Bloomberg BNA

Medical Research Law & Policy Report®

Impact of the European Union's Approved General Data Protection Regulation On Scientific Research and Secondary Uses of Personal Data





By Mark Barnes, Rohan Massey, Heather Sussman, David Peloquin and Sara Shanti

On Dec. 16, 2015, nearly four years after the European Commission's initial proposal, the European Parliamentary Committee on Civil Liberties, Justice, and Home approved the text of the General Data Protection Regulation ("GDPR").[1] Upon Parliament's approval of the text, expected in early 2016, the GDPR will become law, superseding the existing Data Protection Directive ("Directive").[2] In contrast to the Directive, which is binding only on European Union ("EU") member states and requires the member states to "transpose" the Directive's principles into national law before becoming binding on data users, the GDPR is an EU-wide "regulation" that has direct effect and applies immediately as the rule in all EU countries, without needing to be transposed into national law. While as a regulation rather than a directive the GDPR will create consistent data protection standards and enforcement throughout the EU,[3] its impact on the processing and transmission of personal health data will directly affect

Mark Barnes and Heather Sussman are partners, and David Peloquin is an associate, with Ropes & Gray LLP in Boston.

Rohan Massey is a partner with Ropes & Gray LLP in London.

Sara Shanti is an associate with Ropes & Gray LLP in Chicago.

[1] The European Commission, the Parliament, and the Council agreed on the GDPR text during the Dec. 15, 2015, trilogue meeting. For the full consolidated text of the outcome of this meeting, *see* the European Parliament Agenda, *available at* http://tinyurl.com/nea3l8m.

[2] *See* Directive No. 95/46/EC of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data, O.J. L. 281/31 (1995).

[3] In addition to being binding in the 28 member states of the EU, the GDPR will also replace the national privacy laws of the three non-EU member states that have adopted EU privacy law: Iceland, Liechtenstein, and Norway. Together, these three

 ISSN 1539-1035

researchers' ability to process the data for scientific research. Fortunately for the research community, as will be explored in further detail below, the final draft of the GDPR appears much more favorable to research uses of data than had earlier drafts of the regulation.

Personal Data Protection

The GDPR regulates the processing and transmission of ''personal data,'' a term that is defined to mean:

> [A]ny information relating to an identified or identifiable natural person ''data subject''; 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.[4]

This definition expands the definition of personal data contained in the Directive by adding name, location data, online identifier and factors specific to genetic identity to the list of references that may make one identifiable. The GDPR states that ''personal data'' include both (i) identifiable personal data, and (ii) pseudonymised data.[5] The reference to pseudonymised data is important for the research community because techniques commonly employed to protect privacy in research studies, such as the key-coding of data, involve the use of ''pseudonymisation.'' While data that have been ''pseudonymised'' continue to be treated as ''personal data'' under the GDPR,[6] as is discussed further below, the GDPR recognizes that ''pseudonymisation'' may be an appropriate technique for safeguarding personal data, particularly in the research context.[7]

Notably, the GDPR's principles of data protection do not apply to anonymised data, including where the data are used for scientific research purposes.[8] The ability to render data anonymous remains difficult, however, for two reasons. First, the GDPR does not provide a ''safe harbor'' for anonymisation such as that found in U.S. law in the regulations of the Health Insurance Portability and Accountability Act of 1996 (''HIPAA'') pursuant to which data can be de-identified and taken outside of the ambit of HIPAA by removing a list of 18 identifiers.[9] Accordingly, anonymisation remains very much a facts-and-circumstances test. Second, the GDPR makes clear that to determine whether data are identifiable, ''account should be taken of all means reasonably likely to be used, such as singling out, either by the data controller *or by any other person* to identify the individual directly or indirectly.''[10] Accordingly, unlike in the U.S., where a researcher may be judged not to be using identifiable data if he or she lacks the ability to re-identify the data,[11] under the GDPR, the data are considered personal data, subject to the protections of the GDPR, if there exists the ability to re-identify the data.[12] Thus, when processing data believed to be anonymised, researchers using data derived from the EU must take special care to assess the potential for re-identification before diverging from processing practices required by the GDPR.

The GDPR also discusses certain ''special categories'' of data, including personal data concerning health,[13] as well as genetic data[14] and biometric data,[15] which the regulation states deserve a greater degree of protection.[16] As such, and as described more fully below, the processing of these special categories of personal data requires additional measures to meet the data minimization principle, including appropriate pseudonymisation. Importantly, the GDPR does not state explicitly that all genetic information is ''personal data'' subject to the protections of the GDPR. Rather, the definition of ''genetic data'' states that it means ''*all personal data* relating to the genetic characteristics of an individual,'' thus implying that genetic data is a subset of personal data.[17] This suggests that, as with any other type of personal data, genetic information, such as whole genome sequencing, must be evaluated on a case-by-case basis to determine whether it can be used to identify the individual to whom it pertains before determining whether it is personal data subject to the regulation. Such an interpretation is supported by the fact that earlier drafts of the GDPR had defined genetic data as ''*all data*, of whatever type, concerning the characteristics of an individual which are acquired during early prenatal development,'' thereby suggesting that ''genetic data,'' rather than being a subset of personal data, constituted instead a separate type of data altogether that was also protected by the regulation.[18] The GDPR narrows this

non-EU member states and the EU's 28 member states make up the European Economic Area.

[4] GDPR, Article 4(1).

[5] The GDPR states that personal data have been ''pseudonymised'' when they are processed ''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 kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.'' GDPR, Article 4(3b).

[6] *See* GDPR, Article 4(3b); *see also*, GDPR, Article 4(1).

[7] *See* GDPR, Recital 23; GDPR, Article 83(1).

[8] GDPR, Recital 23 (stating that ''anonymised data'' include ''information which does not relate to an identified or identifiable natural person'' and ''data rendered anonymous in such a way that the data subject is not or no longer identifiable.'').

[9] *See* 45 C.F.R. § 164.514(b).

[10] GDPR, Recital 23 (emphasis added).

[11] *See* 45 C.F.R. § 46.102 (emphasis added) (noting that private information is individually identifiable only where identity of the research subject may ''readily be ascertained *by the investigator*'').

[12] The GDPR does *not* apply to data of deceased individuals, although it expressly permits member states to implement national rules to protect such information. *See* GDPR, Recital 23.

[13] ''Data concerning health'' means ''personal data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status.'' GDPR, Article 4(12); *see also*, GDPR, Recital 26.

[14] ''Genetic data'' means ''all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question.'' GDPR, Article 4(10).

[15] ''Biometric data'' means ''any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data.'' GDPR, Article 4(11).

[16] *See* GDPR, Article 83 and Recital 42(a).

[17] GDPR, Article 4(10) (emphasis added).

[18] *See* Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free

   ISSN 1539-1035

scope, and now triggers application of the regulation when genetic data can be used to identify the subject of the data. Nevertheless, it bears noting that as genetic sequencing becomes more sophisticated and public and private databases of genetic information expand, it seems increasingly likely that a particular set of genetic information could be used to identify a particular individual, thereby rendering genetic information as ''personal data'' protected by the regulation and subject to the greater protections the regulation affords to ''genetic data.''

Because scientific research and clinical trials will often require special categories of data identified by the GDPR as needing higher protection, the differentiation between data categories is an important first step in determining the extent to which a given data set may be processed.

Processing Personal Data for Research

The GDPR imposes several specific requirements on processing of ''personal data'' that are applicable to research. In this final draft, the GDPR maintains an overall approach for the protection and processing of personal data that is consistent with that of the Directive; however, it appears to be mindful of researchers' needs by permitting some exceptions to general data processing requirements for data processed for scientific research purposes if certain safeguards, such as pseudonymisation of data, are employed.

The GDPR states that the processing of personal data shall be lawful provided that one of the bases for processing set forth in Article 6 applies. One of the bases for processing is that the data subject has consented to the processing of the data for a specific purpose.[19] Article 6 also allows for processing that is ''necessary for the purposes of the legitimate interest pursued by the controller or by a third party'' (hereinafter, ''legitimate interest'').[20] In the absence of further guidance, it appears that the GDPR may permit certain controllers and third parties to conduct scientific research in accordance with the legitimate interest exception, even in the event the controller has not secured consent from the data subject. We explore further each of these bases for processing in the next section of this article.

Notably, when ''personal data'' are processed for scientific research purposes pursuant to one of the legal bases described above, the GDPR provides that appropriate safeguards must be employed and identifiable data should be used only where anonymised data or pseudonymised data could not otherwise fulfill the research purpose. Specifically, Article 83 of the GDPR expressly requires that personal data processed for scientific research be subject to ''appropriate safeguards. . ., [which] shall ensure that technical and organisation measures are in place in particular in order to ensure the respect of the principle of data minimisation.''[21] The regulation clarifies that such measures may include pseudonymisation, but also states that, if the research can be fulfilled by processing personal data without the identification of the data subjects, it must be fulfilled in such manner.[22] The regulation further grants member states the ability to provide for derogations from various individual rights under the GDPR (most notably, rights related to access, rectification and restriction) if the rights would likely ''seriously impair'' the research purpose.[23] Thus, member states may continue to pass certain national legislation that will impact the manner in which researchers can use personal data.

Consent

The GDPR provides that the processing of personal data is lawful with the data subject's consent,[24, 25] including for the purpose of scientific research. Proper consent should be given ''by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to personal data relating to him/her.''[26] This may include a written or verbal statement, or by ticking a box when visiting an Internet website; these are distinguished from silence, pre-ticked boxes or inactivity by the data subject, which do not constitute proper consent.[27]

To ensure that consent is freely given and specific, the GDPR requires that, if the data subject's consent is given in a writing concerning other matters, the request for consent must be discernible from the other matters using clear and plain language.[28] That is not to say that consent cannot be broad, as long as the consent is given through clear affirmative action.[29] In fact, the GDPR recognizes that ''it is often not possible to fully identify the purpose of data processing for scientific research at the time of data collection. . ., [therefore, data subjects] should be allowed to give their consent to certain areas of scientific research.''[30] This language supports the existence and permissibility of broader consent under the GDPR, potentially resulting in obtaining the consent of users for secondary uses of the data for future research.

Generally, processing of special categories of data, including data concerning health, genetic data and biometric data,[31] is prohibited unless the data subject provides ''*explicit consent*''; however, such explicit consent is not required if the data are necessary for scientific research and are appropriately safeguarded.[32] Appropriate safeguards must be used in accordance with Article 83(1), which requires that data processed for scientific research be processed without identification of the data subject insofar as the purpose can be fulfilled in this manner.[33] Because the GDPR gives member states the power to ''maintain or introduce further conditions, in-

Movement of Such Data (General Data Protection Regulation) 2012/0011 (COD) C7-0025/12, Article 4(10); Article 9.

[19] GDPR, Article 6(1)(a).

[20] GDPR, Article 6(1)(f).

[21] GDPR, Article 83(1); *see also*, GDPR, Recital 30.

[22] GDPR, Article 83(1).

[23] GDPR, Article 83(2); *see also*, GDPR, Recital 42a.

[24] ''Data subject's consent'' means ''any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.'' GDPR, Article 4(8).

[25] GDPR, Article 6(1)(a).

[26] GDPR, Ch. 1, Article 4(8); GDPR, Recital 25.

[27] GDPR, Recital 25.

[28] GDPR, Article 7.

[29] *See* GDPR, Recital 7.

[30] GDPR, Recital 25(aa).

[31] Special categories of data also include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life and sexual orientation.

[32] GDPR, Article 9(2)(i); *see also*, GDPR, Article 83(1).

[33] GDPR, Article 83(1).

cluding limitations,'' for processing health data,[34] controllers must ensure that more restrictive national laws do not apply.

Also notable is that consent for the processing of personal data for scientific research may be obtained contemporaneously with the informed consent for clinical trial participation.[35] This is similar to the process in the U.S. of combining an informed consent for research with an authorization for use and disclosure of protected health information under HIPAA. Finally, data subjects shall have the right to withdraw consent at any time. Importantly for clinical research, however, when the GDPR is read in concert with the EU's Clinical Trial Regulation, expected to take effect later this year, it appears that if a data subject participating in a clinical trial withdraws his or her consent for processing of data, those data that were collected prior to withdrawal of consent may continue to be processed.[36]

Legitimate Interests

In the absence of consent, the GDPR permits processing of personal data as necessary for the legitimate interests pursued by the controller or third party. For some controllers, processing data for scientific research may constitute a legitimate interest. The personal data can only be lawfully processed under this exception, however, if the legitimate interest does not override the interests or fundamental rights of the data subject.[37] Although the term ''legitimate interest'' is not further defined in the GDPR, necessitating careful assessment of whether the data subject ''can reasonably expect at the time and in the context of the collection of the data that processing for this purpose may take place,''[38] the regulation does provide that a legitimate interest may exist when there is an appropriate relationship between the controller and the data subject such as the data subject being a client of the controller.[39]

In 2014, the Article 29 Data Protection Working Party (''Working Party'') issued Opinion 06/2014, providing additional analysis and guidance on the application of the legitimate interest exception, as set forth in Article 7(f) of the Directive, and factors to consider.[40] The Working Party opined that the concept of ''interest'' is closely related to, but distinct from, the Directive's use of the term ''purpose,'' stating that a purpose ''is the specific reason why the data is processed . . . [a]n interest . . . is the broader stake that a controller may have in the processing, or the benefit that the controller derives—or that society might derive—from the processing.''[41] The Working Party also expressly identified ''processing for research purposes (including marketing research)'' as a common context, in which the issue of legitimate interest may arise,[42] and specially found historical and other kinds of scientific research to be an ''important context where the legitimate interests of third parties may be relevant.''[43, 44]

The Working Party's findings appear to have been adopted by the GDPR, stating that where the processing is for a legitimate purpose, which is not the same purpose for which the data were initially collected, the controller must take into account certain factors, such as the nature of the personal data, the consequences of the secondary use of the data and existing safeguards protecting the data.[45] Although the GDPR requires that personal data only be collected for ''specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,'' it also provides a carve-out for scientific research, in agreement with the Working Party, by explicitly stating that further processing for scientific and historical research purposes shall not be considered incompatible with the initial purpose of data processing.[46] Therefore, the legitimate interest exception may apply to secondary uses of personal data as well as the legitimate interests of third parties, when the processing is for scientific research, which could be of significant value to researchers.

When special categories of personal data are being processed, then under this legitimate interest exception, explicit consent is not additionally required if the processing is *necessary* for scientific research purposes.[47] In all instances, what is ''necessary'' for the legitimate interests of the controller or third party will be construed very narrowly and should, therefore, be carefully considered by the party before relying on this method of processing legitimization. It is worth repeating, however, that even when the special categories of data can be processed without explicit consent, if the purpose of processing the data is for scientific research purposes, then safeguards and pseudonymisation (where possible) are required to meet the data minimization principle, in accordance with Article 83.[48]

Right to Transfer Personal Data

The intention of the GDPR is to protect personal data both within the borders of the EU and to ensure that data that are transferred from the EU to a foreign jurisdiction receive an adequate level of protection. Consequently, the GDPR restricts the transfer of personal

[34] GDPR, Article 9(5).

[35] *See* GDPR, Recital 126b; *see also*, EU Regulation 536/2014.

[36] EU Regulation 536/2014, Article 28(3); GDPR, Article 7(3).

[37] GDPR, Article 6(1)(f).

[38] GDPR, Recital 38.

[39] *Id*.

[40] ''Factors to consider when carrying out the balancing test include: the nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned; the impact on the data subject and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed; additional safeguards which could limit undue impact on the data subject, such as data minimisation, privacy-enhancing technologies; increased transparency, general and unconditional right to opt-out, and data portability.'' *Article 29 of the Data Protection Working Party*, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, *see* pages 3, 51, and 56 (adopted April 9, 2014).

[41] *Id*., page 24.

[42] *Id*., page 25.

[43] *Id*., page 28.

[44] *Id*., *see* pages 64-65 (providing examples of permissible scientific research, which balances sufficient privacy and security to meet the legitimate interest rationale under the Directive).

[45] GDPR, Recital 40.

[46] GDPR, Article 5(1)(b), *see also*, GDPR Recital 40.

[47] GDPR, Articles 9(2)(a) and 9(i).

[48] Additionally, GDPR, Recital 125aa states that in order ''to facilitate scientific research, personal data can be processed for scientific research purposes subject to appropriate conditions and safeguards set out in Member State or Union law.''

   ISSN 1539-1035

data, allowing transfer to a country outside of the European Economic Area[49] or an international organization, without a specific authorization, only if the European Commission has decided that the country or organization ensures an adequate level of protection.[50] In the absence of such a decision, personal data may be transferred only in limited situations. Those that appear most relevant for the research context include where (i) the controller has adduced appropriate safeguards, including through the use of binding corporate rules, standard data protection contractual clauses (''model clauses'') adopted by the European Commission or an approved code of conduct,[51] or (ii) the data subject provides explicit consent to the proposed transfer upon being informed of the risks.[52] These legal bases for transfer exist currently under the Directive, and thus should be familiar to those in the research community who have experience transferring personal data from the EU to a country that lacks an adequate level of protection.

If a given transfer does not meet the requirements necessary to support a legal basis for transfer, the GDPR has introduced another mechanism for transferring data 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 subject.''[53] In order to qualify as a transfer for a compelling legitimate interest, the GDPR requires that the transfer (i) is not repetitive; (ii) concerns a limited number of data subjects; (iii) is necessary for legitimate interests that are not overridden by the data subjects' interests or rights; (iv) has been assessed by the controller; (v) includes documentation of the assessment adducing suitable safeguards; and (vi) is communicated to the supervisory authority by the controller.[54] Notably for the research community, the GDPR's recitals suggest that when the transfer is for scientific research purposes, the legitimate expectations of society for an increase of knowledge should also be taken into consideration to determine whether a compelling legitimate interest exists.[55] Although the GDPR may allow the transfer for research purposes of personal data from the EU to a third country lacking adequate protections under this compelling legitimate interest rationale, in practice it seems unlikely that there will be many situations in which a researcher would be able to rely on this basis of transfer because the researcher could not otherwise transfer the data under another clear basis of legal transfer, such as obtaining the consent of a data subject to the transfer or entering a contract containing the model clauses.

We note also that under the Directive, one of the most common bases for transfer of personal data from the EU to the U.S. was the U.S. Department of Commerce's U.S.-EU Safe Harbor Framework.[56] In October 2015, the European Court of Justice (''ECJ'') invalidated the European Commission's decision on the adequacy of the U.S.-EU Safe Harbor Framework.[57] As a result, U.S. and EU officials have negotiated a new mechanism, the EU-U.S. Privacy Shield, to allow for the secure transfer of personal data between the EU and U.S. The EU-U.S. Privacy Shield will require more robust data protection by companies in the U.S. and stronger enforcement and monitoring by the U.S. Federal Trade Commission (''FTC''). The EU-U.S. Privacy Shield was announced on Feb. 2, 2016, and an ''adequacy decision'' by the ECJ is expected in the following weeks with implementation of a final agreement thereafter. In the meantime, entities are encouraged to watch for important compliance dates and prepare to take action to legitimize data flow under new standards.

Right to Erasure

The GDPR provides an individual with the right to request the deletion of any personal data identifying him or her that is held by a data controller, a right which is commonly known as the ''right to be forgotten'' or ''right to erasure.'' As proposed in earlier drafts of the GDPR, this right appeared to pose a challenge for researchers as the erasure of data by data subjects could pose a significant challenge to maintaining the integrity of research data. Under the GDPR, data subjects in general have the right to obtain the erasure of personal data without undue delay when the data are no longer necessary for the initial purpose or when consent for the use is withdrawn.[58] However, the GDPR expressly carves out an exception to this general rule for research if the right to erasure would likely ''render impossible or seriously impair the achievement of the objectives of the . . . scientific and historical research purposes.''[59] In such event, researchers may further retain and process personal data for scientific research despite a data subject's request for erasure.[60]

This is a welcome exception to many researchers because honoring the right to erasure in research would seriously impair or even negate the findings made in a clinical trial or other study. Notwithstanding this exception, principles of data minimization and implementation of safeguards required under the GDPR continue to apply to the personal data that are maintained for the permissible purpose, regardless of whether the right to erasure applies to the data.[61]

Conclusion

While the GDPR has brought assurances that the regulation does not intend to hinder scientific research, the GDPR nevertheless requires thoughtful action prior to processing personal data for research purposes. The GDPR will not be enforced before 2018; however, enhanced penalties up to the greater of €20 million ($22.5

[49] *See supra*, Note 3 (noting that the European Economic Area is made up of the 28 EU member states as well as Iceland, Liechtenstein and Norway).

[50] GDPR, Article 41(1). Note that the European Commission has found only a handful of jurisdictions to offer adequate data protection. These include Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey and New Zealand.

[51] GDPR, Article 42(1); *see also*, GDPR, Article 43.

[52] GDPR, Article 44(1)(a).

[53] GDPR, Article 44(1)(h).

[54] GDPR, Article 44(1)(h) and (6).

[55] GDPR, Recital 88.

[56] Note that the U.S.-EU Safe Harbor Framework is not available for not-for-profit entities.

[57] Federal Trade Commission's Update on the U.S.-EU Safe Harbor Framework, *available at* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

[58] GDPR, Article 17(1).

[59] GDPR, Article 17(3)(d).

[60] *See* GDPR, Recital 53.

[61] *See* GDPR, Article 5(1)(c).

million) or 4 percent of annual revenue highlights the importance of compliance. Additionally, due to the anticipated new EU-U.S. Safe Harbor agreement, researchers and entities should continue to monitor the use and transmission of personal data and consider how best to respect the GDPR's requirements related to consent, pseudonymisation and other safeguards so that research data are used to their maximum value without risking noncompliance.

  MRLR ISSN 1539-1035