Contribution ID: 44739abe-c0b5-4c7d-83ce-c8b9ab290c7e
Date: 09/04/2021 03:57:53

EDPB Stakeholder event on the application of the GDPR to the processing of personal data for scientific research purposes
30th April 2021

Fields marked with * are mandatory.

Preparatory stakeholder survey

Prior to the stakeholders event on 'the application of the GDPR to the processing of personal data for scientific research purposes' (April 30, 2021) the EDPB would like to invite participants to provide their feedback on how challenges in the application of the requirements of the GDPR in the field of scientific research can be met.

This survey is particularly aiming at gathering information on solutions and good (scientific research) practices that are currently being used, considered, developed and implemented by stakeholders. It also aims at identifying on which points a further clarification of the requirements of the GDPR is needed.

This will allow the EDPB to prepare a discussion paper as input for the stakeholders event in order to focus the discussion on solutions to promote GDPR-compliant, good scientific research practices on the relevant issues and to identify the role various actors can play to reach this goal.
This stakeholder event is without prejudice to the public consultation which will be carried out after the publication of EDPB guidelines, still to be adopted, on processing personal data for scientific research purposes.

Please note that your replies will be anonymous, only used in the context of the stakeholders event and in order to give the opportunity to stakeholders who will not participate to the event to provide their input.

---

* **Have you been invited to participate in the event?**

- ○ Yes
- ◉ No

Question 1 – A definition of scientific research.

In the GDPR it is foreseen that certain requirements for controllers do not apply or are modified in case of ‘processing of personal data for scientific research purposes’ (research exemptions). In order to rely on said exemptions it is important to know what criteria to use to determine what - under the GDPR - can and cannot be considered ‘scientific research purposes’ and/or ‘scientific research’. The GDPR does not provide a definition and/or clear criteria. Both EDPB and EDPS have given an opinion on the matter. But making a distinction, for instance based on whether or not the scientific research is in the ‘public interest’ remains controversial.

What are your ideas/suggestions on how to clarify this issue?

It would be helpful to the scientific research community if a definition of research could be provided in the upcoming EDPB guidance on GDPR and scientific research. A common definition of “research” that would provide clarity but also flexibility would be the following:

"A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."

Much research that is sponsored, funded or conducted by private parties can have benefit to society at large. For example, clinical trials sponsored and funded by private industry often result in the development of new medicines or medical devices that advance human health. Including a “public interest” requirement in the research provisions of GDPR may cause confusion as to whether privately-funded research can qualify for the research exemptions. We would thus urge that the upcoming guidance not include such a requirement.

Question 2 – Research exemptions and the need to provide for additional safeguards.

In most ‘research exemptions’ in the GDPR, reliance on such an exemption is made conditional on the provision of additional and/or compensatory safeguards and measures to protect the rights and interests of data subjects. Article 89(1) GDPR also - in general terms – requires appropriate safeguards in case of processing for scientific research purposes.

What would you consider to be appropriate safeguards and measures to protect (which) rights and interests of data subjects in (which) cases of processing personal data for scientific research purposes?

The most important and practical safeguard is to respect the principle of data minimization, which prescribes that the researcher should not access more data than is necessary to complete the research. In many research contexts this is often achieved through using pseudonymised as opposed to fully identifiable data. The GDPR's text already provides for this appropriate safeguard through the requirement in Article 89(1) that processing for scientific research purposes ensure that technical and organizational measures be put in place to safeguard the data and ensure respect for the principal of data minimization. Given the large variation in data needs for different types of scientific research, it seems appropriate to maintain the general principles set forth in Article 89(1) as opposed to trying to impose more prescriptive safeguards.

Question 3 – Further processing of personal data for scientific research purposes

Both the concept of ' broad consent' and the 'compatibility presumption' could play a role in facilitating the further processing of personal data for scientific research purposes.

What are your ideas on how to reconcile the use of such concepts with essential GDPR principles pertaining to the specificity of consent and to purpose limitation?

One challenge of reconciling scientific research practices with GDPR has been that the concept of informed consent lies at the center of ethical principles of research, yet certain interpretations of GDPR have disfavored the use of consent as a basis for processing personal data for research purposes. The Declaration of Helsinki, a cornerstone document of research ethics, provides that for individuals who are capable of giving informed consent, their consent must be sought before they are enrolled as subjects in research. The Declaration of Helsinki also provides that for medical research using identifiable human material or data, such as research on material or data contained in biobanks or similar repositories, individuals should be asked to provide consent for collection, storage and/or reuse of data, except where it would be impossible or impracticable to obtain such consent. In all cases in which consent is sought, the consent must be voluntary.

The text of GDPR is congruent with these principles of research ethics: Article 9(2)(a) permits explicit consent to serve as a condition that lifts GDPR's general prohibition on processing "special categories" of personal data and Recital 33 provides that "data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research." The EDPB could facilitate this congruence in its upcoming guidance on GDPR and scientific research by clarifying that consent that would satisfy the standards for informed and voluntary consent under the Declaration of Helsinki should also satisfy the standard for explicit consent under GDPR. There is no principled reason why an investigator should be able to obtain voluntary consent from subjects to participate in a clinical trial of a medicine of unknown safety and efficacy while not at the same time being able to obtain the subject's consent for processing of their data for research purposes.

The GDPR's concept of compatibility is congruent with the concept of consent outlined in Recital 33. In cases in which obtaining consent is not possible or would prove impracticable, the concept of compatibility provides a pathway for processing of personal data for scientific research. In this way, Recital 33, when read in concert with the concept of compatibility, is aligned with the principles of research ethics set forth in the Declaration of Helsinki. Because the concept of compatibility is agnostic as to the requirements of EU member state law, permitting compatibility to be invoked for processing for scientific research purposes provides a consistent pathway to enable scientific research across EU member states. This is in contrast to certain GDPR conditions that permit processing of special categories of personal data, such as Article 9(2)(j), which may be invoked only when permitted by EU or member state law. The concept of compatibility is thus aligned with GDPR's goal of harmonizing data protection law across the EU.

Question 4 – Transparency.

In case of the storage of personal data in large databases, for long-term use for unspecified scientific research purposes, transparency on and control over the use of such personal data can be at risk.

What are your ideas on how data subjects can be provided with appropriate information and means to maintain control in such cases? What types of governance would you consider appropriate for such situations?

In instances in which subjects are asked to provide consent for storage of their data in databases for future research purposes, the consent process can be used to provide data subjects with information about how their information will be processed and how they may withdraw consent to further data processing. Technology may be harnessed to update individuals about the purposes for which data are used, such as through providing email updates to interested subjects about research projects that use data from the databank. The ability of the subject to withdraw consent to further processing of his or her data is a key means by which the data subject can exercise control. The consent should explain limitations on such withdrawal, such as instances in which data have been released for future research projects in which deletion of a particular data subject's data would compromise the integrity of the research.

In instances in which obtaining consent would be impracticable and processing thus occurs on the basis of compatibility or article 9(2)(j), GDPR provides that the general notice requirement can be excused, but that the controller "shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available." (See GDPR Article 14(5)(b)). These requirements might be accomplished by creating a public website that provides information about the research and contact information for those wishing to learn more about research uses of personal data.

Question 5 - Codes of conduct.

What issues do you consider suitable to be clarified and/or elaborated upon in a code of conduct? Who could take the lead in such a process? What would be determinants in successfully pursuing such a route?

A key principle of GDPR is that of compatibility. A code of conduct could set forth principles to be used by code adherents to determine when processing of personal data for scientific research purposes is compatible with the purposes for which the data have been collected.

GDPR has posed particular challenges for transnational research collaborations given the limitations it places on the transfer of personal data from the EU to "third countries" that have not been found by the European Commission to maintain adequate data protection legislation. Article 46 of GDPR provides that a code of conduct may be one mechanism to permit cross-border transfers of personal data to countries that lack adequacy decisions. A code of conduct could be particularly useful in establishing a mechanism for cross-border data transfer. Given that scientific research is an activity that often involves both commercial, for-profit entities and charitable, not-for-profit entities, the organization that performs the monitoring activity required under GDPR Article 41 should be one that contains members from both of these types of organizations.

Question 6 – Agreements between joint controller or controller and processor.

Partners collaborating in research projects, especially in large research consortia, should be aware of their respective responsibilities under the GDPR and make the appropriate agreements. For the field of 'scientific research', what would you consider good examples and/or models of joint controller agreements and/or 'controller-processor agreements'?

The joint controller agreement should specify in which cases the parties act as joint controllers and in which cases they act as independent controllers. In research consortia, certain activities, such as the creation and management of a research databank, are typically undertaken jointly by multiple organizations who together determine the conditions pursuant to which data may be collected for the databank and made available to researchers. By contrast, the individual research projects for which data are made available from the databank are often designed not by the entire consortium but rather by individual researchers and their organizations. For those projects, the individual researchers and their organizations act as independent controllers.

The joint controller agreement should set forth clearly the circumstances in which the parties act as joint controllers and those in which the parties act as independent controllers. The joint controller agreement should address the process through which notice is furnished to data subjects, the process for establishing a basis for processing personal data, the identity of the party that will serve as a contact person for the exercise by data subjects of their rights under GDPR, the identity of the party that will be responsible for notifying data subjects and supervisory authorities in the event of a data breach, and the mechanism to legitimize cross-border data transfers. With respect to cross-border data transfers, the joint controller agreement may include standard contractual clauses between members to facilitate such transfers.

In the context of a research consortium, the participating members typically would not act as "processors." There may, however, be vendors performing services on behalf of the consortia that act as "processors." For example, there may be cloud computing services or statistical analysts that act as a processor because they perform a service at the direction of the consortium without having input into the purposes and means for which data are processed. In such circumstances, a controller-processor agreement will be needed between the consortium and the processor. If the consortium is not itself a legal entity with the ability to contract for services, the joint controller agreement should specify which members of the consortium will enter the controller-processor agreement with the service provider and the terms of such agreement.

Contact

edpb@edpb.europa.eu