in order to make data subjects aware of the impact of their choices
      ii) Other consideration: Data transparency policies that conflict with data subjects’ rights (i.e., withdrawal of consent) under the EU GDPR
          (1) EMA Policy 0070
          (2) 2018 ICMJE Policy
          (3) EU GDPR Article 9
   c) Informed
      i) Must include:
         (1) Controller’s identity
         (2) Purpose(s) of each of the processing operations for which consent is sought
(3) The types of personal data to be collected and used
(4) The existence of the right to withdraw consent
(5) Information about the use of the data for decisions based solely on automated processing, including profiling
(6) If the consent relates to data transfers, about the possible risks of data transfers to countries outside of the EEA in the absence of an adequacy decision and appropriate safeguards

d) **Unambiguous indication** by a statement or a clear affirmative action
   i) Written consent ([Article 4(11)](#))
   ii) Electronic consent ([Recital 32](#))
   iii) Verbal consent should be recorded and the controller should document the information that was made available to the data subject about the processing prior to consent

2) **Breadth of consent:**
   a) Data subjects should be allowed to give their consent to certain areas of scientific research
   b) Obtain additional consent as research advances and more details are known about future research activities
   c) If details of research at not known with specificity at outset, updates regarding details of the research should be provided to subjects as the information becomes known so that subjects can determine whether to exercise their right to withdraw

3) **Withdrawal of consent:**
   a) Requests for erasure 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
      i) 

4) **Duration: how long a consent is valid, and how long data is maintained**
   a) Depends on the context, the scope of the original consent, and the expectations of the data subject and should be refreshed at appropriate intervals
   b) No time limit, however if it is not possible to state a specific period, must describe the criteria used to determine that period

5) **Re-consent of subjects in ongoing research:**
   a) It is not necessary for the data subject to give his/her consent again if the manner in which the consent has been given is congruent with the conditions of the regulation
      i) If notice requirements from [Articles 13 and 14](#) is not described in the existing consent, it can be provided in a separate privacy notice

6) **If applicable, additional content:**
   a) Identity and contact details of the controller
   b) Terms and conditions and procedure for withdrawal from research
   c) Whether data will be pseudonymized and who to contact when exercising Right of Access
   d) Conditions and protections for the transfer of data from the EU to the US

[Article 7](#)
[Key Issues - Consent](#)
[Article 29 Working Party](#)

**Contents of the Required Privacy Notice**
Notice is to be provided at the time personal data are collected

1) Identity and **contact details** of the data controller, and where applicable, of data controller’s representative
2) Contact details of **data protection officer**, where applicable
3) **Purposes of processing** for which the personal data are intended and legal basis for processing
4) The **legitimate interests pursued** by the data controller or third party (if legal basis relied upon is legitimate interests)
5) Recipients or **categories of recipients** of the personal data, if any
6) Where the personal data was not obtained from the data subject, the **source from which the personal data originated**, and if applicable, whether it came from publicly accessible sources
7) Where applicable, information about international **data transfer**, and reference to appropriate or suitable **safeguards**, and the means by which to obtain a copy of them or where they have been made available
8) The **period for which the personal data will be stored**, or if that is not possible, the criteria used to determine that period
9) The existence of **automated decision-making**, including, profiling, where applicable, and meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject

**Articles 12-14**

<table>
<thead>
<tr>
<th>Data Subject Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1) Right of Access:</strong></td>
</tr>
<tr>
<td>a) Obtain confirmation of and information about processing, as well as access to data processed</td>
</tr>
<tr>
<td>b) <strong>All</strong> personal data about subject regardless of how collected</td>
</tr>
<tr>
<td>c) Obtain additional information in an accounting of disclosures, including the source of the personal data if the source is not the data subject himself/herself <em>(Article 15, 45 CFR 164.528)</em></td>
</tr>
<tr>
<td>d) Exceptions:</td>
</tr>
<tr>
<td>i) Cannot adversely affect rights and freedoms of others</td>
</tr>
<tr>
<td>ii) If there is a large of amount of data, ask the data subject to specify a subset</td>
</tr>
<tr>
<td>e) Note: when a US sponsor is performing whole genome sequencing (WGS) as part of the research, the results cannot be released if the WGS was performed by a non-CLIA lab; if the EU GDPR is applicable to the research, there is a potential obligation to release the WGS results</td>
</tr>
<tr>
<td><strong>2) Right to Rectification:</strong></td>
</tr>
<tr>
<td>a) Amend (all) personal data if it is inaccurate or incomplete</td>
</tr>
<tr>
<td>b) Exception:</td>
</tr>
<tr>
<td>i) Controller may keep earlier collected data if required for legitimate purpose, provided that subjects are informed of this</td>
</tr>
<tr>
<td><strong>3) Right to Erasure:</strong></td>
</tr>
</tbody>
</table>
| a) Have personal data deleted or removed, if:
i) Personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
ii) Data subject withdraws consent on which the processing is based
iii) Data subject objects to processing that was based on legitimate interest of the controller and the controller cannot demonstrate compelling legitimate grounds for the processing
iv) Personal data have been unlawfully processed
v) Personal data have to be erased for compliance with a legal obligation in the EU or a member state law to which the controller is subject to

b) Includes all personal data held by controller
c) If data has been published or made public, controller must use best efforts to contact third parties to inform them of the erasure request
d) Exceptions:
   i) Exercising the right of freedom of expression
   ii) Compliance with legal obligations that require processing by the EU or a member state law
   iii) Reasons of public interest in the area of public health
   iv) Scientific or historical research purposes if erasure is likely to render impossible or seriously impair the achievement of the research
      (1) Inform data subjects at the time notice of processing is given, that personal data will be processed for the conduct of research, as well as to meet US legal obligations, using the “legitimate interest” of the University of California as the lawful basis for compliance with US law
   v) Establishment, exercise, or defense of legal claims

4) Data Portability:
a) Where the processing is based upon consent or pursuant to a contract with the data subject, and the processing is automated, data subjects have a right to receive the personal data which they have provided to the controller in a commonly-used and machine readable format, as well as the right to have that data transmitted to another controller (the University of California would be required to transfer personal data to another researcher upon the data subject's request where the University of California relies upon consent to conduct research using personal data)

5) Objection / Withdrawal:
a) Controllers must act upon a data subject's withdrawal of consent and either delete or anonymize the personal data if it wishes to continue to use the data for the research purpose

6) Required Privacy Notice:
a) Notice is not required where a source other than the data subject provides the personal data to the controller, and providing notice would be impossible or involve a disproportionate effort, particularly where the data is being used for research purposes. (This exemption does not apply where the data subject has provided the information.)
b) Where the personal data has not been provided by the data subject it concerns, the regulation exempts the notice where the personal data must remain confidential due to an obligation of professional secrecy regulated by the EU or a Member State Law (i.e., a patient informs a doctor of the medical history of his/her relative for the patient's own care; the regulation exempts notice to the relatives -- if the physician were to provide this information to the relatives, the obligation of professional secrecy, which the physician owes the patient, would be violated).
7) Automated Processing:

a) The regulation gives data subjects the right not to be subject to a decision based solely on automated processing, including profiling, where there is a legal or similarly significant effect on the person (the regulation prohibits automated processing where there is no meaningful human involvement in the decision and where the decision either impacts one's legal rights, or the decision has the potential to significantly influence the circumstances, behavior, or choices of the individuals concerned).

b) Other considerations:

i) Research affecting the healthcare a person receives, where there is no human involvement in the decision, would be considered covered under the regulation (i.e., assigning trial subjects to receive an intervention or placebo, based solely on the individual's personal data, i.e., test results).

ii) The regulation allow decisions to be made based on pure automated processing where the individual explicitly consents to the activity and where the controller implements measures to safeguard the person's data and rights.

(1) Safeguards include:

(a) Right to be provided meaningful information about the logic involved
(b) The potential consequences to the data subject
(c) Right of the data subject to obtain human involvement in the processing
(d) To challenge the decision

(2) Explicit consent is required where using special categories of data to make decisions based solely on automated processing.

Controllers who do not need to know identity of data subject are not required to learn identity to comply with exercise of rights of access, rectification, erasure, restriction of processing, or portability (often the case for research entities that hold only pseudonymised data).

- If the University of California can demonstrate that it is not in a position to identify data subjects, the University of California would not be able to address data subject requests for access, rectification, erasure, restriction, or data portability.

---

**BREACH OF PERSONAL DATA**

Both controllers and processors have obligations to respond to a personal data breach. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed, in any form or medium and is not limited to unauthorized access to electronic data.

A controller must report a data breach to the data protection authority in the affected individual's country without undue delay, and where feasible within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to affected individuals.

In the event of a breach causing a high risk to affected individuals, a controller must notify the affected individuals without undue delay, unless it qualifies for one of several enumerated exceptions.

*Articles 33-34, Data Breach*
*Article 83, Fines for the Infringement of this Regulation*

**Templates**

See [EU GDPR Informed Consent Form Addendum](#)
<table>
<thead>
<tr>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU GDPR</td>
</tr>
<tr>
<td>Article 29 Working Party (EU)</td>
</tr>
<tr>
<td>US DHHS SACHRP Recommendations</td>
</tr>
<tr>
<td>OHRP - Compilation of Guidance based on Country</td>
</tr>
<tr>
<td>UCI Information Security and Privacy – Resource and Guidance</td>
</tr>
</tbody>
</table>