Updated: November 6, 2018

The Implications of the General Data Protection Regulation (GDPR) on Research for Penn State

TABLE OF CONTENTS:

EXECUTIVE SUMMARY[1]

At Penn State, the GDPR will affect research in which data on **human subjects** is collected. Penn State researchers who wish to conduct human subjects research in the EU must:

1. where reasonable and appropriate, anonymize their data;
2. if anonymization is not reasonable or appropriate, pseudonymize their data; or
3. where reasonable and appropriate, obtain unambiguous consent from their data subjects and, in any case, provide notice to the data subjects of what the processing entails.

If requirements 1-3 cannot be met, the researcher must consult with and receive approval from Penn State's Chief Privacy Officer[2].

Points 1 and 2 are critically important because, if the data is truly anonymized, the GDPR does not apply, and if it is pseudonymized many of the GDPR's provisions are relaxed, including, without limitation, the requirement to comply with the right of erasure (right to be forgotten), as Researchers can be exempted if erasure is "likely to render impossible or seriously impair the achievement of the [research] objective."
Note: determination of impairment to the research objective is at the discretion of the researcher.

It is also important to note, that if an existing data set is received from another party, there may be certain compliance obligations and/or contractual terms that would require review by the Chief Privacy Officer.

[1] Sources: How GDPR Changes the Rules for Research; Top 10 Operational Impacts of the GDPR: Part 8 - Pseudonymization; GDPR – Full Text; GDPR – Recitals

[2] Holly Swires is currently Penn State's Chief Privacy Officer (email hzl104@psu.edu or privacy@psu.edu; phone 814-863-5915)

BACKGROUND

1. **Application of the GDPR**
   a. Recital 159 explicitly states that the GDPR applies "where personal data[3] are processed for scientific research purposes."
      i. "…the processing of personal data for scientific research purposes should be interpreted in a broad manner including, for example, technological development and demonstration, fundamental research, applied research, and privately funded research...scientific research purposes should also include studies conducted in the public interest in the area of public health."
      ii. That said, the GDPR aims to encourage innovation, as long as organizations implement the appropriate safeguards.

2. **Research as a basis for processing**
   a. Article 6(1) delineates the lawful bases for processing, which include where: (i) the data subject has given consent to the processing, (ii) processing is necessary for the performance of a task carried out in the public interest, and (iii) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.
      i. For the sake of clarity, **research is not explicitly designated as its own lawful basis for processing**.

   b. **Research where the data subject has given consent**
      i. Consent must be "unambiguous" and specific to the processing operation
         1. In the event that it is not possible to fully identify the purpose of the personal data processing for scientific research purposes at the time of collection, Recital 50 specifies "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations."
            a. Further, Article 5(1)(b) states "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."

3. **Conditions for research exemptions (Article 89 protections)**
   a. Controllers must put in place "technical and organizational measures" to ensure that they process only the personal data necessary for the research purposes, in accordance with the principle of data minimization[4] outline in Article 5(c).

   b. Pseudonymization

   c. "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is

[3] "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, genetic, mental, economic, cultural or social identity of that person"
[4] Personal data shall be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed"

kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable information"[5] (Article 4(3)(b)).

i. **Does <u>not</u> = anonymization.**
   1. Anonymous data[6] falls **out of the scope of the GDPR**

ii. Relaxes some of the provisions of the GDPR

iii. Not required but encouraged: "as long as [the research purposes] can be fulfilled in this manner" (Article 89(1)).

iv. If a controller deletes the directly identifying data rather than holding it separately, it may not be capable of reidentifying the data without collecting additional information. In this case, an exemption from the rights to access, rectification, erasure, and data portability exists.
   1. The exemption <u>only</u> applies if "the controller is able to demonstrate that it is not in a position to identify the data subject" (Article 11).[7]

4. <u>Notice</u>

a. Regardless of whether consent is the basis for processing, controllers are still bound to the notice requirements of Article 12(1).

i. Controllers must "take appropriate measures" to inform the data subjects of the nature of the processing activities and the rights available to them.
   1. The notice must be written "in a concise, transparent, intelligible, and easily accessible form, using clear and plain language."
   2. The notice must:
      a. Be provided at the time when the data is <u>first</u> collected;
      b. Include the controller's identity and contact information;
      c. Include the intended purposes of the processing activities[8];
      d. Include whether the data will be transferred to another entity or to another country;
      e. Per Article 13(2), include notice of the data subject's rights to access, rectification, erasure, and to object to processing; and
      f. "the period for which the personal data will be stored, or if that is not possible, the criteria used to determine the period."
   3. If the controller intends to further process for a different purpose, an updated notice <u>must</u> be provided

b. **Exemptions to the notice requirement**

i. If the personal data is received from someone other than the data subject (*e.g.*, a publicly available source) Article 14(5)(b) exempts the notice requirement if: "the provision of such information proves impossible or would involve a disproportionate effort."

ii. A researcher may also claim exemption if providing notice would be "likely to render impossible or seriously impair the achievement of the [research] objectives," provided

[5] In easier to manage language, pseudonymization involves removing or obscuring direct identifiers and, in some cases, certain indirect identifiers that could combine to reveal a person's identity. These data points are then held in a separate database, linked to the deidentified data base with a key.

[6] Data is considered anonymous only when it cannot be identified by any means "reasonably likely to be used…either by the controller or by another person" (Recital 26)

[7] If, however, a data subject provides the controller with the additional information that allows her to be identified in the data set, she must be permitted to exercise her rights under Articles 15-20.

[8] Recital 33 relaxes this provision if the scope of the researcher is not explicitly known.

there are appropriate safeguards in place, "including making the information publicly available."

5. **Exemptions from data subject rights**
    a. Right to be forgotten
        i. Article 17(3)(d) provides an exemption for research from the right of erasure insofar as it is "likely to render impossible or seriously impair the achievement of the [research] objective."
    b. Right to object to processing
        i. A researcher may override a data subject's objection if "the processing is necessary for the performance of a task carried out for reasons of public interest" (Article 21(6)).
            1. For a task to be justified by public interest, Recital 45 specifies that it "should have a basis in Union or Member State law."

6. **Transferring personal data to third countries for research purposes**
    a. The transfer of personal data to countries outside of the EU is prohibited unless the controller offers an "adequate level of protection" as determined by the European Commission (Article 45(1)). This transfer does not require any specific authorization.
    b. A controller may also transfer personal data to a third country if it has implemented specific safeguards, including Binding Corporate Rules[9] and standard contractual clauses, or if the data subject has provided explicit consent after being informed of the risks related to the transfer (Article 46(2); Article 49(1)(a)).
        i. United States corporations, including Penn State, would require one of the controls in 6.b.
    c. A controller may also transfer data to a third country when "necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subjects" (Article 49(1)).
        i. Such a transfer may be based on this ground only if it:
            1. Is not repetitive;
            2. Concerns a limited number of data subjects; and
            3. "the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards."
    d. The controller must inform the data subject as well as the data protection authority of the relevant member state of the international transfer

7. **Profiling**
    a. "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements" (Article 4(4)).
    b. To protect individuals from profiling and related processing, Article 35(2)(a) requires controllers to conduct a PIA any time "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person."

[9] As defined in Article 47

8. **Research concerning sensitive personal data**
    a. The processing of sensitive personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) is **prohibited**, unless:
        i. The data subject has given explicit consent to the processing for one or more specified purposes[10] (Article 9(2)(a)).
        ii. Processing relates to personal data which are manifestly made public by the data subject (Article 9(2)(e)).
        iii. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical 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.[11]

[10] Unless Union or Member State law provide that the prohibition may not be lifted by the data subject
[11] Clarified in Recital 52: research serves as a basis for processing sensitive data only "when provided by Union or Member State law and subject to suitable safeguards."