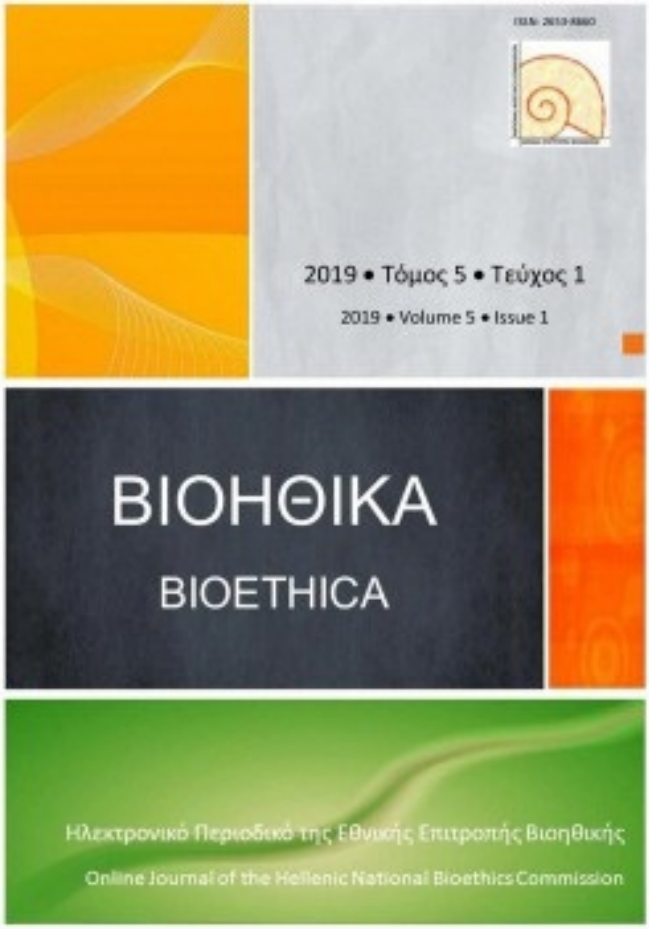
Bioethica

Vol 5, No 1 (2019)

Bioethica



General Data Protection Regulation and Horizon 2020 Ethics Review Process: Ethics Compliance under GDPR

Albena Kuyumdzhieva

doi: 10.12681/bioeth.20832

To cite this article:

Kuyumdzhieva, A. (2019). General Data Protection Regulation and Horizon 2020 Ethics Review Process: Ethics Compliance under GDPR. *Bioethica*, *5*(1), 6–12. https://doi.org/10.12681/bioeth.20832

General Data Protection Regulation and Horizon 2020 Ethics Review Process: Ethics Compliance under GDPR

Albena Kuyumdzhieva[1]

[1] Programme Manager Research/Ethics Review, Scientific Advise Mechanism, Ethics and Research Integrity Sector, DG RTD, European Commission.

albena.kuyumdzhieva@ec.europa.eu

Abstract

The present manuscript examines the new ethics data protection requirements introduced for the research projects funded by the European Programme Horizon 2020.

Initially, reference is made to the basic data protection principles introduced by the General Data Protection Regulation (GDPR) and the derogations permitted in the research field in favor of the science advancement. Although these derogations are subject to a number of safeguards to protect personal data, new ethics requirements are introduced for research projects funded by the European Programme Horizon 2020. The aim of these safeguards is the increased transparency and accountability at the data processing and the consequent enhanced protection of the individuals' rights. These requirements are geared to the main research ethics postulate, which requires free, voluntary and informed participation of the research subject.

Under these new requirements, Horizon 2020 beneficiaries/applicants must comply with a set of predefined standards, reflecting their ethical and legal obligations, provide a detailed and precise description of the technical and organisational measures that will be implemented in order to safeguard the rights of the research participants and also demonstrate their observance. In addition, depending on the type of the data being processed and the data processing techniques, the H2020 applicants/beneficiaries may need to provide a number of additional documents/explanations and implement further measures.

Keywords: General Data Protection Regulation, GDPR, Horizon 2020, ethics review.

Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (ΓΚΠΔ) και διαδικασία ηθικής αξιολόγησης στο πλαίσιο του Ορίζοντα 2020: Συμμόρφωση ηθικής και δεοντολογίας υπό τον ΓΚΠΔ

Albena Kuyumdzhieva[1]

[1] Programme Manager Research/Ethics Review, Scientific Advise Mechanism, Ethics and Research Integrity Sector, DG RTD, European Commission.

Περίληψη

Το παρόν κείμενο εξετάζει τις νέες απαιτήσεις δεοντολογίας για την προστασία των προσωπικών δεδομένων που εισήχθησαν στο πλαίσιο των χρηματοδοτούμενων από το ευρωπαϊκό προγράμμα Horizon 2020 ερευνητικών έργων.

Αρχικά, γίνεται αναφορά στις βασικές αρχές προστασίας δεδομένων που εισάγονται από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και τις παρεκκλίσεις που επιτρέπονται στον χώρο της έρευνας με σκοπό την πρόοδο της επιστήμης. Παρόλο που οι παρεκκλίσεις αυτές υπόκεινται σε ορισμένες διασφαλίσεις για την προστασία των προσωπικών δεδομένων, νέες απαιτήσεις δεοντολογίας εισάγονται για τα ερευνητικά έργα που χρηματοδοτούνται από το ευρωπαϊκό πρόγραμμα Horizon 2020. Στόχος των διασφαλίσεων αυτών είναι η αυξημένη διαφάνεια και ευθύνη κατά την επεξεργασία δεδομένων και η συνακόλουθη ενισχυμένη προστασία των δικαιωμάτων των φορέων των δεδομένων. Οι απαιτήσεις αυτές είναι προσανατολισμένες στην κύρια αρχή της δεοντολογίας της έρευνας που προϋποθέτει την ελεύθερη και ενημερωμένη συμμετοχή του υποκειμένου στην έρευνα.

Στα πλαίσια αυτών των νέων απαιτήσεων, οι ερευνητές του προγράμματος Horizon 2020 πρέπει να συμμορφώνονται με ένα σύνολο προκαθορισμένων προτύπων που αντικατοπτρίζουν τις δεοντολογικές και νομικές υποχρεώσεις τους και να περιγράφουν με λεπτομέρεια και ακρίβεια τα τεχνικά και οργανωτικά μέτρα που θα ληφθούν προκειμένου να διαφυλαχθούν τα δικαιώματα των συμμετεχόντων στην έρευνα, καθώς και να αποδεικνύουν την τήρησή τους. Ανάλογα δε με τον τύπο των δεδομένων που υποβάλλονται σε επεξεργασία και τις τεχνικές επεξεργασίας δεδομένων, οι συμμετέχοντες στο πρόγραμμα χρειάζεται να παράσχουν μια σειρά προσθέτων εγγράφων και εξηγήσεων και να λάβουν περαιτέρω μέτρα.

Λέξεις κλειδιά: Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα, ΓΚΠΔ, Ορίζοντας 2020, αξιολόγηση ηθικής και δεοντολογίας.

I. Introduction

The rapid digital revolution changed the way people live and communicate, thus creating research development opportunities that were hardly existing in the 'off-line' era. And while the benefits of these new developments are undeniable, they can sometimes come at a 'price' to ethics, as the daily interactions between the different technologies and the social fabric can have unforeseen social, political, environmental and human impacts that go far beyond the initial purpose of the applied technologies/research methods.

Safeguarding the basic rights to privacy and data protection[1] in all H2020 funded projects is therefore among the main priorities of the Ethics Review Process. The entry into force of the EU General Data Protection Regulation 2016/679 (GDPR) underpinned the right to privacy and data protection, by translating these principles into an enforceable legal framework. While the Regulation (which entered into force on 25th of May 2018), builds on the principles of the previous EU Data Protection Directive 95/46/EC (repelled by GDPR), it introduces new elements, aimed at increasing transparency and accountability of the data processing and enhancing the data protection rights of the individuals. Among them are:

- Enhanced accountability: data controllers/processors are accountable for the data processing operations and must be able to demonstrate compliance with GDPR at all times (record-keeping). Failure to do so may result in a number of sanctions and administrative fines (up to 20 0000 or 4% of the global turnover, whatever is higher).
- Risk based approach: A number of technical and organisational measures must be introduced to safeguard the data subject's rights during the data processing operations. These include amongst others: data minimisation; data protection by design and by default; notification of data breach to the National Data Protection Authorities and data subjects; data protection impact assessments; appointment of data protection officer etc. The appropriateness of those measures should be assessed when taking into consideration the nature, scope, context and purpose of the processing activities and the risks to the human rights and freedoms of the data subjects, associated with the processing.

II. GDPR in the context of scientific research

Acknowledging the importance of personal data processing for scientific purposes, GDPR enables science advancement by providing a number of research specific derogations. The most significant of them refer to purpose and storage limitations, processing of special categories of data, secondary use and data subject rights.

- ***Special categories of data (formerly known as sensitive data.)***[2] the processing of such data is generally prohibited, with a few notable exceptions, such as scientific research.
  The processing of special categories of data for research purposes is however subject to the application of appropriate safeguards, aimed at protecting the fundamental rights and interests of the research participants and ensuring proportionality between the aim of the processing and the nature of the processed data. Member states are empowered to choose to maintain or introduce further conditions or limitations with regard to the processing of genetic, biometric and health data and adopt derogations for some of the

[1] Art. 8 EU Charter of Fundamental Rights and art. 16 (1) TFEU

[2] Special categories of personal data include: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation (art. 9.1 GDPR).

data subjects' rights (art. 9(4) and art. 89(2) GDPR).

- ***Broad consent:*** Consent under GDPR must be free, specific, informed and unambiguous, given by clear affirmative action.[3]

For research purposes, however, GDPR provides specific derogation, introducing the notion of *broad consent*. This notion is applicable in cases where it is difficult, if not impossible to envision all purposes of personal data processing at the moment of data collection. Such exception suggests that researchers may apply the notion of broader consent, covering not only the specific study but particular areas of scientific research. The latter is possible only if the rights of the data subjects are safeguarded by adherence to the recognised ethical standards of scientific research (recital 33 GDPR). Key consideration should be given to the fairness of data processing in this regard.

- ***Storage limitation*:** Under GDPR, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

In the research context, GDPR allows research data to be stored longer than it is absolutely necessarily for the purposes for which the data are processed, providing that appropriate justification and technical and organisational measures are set in place.

- ***Right to information:*** GDPR strengthens the data subject rights by providing extensive list of elements, comprising the information rights of the individuals along with the rights to access and rectification, right to be forgotten, right to restriction of processing, right to be informed and object profiling etc. (art.13-21).

Under certain conditions (e.g. when the personal data have not been obtained from the data subjects directly), GDPR exempts the researches from their obligation to provide information to the research participants, if this proves impossible or involves disproportionate effort [art.14.5 (b)]. In applying this exemption, the number of the individuals involved, the age of the data subjects and the safeguards adopted should be taken into consideration along with the requirement for fair data processing;

These derogations are subject to a number of safeguards ensuring that appropriate technical and organisational measures for protecting the rights and freedoms of the data subjects are set in place (art.89). These include upholding the principle of data minimisation at all times and using anonymised/pseudonymised data, if the research purposes can be achieved in this manner. Data protection impact assessments and the appointment of data protection officers, along with the possibilities for enforcing sanctions and substantial administrative fines complement the privacy and data protection safety net.

III. New Ethics Data Protection Requirements for Horizon 2020 Funded Projects

A number of ethics requirements aimed at ensuring the fairness of the data processing and safeguarding the human rights and freedoms of the research participants have been established within the framework of H2020 Ethics Review Process. These are geared around the main research ethics postulate that research participation should be free, voluntary and informed, or in other words, no person should become unwilling or involuntary participant in a research experiment.

Depending on the type and scale of the processed personal data, the methodology used, and the potential risks for the research participants, Horizon 2020 beneficiaries/applicants must comply with a set of pre-established standards, reflecting their ethical and legal obligations.

[3] For research involving clinical trials, the processing of data should also comply with the requirements established in the Regulation (EU) 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.

As a general rule, whenever the research project involves the processing of personal data, H2020 applicants/beneficiaries must demonstrate that the principle of data minimisation (collect only data which is relevant and limited to the purposes of the research project) is adhered at all times and consider if their research objectives cannot be met by using anonymimised or pseudonymised data. They must also provide a detailed description of the technical and organisational measures that will be implemented in order to safeguard the rights of the research participants. Such measures include, but are not limited to:

- the involvement of institutional data protection officer (DPO) in the design of the data processing operations and disclosure of his/her contact details to the research participants;
- elaboration of a project specific data protection policy, including description of the security measures to prevent unauthorised access to personal data, details of the anonymisation /pseudonymisation techniques; justification of why research data will not be anonymised/ pseudonymised (if relevant), explanation on how is all of the processed data relevant and limited to the purposes of the project ('data minimisation' principle).
- Detailed description of the data transfers (type of data transferred and country to which it is transferred - for both EU and non-EU countries).

In addition, the applicants/beneficiaries must also provide details of the informed consent procedures that will be implemented and - depending of the severity of the research intervention- submit templates of the informed consent forms and information sheets (if available at the time of the application).

Depending on the type of the data which is processed and the data processing techniques, the applicants/beneficiaries may need to provide a number of additional documents/explanations. These refer to the following cases:

Processing of special categories of personal data

The processing of special categories of data may potentially expose the research participants to higher risks, and therefore a higher level of protection must be ensured for such data processing operations. If such type of data is processed within the proposed project, the researcher must justify the need for such processing and provide comprehensive description of the data protection policy and security arrangements.

Further on, the processing of genetic, biometric and health data requires additional attention as EU Member States have the right to adopt special derogations pertaining to the processing of such data. The researchers should therefore check if special derogations have been established under the national legislation of the country where the research takes place, ensure compliance with the latter and submit a declaration of compliance to the funding agency.

Data processing involving profiling, systematic monitoring of individuals or processing of large scale of special categories of data, intrusive methods of data processing or any other data processing operation that may result in high risk to the rights and freedoms of the research participants.

Some data processing techniques might be extremely privacy intrusive and may expose the research participants at higher ethics risks. Examples of such intrusive methods include: behaviour profiling, tracking, surveillance, audio and video recording, geo-location tracking etc.

In case H2020 applicants/beneficiaries intend to use any privacy intrusive data processing methods, they must include in their research protocol a comprehensive description of the latter and carry out a comprehensive assessment of the ethics risks associate with the data processing activities. The researchers must also reflect on the potential harms to the rights of the research participants and devise risk mitigation measures. In cases the data processing operations may result in high risks for the data subjects, the researchers should also seek the opinion of the data controller on the need for a data protection

impact assessment in accordance with art. 35 GDPR.

In case the proposed research involves profiling, researchers must also provide description of the procedures for informing the research participants about the profiling and its possible consequences, and explain the adopted risk mitigation measures.

Further processing of previously collected personal data

In case the research will involve data processing of previously collected data, (e.g. use of pre-existing data sets or sources, merging existing data sets), the applicants/beneficiaries must provide details of the database used or of the source of the data and the particular data processing operations, along with the permission of the owner/manager of the data sets (when relevant).They must explain how the privacy and data protection rights of the research participants will be safeguarded. This is particularly pressing in the cases, where the personal data is not collected by the researcher (but a third party) and the research participants are unaware that they take part in this particular research. This is why it is of crucial importance for the applicants/beneficiaries to be able to explain the lawful basis for the further processing and demonstrate that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects.

Processing of publicly available persona data

H2020 applicants/researchers must be aware that the mere fact of posting information on any media platform does not mean that these data become 'open'[4] and can be used by everyone. When using such data, they must consider the reasonable expectations of privacy of the data subjects (e.g. privacy-settings, closed groups discussions, limited audience to which the data were made available etc.)

Moreover, the utilisation of publicly available data, should be also examined in the context of the 'right to be forgotten', enabling the data subjects to have their personal data erased and no longer processed, where this is no longer necessarily; the consent has been withdrawn; the processing has been objected or/and the data processing does not comply with GDPR. In order to ensure that the privacy and data protection rights of the data subjects are not violated, H2020 applicants/beneficiaries should factor in these considerations in their research proposal and confirm that the data used in the project is publicly available and can be freely used for the project purposes.

Transfer of personal data from EU to Non-EU countries

Transfer of personal data from EU to non-EU countries require special attention. Such transfer can raise ethics and legal concerns related to the level of personal data protection offered in some non-EU countries. Researchers should bear in mind that data transfers occur not only when the data is actually 'send' to third party, but also when it is accessed and processed by partners and service providers located outside of EU. Researchers should therefore check if all third party services they wish to use (e.g. survey tools, data analytics, cloud storage etc.) are based in EU or legally represented in the EU in accordance with the GDPR. If this is not the case, appropriate legally binding and enforceable agreements with partners or service providers prior to data transfers should be concluded. The latter must ensure the appropriate level of data protection (organisational and technical measures) and prevent 'onward transfer" of personal data by members of the consortium and any other recipients outside the framework of such agreements.

To comply with their ethical and legal obligations, researchers, wishing to transfer personal data from EU to non-EU country should explain in details (in their research proposal) what types of personal data will be exported and how the rights of the research participants will be

[4] According to the definition of Open Data Institute, "Open data and content can be freely used, modified, and shared **by** anyone **for** any purpose". For more information see: http://opendefinition.org/

safeguarded. They must also submit a declaration, confirming compliance with Chapter V of the GDPR.

Based on its assessment of domestic legislation and international commitments, the European Commission has granted to a number of countries the so called 'adequacy decision'. The latter means that these countries provide adequate level of personal data protection and personal data can be transferred from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. As of August 2018, these countries are Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework). Researchers who will share personal data with their partners and collaborators, outside of EU should therefore check if such data transfer is covered by adequacy decision (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en).

Transfer of personal data from non-EU countries to EU

The collection of personal data outside of EU and the existence of national law of a third country that covers such data transfer does not mean that GDPR and EU ethics principles do not apply. As a general rule, EU's ethics standards apply to all EU-funded research irrespective of where it takes place. Moreover, GDPR covers in its scope the data processing of all data controllers, based in EU, irrespectively of where the processing takes place. Researchers wishing to transfer personal data from non-EU country to EU must therefore fully comply with the ethics and legal standards, provided by GDPR. They should also ensure that they adhere to the data protection laws of the country where data is collected and submit a declaration of compliance in this regard, along with the details of the personal data to be imported to EU.

Further comprehensive information on the ethics requirement related to data processing can be found in the EC Guidance ' How to complete your ethics self-assessment', available at: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf.

The Ethics Appraisal process in Horizon Europe will be based of the current process. In applying the principles of simplification and verifiable trust, the new process will depend greatly on the local structures (ethics committees, data protection officers etc.) for further streamlining the procedures and avoiding duplication of work. Nevertheless the European Commission will enhance its adherence to the ethics principles described in article 10 of the Horizon Europe proposal by strengthening the ethics checks during the life of research projects, focusing on projects that raise serious ethics issues and concerns.