Essays

The processing of personal data in the context of scientific research. The new regime under the EU-GDPR

Maria Luisa Manis*

ABSTRACT: This Article analyses the framework of rules governing the processing of personal data for scientific research purposes established by the European Data Protection Regulation ("GDPR"). The GDPR upheld the social function of data processing in the context of scientific research and confirmed the facilitating regime with only minor changes compared to the Directive 95/46/EC. At the same time the GDPR didn't exhaustively regulate key issues of data protection in this field and ultimately left to Member States the task of reconciling the benefits to society deriving from scientific research with the participants' rights to data protection. As the EU legislator had to give up the aim to harmonize data protection rules in the context of research, only "the consistency mechanism"(which is the main institutional novelty of the GDPR) may prevent the regulatory fragmentation and legal uncertainty that the Data Protection Reform Package sought to remove.

KEYWORDS: Data protection; GDPR; scientific research; exemptions; facilitating regime

SUMMARY: 1. Introduction – 2. The Facilitating Regime for Scientific Research under the GDPR – 3. Safeguards for Data Processing in the context of Research. – 4. General Rules applying to Scientific Research – 5. Rules on Data Transfer to Non-EU Countries and International Organizations – 6. Conclusion.

1. Introduction

After over four years of preparation and debate, the long-awaited General Data Protection Regulation ("GDPR") was adopted in April 2016. [1] The GDPR is a central component of the reform package on data protection presented by the European Commission in January 2012, aimed at strengthening individuals' rights to their personal data while reducing legal uncertainty and burdens for companies and public authorities as well as adapting rules to the challenges of the

* *LL.M. in Intellectual Property (GW), mlm@mlmanis.com.* *The article was subject to a double blind peer review process.*

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88. The GDPR replaces the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995 pp. 0031 – 0050.

digital era. [2] The proposal of the Commission was accepted in ordinary legislative procedure and in March 2014 the European Parliament approved its own version of the Regulation in its first reading, which served as the basis for negotiation among the institutions. On June 2015 the Council adopted a general approach allowing the Regulation to pass to the final stage of "*trilogue*" negotiations between the representatives of the Commission, the Parliament and the Council. On 15 December 2015 a political agreement was reached in trilogue negotiations and the reform package was first adopted by the Council on 8 April 2016 and then approved by the European Parliament in plenary on 14 April 2016. The GDPR entered into force 20 days after its publication in the EU Official Journal, but it will be fully applicable only after a two-year transition period.

With full effect from 25 May of 2018, the GDPR replaces Directive 95/46/EC introducing a comprehensive framework governing any type of processing of personal data within the European Union ("EU"). As the GDPR is a regulation type of legislative act, from the set date for its full application, one single pan-European corpus of rules on data protection will have binding effect throughout the all Member States, superseding any national incompatible rule.

During the two-year transition period, Member States may enact legislation to invalidate their current rules on data protection and even to make the GDPR provisions more comprehensible to data controllers, processors and data subjects. By contrast, States don't have margin of manoeuvre to modify the provisions of the Regulation, which are mostly regulated exhaustively and intended to apply uniformly throughout the Union.

Nevertheless, the GDPR also contains a limited number of open clauses that Member States have to concretize and further specify in view of the principles and rules of the Regulation. In particular such discretion is guaranteed to National Legislators for the *Specific Processing Situations* listed in Chapter IX, which include data processing for scientific research purposes.[3]

Scientific research is considered a specific context of personal data processing as a consequence of the EU multi-level system of fundamental rights protection.[4] More specifically the EU, in the absence

[2] In 2010 the Commission presented a Communication to the European Parliament, the Council of the European Union, the Economic and Social Committee of the Regions entitled "*A comprehensive approach on personal data protection in the European Union*" which represented the Commission's basis for the proposal of a comprehensive Data Protection Reform Package including the *Proposal for a General Data Protection Regulation* 2012/0011 of 25 January 2012. In parallel with the Proposal for a General Data Protection Regulation, the Commission presented a Communication on "*Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century*" (COM/2012/09) and a *Proposal for a Directive on data processing for law enforcement purposes* (COM/2012/010). The new Directive is intended to replace the *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters* (OJ L 350, 30.12.2008 pp.60-71).

[3] Specific processing situations' list (Chapter IX of the GDPR) includes: Processing and freedom of expression and information (Article 85); Processing and public access to official documents (Article 86); Processing of the national identification number (Article 87); Processing in the context of employment (Article 88); Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89); Obligations of secrecy (Article 90); Existing data protection rules of churches and religious associations (Article 91).

[4] See generally G. Di Federico, *Fundamental Rights in the EU: Legal Pluralism and Multi-level Protection After the Lisbon Treaty*, in D. Giacomo (eds), *The EU Charter of Fundamental Rights. Ius Gentium: Comparative Perspective on Law and Justice*, Dordrecht, 2011,vol. 8, pp. 15-54.

ISSN 2284-4503

of a formal constitution, can only operate within the authority delegated by the treaties between the constituting Member States. The *Treaty on the Functioning of the European Union* ("TFEU") gives express mandate to the EU to lay down the rules on data protection only with respect to the processing of personal data by those institutions and/or regarding those activities that fall within the scope of the EU Law (Article 16.2 TFEU). [5] However, Title XIX of TFEU makes it clear that in the field of scientific research the Union has only a competence within the meaning of Article 6 of the TFEU, consisting in supporting, coordinating and supplementing the actions of Member States. It follows that EU is not granted the power to intervene in place of States in the field of research, and thus it cannot even adopt legally binding acts to harmonize legislation of Member States.

Due to this distribution of legislative competences, the GDPR framework of data protection rules in the context of scientific research is mainly composed of open clauses to be further implemented by the States of the European Union.

A peculiar feature of data processing in the context of research is also that intrinsic conflict between two fundamental rights: the right to the protection of the personal data and the right to academic and scientific research freedom. The *EU Charter of Fundamental Rights* recognizes both these rights respectively in Article 8 and Article 13 and requires the EU to balance and reconcile them in its actions, decisions or legislation, in accordance with the principle of proportionality.[6] In consideration of the relevant social benefits deriving from scientific research activities and the utmost importance of facilitating accessibility to and processing of personal data to researchers, Directive 95/46/EC had established for scientific research a series of exemptions from general data protection rules. Exemptions contained in the Directive have been implemented by Member States according to divergent interpretations and applied not uniformly through the EU, but nevertheless served to avoid excessive administrative burden for an activity, such as research, that heavily depends on a relative free access and use of datasets that include personal data.[7]

During the prolonged trilogue between the European Commission, Parliament and Council on the text of the GDPR, scientific research provisions have been subject to an intense debate, in particular

[5] *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union*, OJ C 326, 26.10.2012 pp. 0001-0390.

[6] *Charter of Fundamental Rights of the European Union*, OJ C 326, 26.10.2012, pp. 391–407. The inclusion of an independent Right to Data Protection (in addition to the Right to Privacy) is a peculiarity of the EU Charter since other International Human Rights Documents consider the Right to Data protection as a subset of the Right to Privacy. Moreover, within the EU Charter, Article 8 is particularly detailed compared to other rights of the Charter, such as the right to academic freedom for example. For an analysis of Article 8 of the EU Charter see generally: G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, in *International Data Privacy Law,* Vol. 5, Issue 1, 2015, pp. 91–94; O. LYNSKEY, *Deconstructing Data Protection: the "Added Value" of a right to data protection in the EU Legal Order,* in *International&Comparative Law Quarterly BICL*, Vol.63 Issue 3, 2014, pp.569-597. On the Principle of Proportionality and its application in the EU, see generally W. SAUTER, *Proportionality in EU Law: A Balancing Act?*, TILEC Discussion Paper, 003, 2013, available at SSRN: https://ssrn.com/abstract=2208467 (last visited 26/10/2017).

[7] On EU Member States implementation of Directive 95/46 see Footnote 23.

after the LIBE amendments.[8] The first proposal of the Commission had confirmed the facilitating regime, but its legacy has been re-examined by the LIBE in light of the announced aim of the Reform Package to strengthen data subjects' rights. Eventually the facilitating regime for scientific research was maintained and incorporated without relevant changes from what established by the Directive. At the same time the EU legislator had to renounce to level up the data protection rules in the field of Scientific Research, and the provisions are drafted in the form of open clauses to be further implemented by each Member State.

Ultimately, the task of reconciling the benefits to society deriving from scientific research with a framework of adequate safeguards for the research participants has been devolved to national legislators and national supervisory authorities. In particular, the GDPR directs data protection regulators at all levels to encourage the development of code of conducts to assist with the regulation proper application. Thus, in the next months, national legislators and supervisory authorities will be working together with research organizations and relevant stakeholders to implement the scientific research regime. In Member States' implementing legislations, or in the national code of conduct for scientific research, the GDPR provisions should be specified sufficiently to ensure that all relevant factors are taken into consideration, such as the specific aspects of individual consent in the context of scientific research, the needs of different research fields, the types of data processed, the risks for research participants as well as the social relevance of the scientific purpose pursued through the processing.[9]

2. The Facilitating Regime for Scientific Research under the GDPR

The main provision of GDPR scientific research regime is represented by Article 89. The first paragraph of Article 89 acknowledges that controllers may process data for scientific research purposes subject to appropriate safeguards being in place and lays down some criteria for the implementation of such safeguards. The first paragraph of Article 89 will be further discussed in paragraph 3 of this paper. The second paragraph of Article 89 introduces the facilitating regime for scientific research and lists a series of derogations from general data subjects rights referred to in Articles 15, 16,18 and

[8] In the Parliament the LIBE (the Civil Liberties, Justice and Home Affairs committee of the European Parliament) was assigned the task of formulating the Parliament's amendments. The first draft by the Chairman of the LIBE was criticized for insufficient consideration to the needs of research. On 22 October 2013, after a long period of negotiations and intense lobbying efforts, the LIBE voted on its final amendments to the Commission's proposal but despite some improvements, the overall outcome has been considered disappointing from research organizations perspective; e.g. O. NYRÉN, M. STENBECK AND H. GRÖNBERG, *The European Parliament proposal for the new EU General Data Protection Regulation may severely restrict European epidemiological research*, in *European Journal of Epidemiology*, 29 (4), 2014, pp.227-230; M.G. HANSSON, G.J.V. OMMEN, R. CHADWICK, J. DILLNER, *Patients would benefit from simplified ethical review and consent procedure*, in *Lancet Oncol*., 14(6), 2013 May, p. 451. Science Europe, *Opinion on the Benefits of Personal Data Processing for Medical Sciences in the context of Protection of Patient Privacy and Safety*, May 2013, www.scienceeurope.org. (last visited 26/10/2017); E.B. VAN VEEN, *GDPR facts and comments; LIBE and research*, MedLawConsult, The Hague, February 2013, available at www.medlaw.nl (last visited 26/10/2017).

[9] The drafting and approval of a code of conduct for processing for the purpose of scientific research is not mandatory, but up to Member States. Moreover Member States are not bound by the GDPR to implement the facilitating regime up to a certain degree of detail, nothing prevents Member States to maintain the same wording and open clauses of the GDPR provisions.

21. These derogations can, but don't have to, be provided by Member States or Union law. By contrast Article 21 and Article 17 contain two directly imposed exemptions, which only have to be implemented by Member or Union law. In other articles (such as Articles 1, 5, 9, 15, 17, 21), which contain provisions of general application, a clause has been added to provide an exemption for processing for scientific research purposes.

Each of the GDPR exemptions provisions specifies that the exemption can be implemented as far as appropriate safeguards are implemented for the rights and freedom of data subjects in accordance with paragraph 1 of the Article 89. Furthermore according to Recital 159 «where personal data are processed for scientific research purposes, this Regulation should also apply to that processing », and thus we need to investigate if the provisions of general application, for which no exemption is provided, apply also to processing for scientific research purposes.

In the following paragraphs of this paper we will be analysing the exemptions for scientific research and their scope of application, since the GDPR doesn't define the "scientific research purposes" in its text with sufficient precision. However, it should be clear that GDPR provisions for scientific research apply also to data processing for historical research and statistical research, which are not discussed in this paper. Furthermore when we will be mentioning processing of "data", we refer to personal data. Indeed processing of anonymous information, «including for statistical or research purposes», is outside the scope of application of the GDPR. By contrast, personal data which have undergone pseudonymisation are still considered personal data if they «could be attributed to a natural person by the use of additional information» and thus they fall under the application of the GDPR (Recital 26).[10]

2.1. Rules on Consent, Notice, and Data Storage

Article 5 of the GDPR lists core principles applying to any personal data processing providing that: personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (*Principle of lawfulness, fairness and transparency*); collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (*Principle of purpose limitation*); adequate, relevant and limited to what is necessary in relation to the purpose for which they are collected (*Principle of Data Minimization*); kept accurate and when necessary updated (*Principle of Accuracy*); kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed (*Principle of Storage Limitation*); processed in a manner that ensure appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (*Principle of integrity and confidentiality*).

The obligation on organizations to have a lawful basis in respect of each processing activity is essentially unchanged compared with Directive 95/46. Personal data may be processed only if, and to the extent that, at least one lawful basis applies. Article 6 of the GDPR provides for a series of alternative

[10] Paragraph 2 of this Paper discusses the GDPR test for establishing when pseudonymisation data can qualify as truly anonymised data.

legal grounds, but the *consent of the data subject* to the processing of his or her personal data remains the most common and of general application ground, being the others exceptional.[11]
Moreover the data subject should be provided with a series of information on the processing, especially on the purpose of the processing, in order to give his or her consent. [12] A combined reading of principles of lawfulness, transparency and of purpose limitation shows that personal data cannot be collected for general purposes: data subject should be properly informed of the purpose of the processing and his or her consent has a legal effect limited to that purpose. It follows that when data already collected need to be further processed for a different purpose the data subject has to give a new consent. [13]
As alternative to "re-consent", Article 6.4 permits data controllers to perform a compatibility test to ascertain whether processing for another purpose is compatible with the previous purpose for which personal data were collected.[14] Where the further processing purposes are compatible, then no additional consent (or any other separate legal basis) shall be required. More precisely, in order to lawfully "re-processing" without "re-consenting" both the following conditions should be met: (a) the original processing complied with all requirements for its lawfulness and (b) the compatibility test confirms that the purposes of original processing and those of secondary processing are compatible.
The compatibility test requires the controller to consider several factors including *inter alia* « any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of ap-

[11] In addition to the consent of the data subject, Article 6 paragraph 1 considers other legal grounds for processing such as when « (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the purpose of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular when the data subject is a child. ». An extensive work on the rule and concept of "consent" within the European data protection law before the adoption of the GDPR is contained in the work of E. KOSTA, *Consent in European data protection law*, Leiden, 2013.
[12] Article 12,13 and 14 of the GDPR regulate data controller's notice duties.
[13] Rules on consent and on the legal bases for processing, which represent a concretization of the Principle of Lawfulness of Processing, are contained in Article 6. The Principle of Purpose Limitation has been deeply analyzed by the *Opinion 03/2013* on purpose limitation adopted by the Article 29 Data Protection Working Party the 2 April 2013. The Article 29 Data Protection Working Party ("WP29") was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of the Directive 95/36 and Article 15 of Directive 2002/58/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonized policies for data protection in the EU Member States. Under the GDPR the WP29, whose members were the EU's national supervisory authorities, the European Data Protection Supervisor ("EDPS") and the European Commission, has been transformed into the European Data Protection Board ("EDPB"), with similar membership but an independent Secretariat.
[14] The compatibility test is detailed in paragraph 4 of Article 6 of the GDPR.

propriate safeguards in both the original and intended further processing operations » (Recital 50 and Article 6.4).

This compatibility test can be waived if the further processing is made for scientific research purposes. Indeed the purpose of scientific research won't be considered to be incompatible with the initial purpose by law (Article 5.1 b). Such provision is especially relevant if we consider that in case of further processing necessary for the performance of a task carried out in the public interest (or in the exercise of official authority vested in the controller) a presumption of compatibility can be established only by Union or Member State law (Article 6.3 and 6.4). By contrast, in case of re-processing for scientific research purposes, the presumption is provided by the GDPR itself as harmonized rule applying through all the Union.[15]

The rationale behind this presumption is to provide researchers and research organizations with a certain freedom to re-examine dataset collected or processed in the context of a previous scientific projects.[16] Science, either basic or applied science, is an incremental process and replication and longitudinal studies are fundamental for its progress. In scientific research routinely collected data may subsequently prove to be useful for a research study or hypothesis that couldn't be forecasted at the time of the collection. In addition to these intrinsic needs, which are at the heart of the scientific inquiry, the re-use of dataset is also strongly promoted by several *data-sharing* policies, which expressly require that researchers share their research outcomes, including collected datasets.[17]

The same reasoning is likely to have motivated the EU legislator to use wordings that seems to validate the practice of "broad consent" in scientific research. Indeed Recital 33 of the GDPR recognizes that research participants «should be allowed to give their consent to certain areas of scientific re-

[15] Only in appearance this exemption is something new compared to the Directive 95/46. Indeed essentially both GDPR and the Directive allows further processing for scientific research purposes without need for re-consent if Member States furnish adequate safeguards.

[16] Most of the bioethics studies regarding data protection rules in the field of research have often captured the view of patients and research participants, while focusing less on the perspective of the researchers. One of the most important merits of the debate preceding the GDPR adoption is that highlighted the opinions of the scientific communities as well and its concerns towards general consent models and strict rules on informed consent. See for a scientists' perspective on consent Z.MASTER, L.CAMPO-ENGELSTEIN, T. CAULFIELD, *Scientists' perspective on consent of biobanking research*, in *European Journal of Human Genetics*, 23, 2015, p. 569-574.

[17] Data sharing policies have been adopted by several Universities in Europe. The duty of sharing datasets (which are the outcome of a research project) is considered as a subset of the wider duty of dissemination. The *European Regulation No 1290/2013 of the European Parliament and of the Council* (OJ L 347 20/12/2013 pp. 81-103) laying down the rules for participation and dissemination in Horizon 2020, clarifies how dissemination cannot be limited to the publishing of academic papers, but it may include the sharing of the dataset collected as a result of the research project, in particular when the research project is publicly funded such as projects financed under the Horizon 2020 Program. At the same time it highlights the implication of such data sharing practices with the rules on data protection and thus it requires participants to draft a data management plan to illustrate how the participants will comply with the duties of dissemination and to individuate possible data protection issues. On the duty of dissemination see generally P.M.WILSON, M. PETTICREW, M. W. CALNAN, I. NAZARETH, *Disseminating research findings: what should researchers do? A systematic scoping review of conceptual frameworks*, in *Implementation Science*, 5:91, 2010; A.B. MCVAY, K. A. STAMATAKIS, J. A. JACOBS, R. G. TABAK, AND R. C. BROWNSON, *The role of researchers in disseminating evidence to public health practice settings: a cross-sectional study, Health Research Policy, 2016, 14:42.*

search». Broad consent is not however blanket consent. Rather its concept represents the idea that compliance to the principle of lawfulness, purpose limitation and transparency may be "granular" or "scalable" and that a standard single model of fully informed and specific consent is not practicable and even harmful in the field of research. [18] The practice of "broad consent" in scientific research has been applied in Member States in a very divergent way over the past years. The problem with certain broad or open consent practices is that they substitute the right-based approach that traditionally characterizes data protection compliance in EU, with a «strong harm-based approach» that has not been validated by the GDPR. The GDPR indeed sets a system of limited exemptions from general rules on consent for scientific research; these exemptions apply to the extent that a legislative framework is in place, which specifies conditions and circumstances for their application as well as adequate safeguards for research participants. The GDPR doesn't seem to endorse a case-by-case approach where controllers' compliance to rules on consent can be scalable depending on the degree of risk associated with a specific study or the degree of relevancy or social benefit of the scientific research outcomes. [19]

[18] M.SHEEHAN, *Can broad consent be informed consent?,* in *Public Health Ethics*, 4 (3), 2011 Nov., pp. 226-235; D.HALLINAN, M. FRIEDEWALD, *Open Consent, bio-banking and data protection law: can open consent be "informed" under the forthcoming data protection regulation*?, 2015, in *Life Science Society Policy*, available at www.ncbi.nlm.nih.gov/pubmed/26085311 (last visited 26/10/2017). M.G. HANSSON, G.J.V. OMMEN, R. CHADWICK, J. DILLNER, *op.cit.*, p. 451, the Authors, commenting on the LIBE amendments to the GDPR text and expressing criticism over the proposal that scientific research should not be exempt from strict requirements of specific consent by research participants, states that the LIBE amendments are an «example of how the regulatory framework for the protection of the human research participants seems not to keep pace with development in biomedical research. If the proposed change is implemented, it will have serious consequences for medical research and for patients in need of improved treatment. Epidemiological clinical and lifestyle research that make uses of registries and bio-banks have expanded rapidly in the past 15 years. Studies often depend on the collaboration of international networks, such that research crosses the borders of national regulations. Survey and interview-based studies that carry minimal risks to participants might not need the same degree of oversight by ethical committees as interventional research». It added that «Published accounts and surveys of patients, scientists, and the general public have also suggested that many people believe that observational research should not have the same need for detailed informed consent as is required for more interventional studies with greatest risk»; it also suggests to take as example the proposal of United States Department of Health and Human Services «for a risk based review system for the protection of the research participants of great interest», «the central contention of the proposal is that the ethical review system should take into account the degree of risk associated with a specific study».

[19] See WP29 Opinion 2014 on *Statement on the role of a risk-based approach in data protection legal frameworks*, WP 218 Adopted on 30 May 2014. Legislators called up to implement the scientific research regime may take into account the degree of risks posed by categories of processing to the research to regulate them accordingly (and establishing stricter requirements). This is clearly implied in Article 9.2.j, for research that processes sensitive data. However it is not clear the significance of the assessment of the risks by controllers within the GDPR. We may consider the risk-based approach enshrined by the GDPR not as an assessment intended to furnish a motivation to controllers for possible failures of compliance, but to permit controllers to assess their compliance risk (this is the position of WP29) and also to establish additional safeguards for the protection of the data subjects. According to Gellert, the risk-based approach enshrined by the GDPR doesn't conflict with the right-based approach that is intrinsic to the fundamental right' nature of the data protection; it is rather a different model of compliance approach, R. GELLERT, *Why the GDPR risk-based approach is about compliance risk, and why it's not a bad thing*, in Schweighofer, Kummer, Sorge (eds), *Trends and Communities of legal informatics: IRIS 2017- Proceedings of the 20th International Legal Informatics Symposium*, 2017, pp. 527-532. However it has not yet investigated whether a

Nevertheless, the GDPR permits further processing for scientific research purposes without need of obtaining re-consent. Moreover, as a consequence of the presumption of compatibility pursuant to Article 5.1 b, also the principle of storage limitation is mitigated, in the sense that personal data can be retained beyond the time necessary to achieve the research purpose for which they are collected and/or processed (Article 5.1 e). The only condition is that appropriate safeguards are implemented in accordance with Article 89(1), which includes pseudonymisation of such data. Among these safeguards, compliance with the principle of transparency remains particularly relevant in research. Transparency means first of all that data subjects should be informed of processing activities that concerns their personal data; even in those cases where the consent requirement can be waived by researchers, the notice duties should not be waived except in certain specific circumstances.

Controllers' notice duties are detailed by Articles 12, 13 and 14 that also indicate the type of information that must be communicated to the data subject. Notice should always be provided before the collection or processing (including further processing) and it can be done in writing, by electronic means and in some cases also orally. The GDPR distinguishes the type of information to be provided to the data subject depending on whether data were collected from the data subject (Article 13) or they were not obtained from the data subject (Article 14). In addition, the GDPR distinguishes the notice to be provided before the first collection from the update notice (Articles 13.1, 13.2, 14.1, 14.2). The updated notice is the notice to be given before the further processing of the data (Articles 13. 3 and 14.4).

Information contained in the notice provided before the first collection include identity and contact information of the controller, intended purposes for the collection and/or processing activities, notice of the data subject rights, and, when applicable, indication whether the data will be subject to a transfer to a third country. The updated notice, in addition to the information required for the first notice, should contain indication of the new research purposes.

In limited circumstances the notice requirement can be waived by research organizations. Pursuant to Article 14.5 (b), when data have not been obtained by the research participant, researchers and research organizations can be exempted from notice duties when providing such information proves impossible or it would require a disproportionate effort. In these cases, on the condition that adequate safeguards are provided pursuant to Article 89.1, the controller should also take « appropriate measures to protect the data subject's rights and freedom and legitimate interests, including making the information publicly available». Similar principles and rules applied under the Directive 95/46, and some national code of conducts further specified the conditions upon which the notice may be deferred or even totally omitted and substituted by alternative forms of publicity. [20]

---

different interpretation of the risk-based approach may be valid for scientific research, given the margin of manoeuvre left to National Legislator to adapt the open clauses of the facilitating regime. The Risk based approach in the field of research is further discussed in paragraph 4 and footnote 61 of this Paper.

[20] See Article 6(1)(b) of the Directive 95/46/EC. Implementation of Article 6 of the Directive by the *Italian Code of Conduct for Data Processing for Research and Statistical Purpose* for example clarifies that information notice is obligatory, but can be deferred when this is necessary to achieve the objective of the survey and it can be totally omitted only in limited cases. Alternative forms of publicity are listed. See Article 6 of *Italian Code of*

Implementation under the Directive has shown that there can be ethical, organizational or methodological reasons that make it impossible or excessively difficult to comply with duties of notice in scientific research.
It's notable that this is an area where ethical principles and rules of law may be conflicting. For example in the context of medical research, providing notice on further processing to a data subject who ignores his or her medical condition may cause a material or psychological damage.
All these situations will need to be further regulated and specified by implementing legislation to make sure that notice is omitted only if it is strictly necessary. In particular it has to be clarified when providing notice is impossible or too difficult for researchers and when ethical considerations suggest to exempt researchers from this duty.

2.2. Scientific Research as Lawful Basis for Processing

As a general rule any personal data processing must have a lawful basis. Article 6 of the GDPR lists all possible legal grounds for processing, the most relevant and of widest application being that the «data subject has given his consent to the processing of his or her personal data for one or more specific purposes» (Article 6.1. a).
Another legal ground for processing is that « the processing is necessary for the legitimate interest pursued by the controller or by a third party except, where such interests are overridden by the interests or fundamental rights and freedom of data subjects» (Article 6.1. f).
As we discussed in the previous paragraph, scientific research purposes can be a lawful basis, under certain conditions (consisting in the appropriate safeguards set by article 89.1), for further processing personal data that have been initially lawfully collected or processed. The GDPR, by contrast, doesn't clarify if the same scientific purposes can also be a lawful basis for initial processing or collection of personal data. Scientific purposes however can qualify as legitimate interests within the meaning of letter f of Article 6.1.
This interpretation is supported by an Opinion of Article 29 Working Party ("WP29") of 2014 [21] which is still valid, since rules on lawful basis for processing of personal data contained in Directive 96/45 are only moved to a different article of the GDPR, but they haven't been changed.[22] According to the WP29, to ascertain that this ground for processing can operate the legitimate interest of the controller, or of any third parties to whom the data are disclosed, should be balanced against the interests or fundamental rights of the data subject. More in detail, WP29 specifies: « This assessment is not a straightforward balancing test consisting merely of weighting two easily quantifiable and comparable 'weights' against each other. Rather, the test requires full consideration of a number of factors, so as to ensure that the interests and fundamental rights of data subjects are duly taken into account. At the same time it is scalable which can vary from simple to complex and need not be unduly burden-

Conduct for Data Processing for Research and Statistical Purposes, O.J. no. 190 of August 14, 2004 [En Version doc. web. n. 1115480].
[21] WP29 Opinion 6/2014 on the notion and application of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted the 9 April 2014.
[22] Legal grounds for processing of personal data were contained in Article 7 of the Directive, now in Article 6 of the GDPR.

some ». Among the factors to be considered when carrying out the balancing test, the WP29 listed the following:
- 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.
Moreover the WP29 explicitly indicates the processing for research purposes (including marketing research) as one of the most common contexts in which the issue of legitimate interest in the meaning of this provision may arise.
Under the Directive 95/46, a lack of harmonized interpretation of this provision has led to divergent applications in Member States. In some Member States, like Italy, the balance test pursuant to Article 7(f) of the Directive has been applied in cases specified by the Data Protection Authority ("Garante"), including for initial processing for scientific research. In particular processing for scientific research purposes has been considered lawful based on a general authorization of the Authority that also establishes specific circumstances, conditions and safeguards. Under the Finnish law controllers need to obtain a permit from the Authority if they wish to rely on that test, but the law also provides four special cases, which can be said to be specific examples of the application of that test. [23]
Under the GDPR, a Union or National Law should be laid down to implement the legal ground for processing represented by processing necessary for the performance of a public task in the public interest [24]. By contrast there is no express reference to an implementing law with respect to the legal ground pursuant to letter f of the first paragraph of Article 6, represented by the legitimate interest.

[23] In Finland a controller may apply for permission from the Data Protection Board to process personal data where it considers that it has a legitimate interest to do so, but there are no other legal grounds for such processing. Unlike the laws of several other EU member states, the Personal Data Act does not recognize the legitimate interest of the controller or a third party as a direct ground for allowing the processing of personal data. A detailed overview of different implementation of Article 7(f) of the Directive by EU Member States can be found in D. KORFF, *EC Study on Implementation of Data Protection Directive, Comparative Summary of national laws*, Study Contract ETD/2001/B5 3001/A/49), Human Rights Center, University of Essex (Colchester 2002). According to the Author, the legitimate interest ground and the balance criterion (in general and not specifically in the context of scientific research) have been applied more restrictively by Greece, Spain, Italy and Finland compared to other Member States such as Belgium, Denmark, France, Luxembourg, Netherlands, Portugal, Sweden and UK. The latter group of States' legislations contain the "balance" criterion in identical or similar wording of the Directive (as open clause), without subjecting it to further formal requirements. German Law allows a balance test in the same general terms of the Directive only in the private sector, while it contains a series of different more strict balance tests for processing in the public sector.
[24] With respect to the lawful basis for processing set by letter e, paragraph 2 of Article 6 (which is the «processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller»), in paragraph 3 of Article 6 it is added that: «The basis for the processing referred to in point e) shall be laid down by Union Law or Member State law to which the controller is subject». And this law may contain specific provisions to adapt the application of this rule of the GDPR in consideration

The GDPR refers to the legitimate interest as legal basis for processing in Recital 47 where the test of the mentioned WP29 Opinion is synthetized and some examples of legitimate interest are provided (for example « direct marketing purposes may be regarded as legitimate interest»). Additionally Article 35.7 (a) and Recital 69 incorporated the suggestion of WP29 to require the controller to prove that he or she performed an assessment to evaluate that his or her legitimate interest is not overridden by the data subjects' interests, fundamental rights and freedoms.[25] This assessment is now included as a part of the "Data Protection Impact Assessment" pursuant to Article 35.7 (a).[26]

2.3. The Data concerning health, genetic and biometric data processed for Scientific Research Purposes

The GDPR maintains the distinction between ordinary personal data and sensitive personal data as well as the general prohibition to process sensitive data except for certain enumerated cases.
Sensitive data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data, biometric data and data concerning health or a natural person's sex life or sexual orientation. All these categories of data share the characteristic of being particularly sensitive in relation to fundamental rights and freedoms, and therefore they deserve specific protection as the context of their processing could create significant risks for the data subjects (Article 9.1. and Recital 51).
New definitions have been introduced for Data Concerning Health, Genetic Data and Biometric data, which are relevant in this paper as being personal data that can be processed in the context of medical research and other branches of scientific research. "*Data Concerning Health*" are «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» (Article 4 n.15); "*Genetic Data*" « means 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» (Article 4 n.13); "*Biometric Data*" « means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or

of many circumstances «including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX».

[25] The WP29, in its *Opinion 01/2012* of 23 March 2012 and *Opinion 08/2012* of 5 October 2012 which were released during the debate for the preparation of the GDPR, recommended adding to the Proposed Regulation a specific requirement for data controllers to explain to data subjects why they believe their interests would not be overridden by the data subjects' interests, fundamental rights and freedoms. Also, upon request, data controllers should have made available to data protection authorities the documentation upon which they based the assessment they have conducted before using "*legitimate interests*" as the grounds for processing personal data.

[26] The Data Protection Impact Assessment ("DPIA") regulated by Article 35 and 36 is an assessment of the impact of the processing operations that controllers have to carry out prior to the processing operations, where the processing (because of the use of new technology, or for the nature, scope, context and purpose of the processing) is likely to result in a high risk to the rights and freedom of the data subjects. See Paragraph 4 of this Paper for a discussion on the DPIA in the field of research.

confirm the unique identification of that natural person, such as facial images or dactyloscopic data» (Article 4 n.14).

In general, the processing of sensitive data is prohibited unless the data subject has given explicit consent (Article 9.2. a) or these data were manifestly made public by the data subject (Article 9.2. e). Other exceptions from the prohibition include the processing for specific relevant purposes of public interest (See Article 9.2. b, c, d, f, g, h and i) and the processing for scientific research purposes as well (Article 9.2. j).

In particular, processing of sensitive data for scientific research purposes should be made «in accordance with Art 89 (1)» and «based on an 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 interest of the data subject"» (Article 9.2. j).

Scientific research that processes health data or genetic or biometric data is a subset of scientific research, and so it falls into the scope of the facilitating regime. However, since it processes sensitive data, additional safeguards will need to be implemented to ensure a higher level of protection for research participants. This can be implied by Recital 159 of the GDPR according to which «If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures». Furthermore Article 9.4, although it doesn't specifically address scientific research, states that « Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic, biometric data and data concerning health ».

The GDPR makes clear that processing of sensitive data for research purposes should be based on an Union or Member State law, but leaves a wide margin of discretion to those called up to implement the regime. Additional safeguards, for the processing of sensitive data, should be implemented by Member States in consideration of the risk posed to freedoms of research participants as well of the benefits of research for society. Medical research produces high and relevant social benefits and thus sensitive data gain a "collective" value when processed for purpose of medical research. Therefore, while health-related data are in general considered to expose research participants to a higher risk, such risk should be evaluated by national legislators and weighted against the level of relevancy of the scientific purpose pursued through the processing.

Furthermore, the robustness of the technology and the security of the environment in which the processing takes place should also be taken into consideration. Therefore, while seeking the research participant's consent should be always be the standard, when sufficient safeguards are implemented and consent cannot be obtained, the processing should be permitted without consent either for first processing, based on the legitimate interest of the controller pursuant to Article 6.1 f), or for further processing based on the presumption upon to Article 5.1 b).[27]

[27] The assumption that further processing of sensitive data can be lawful for purposes of scientific research can be implied by Article 6.4, which indicates the factors to be considered to determine the compatibility between the first lawful processing and the further processing. Indeed among these factors Article 6.4 includes «the nature of the personal data, in particular whether special categories of personal data are processed pursuant to Article 9». However there is no explicit indication in the GDPR that the presumption of compatibility upon to Article 5.1 letter b (regarding further processing for scientific research purposes) applies also when the further

Years of application of the Directive 95 in these research fields have shown that there may be many situations when the rule of informed and explicit consent is not feasible. [28] For example in emergency care research, many subjects are physically unable to give their consent; studies where a very large sample size is needed for obtaining robust result, which makes it practically impossible to seek specific, explicit and informed consent from all participants; studies in which asking to the patient his or her consent to further process his or her sensitive data would be contrary to the ethic and deontology rules or even inappropriate. Asking researchers to renounce and erase those sensitive data (with respect to which they couldn't obtain explicit consent) would introduce bias and invalidate the research outcomes. Therefore the "collective" function of these sensitive data should be always properly evaluated together with the risks for research participants. Emphasis should be placed more on transparency of the research processing operations and on how safety and confidentiality of data can be assured within the research domain. [29]

All the GDPR exemptions we discussed in the previous paragraphs (including rules on data storage and notice) should be adapted to fit to these specific sets of research. It is quite noticeable how the EU legislator has renounced to establish harmonized rules in this field and left the task of reconciling the opposite interests to Member States. A key issue is also whether national implementing legislation will opt to detail the research provisions to fit all the different cases, fields of research and types of data or by contrast they will delegate this task to the ethics committees. [30]

Despite this lack of guidance for medical research, the GDPR may have an immediate impact on certain scientific projects related to bio-banking which have been relying on a widest interpretation of the concept of anonymous data. Indeed, as we will discuss in paragraph 3 of this paper, GDPR definition of anonymised data doesn't encompass certain cases of pseudonymised data that under the Directive were considered to be anonymised in certain Member States.[31]Thus, there are fewer chances to escape the application of the data protection and certain bio-banking activities may now fall within the scope of the GDPR and its rules on consent.

---

processing concerns sensitive data. Moreover pursuant to Article 9.2 j processing of sensitive data for research purposes should be based on a Law of States or Union 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 for safeguard the fundamental rights and the interests of the data subject ».

[28] See Science Europe, *Opinion on the Benefits of Personal Data Processing for Medical Sciences in the context of Protection of Patient Privacy and Safety*, *op. cit., p.6,* here a number of cases are discussed where it is not possible to seek consent from study participants in the context of medical research.

[29] E.B. VAN VEEN, *GDPR facts and comments; LIBE and research*, *op.cit*., p.1; see also M.G. HANSSON, G.J.V. OMMEN, R. CHADWICK, J. DILLNER, *op.cit.,* p. 451.

[30] We may expect that those Member States that implemented the Directive 95 research provisions with the adoption of a code of conduct or detailed the requirements and safeguards in their implementing legislation, will be working on the adoption of new codes of conducts to detail the rules and requirements (leaving no or limited room for a case-by-case approach with research ethics committees playing a prominent role).

[31] See for UK, M. M. RUMBOLD AND B. PIERSCIONEK, *The effect of the General Data Protection on Medical Research*, in *J Med Internet Res*, Vol.19, No 2, Feb. 2017, e 47; see also E.B. VAN VEEN, *GDPR facts and comments; LIBE and research*, cit., p. 4.

2.4. Research Participants' Rights to the processing of their personal data

One of the key features of the GDPR is the strengthening of data subjects rights. These rights have been updated and some novelties have been introduced (such as the *right to erasure*) to ensure that data subjects have effective means to regain control over their personal data. Data protection laws exist because it is believed that, without them, technology would enable or cause data controllers and processors to violate fundamental rights and freedoms. But data protection must deal with constant technological changes, which have the effect to make them obsolete, purely formal and thus inadequate to protect data subjects' freedoms. The data protection rules developed at national level in the 1970s and then harmonized within the European Union by Directive 95/46/EC were a response to technological development of the 1960s and 1970s.[32] In the same way GDPR has been enacted because, due to the technology advances occurred after the 1995, the Directive had overridden individuals' rights.

It is interesting to notice how the progressive consolidation of the rights to personal data protection, from the *Convention for the Protection of Human Rights and Fundamental Freedoms of 1950* to the current rules on data protections had the effect to make the duties of confidentiality of researchers, deriving from the professional ethics, as an inadequate and insufficient protection. From the perspective of the research participants, there can't be a control over their personal data if they don't have rights over they data and transparency about what is happening to their data. From the perspective of researchers detailed data protection rules and data subjects' rights are an excessive administrative burden in an area, such as scientific research, which is already high regulated.[33]

In order to reconcile the two opposite interests, the GDPR acknowledges that in certain cases data subjects rights may render impossible or seriously impair the achievement of relevant scientific purposes and sets two exemptions from the rights of erasure and right to object. Additionally the GDPR gives Member States discretion to introduce further exemptions from another series of data subjects rights.

With respect to the two directly provided exemptions, these concern the right to erasure (Art 17) and the right to object (Article 21).

The right to erasure (or "right to be forgotten") consists in the right to obtain that the controller erases personal data without undue delay when the personal data are no longer necessary for the purpose for which they were collected and other relevant cases, including when they were unlawfully collected.[34] The exercise of this right can be a serious threat for the integrity and the value of research datasets, in particular when the erasure is requested on the ground that data are no longer necessary for the purpose for which they were collected. Indeed, in the research context, Article 5.1

[32] *Council of Europe Recommendation 509 on Human Rights and Modern scientific and technological development* (31 January 1968) which analyses the risks posed by the technology development of 1960s to privacy.

[33] These two conflicting perspectives are reflected in the current opposition between a right-based approach to data protection (the traditional compliance approach) and an harm-based approach (which calls for the scalability of the legal requirements of data protection) the latter being championed by the research communities. See for the researchers' perspective Z. MASTER, L. CAMPO-ENGELSTEIN, T. CAULFIELD, *Scientists' perspective on consent of biobanking research*, *op.cit.*, pp. 569-574.

[34] See generally A. MANTELERO, *The EU Proposal for a General Data Protection Regulation and the roots of the "right to be forgotten",* in *Computer Law & Security Review*, 2013, Vol. 29/3, pp. 229-235.

letter e) and Article 5.1 letter b) allow controllers, under certain circumstances and given appropriate safeguards, to retain the data for longer and also to further process the data for a different scientific purposes. Accordingly Article 17.3.e provides that the right to erasure doesn't apply when it is «likely to render impossible or seriously impair the achievement of the objectives of the processing».

The second directly provided exemption of the GDPR relates to the right to object (Article 21). As a general rule when the data subject objects to the processing, then the controller cannot longer process the data, unless the controller can demonstrate that his or her compelling interests to process data override the data subjects interests (Article 21.1). [35]

The right to object can be exercised against processing of data or profiling based on legal grounds set by letters e) and f) of Article 6.1[36]. Also in the context of research, the right to object can be exercised by the research participant against the processing of his or her data for scientific purposes, but if the processing is «necessary for the performance of a task carried out of public interest », the research interest prevails and the controller can reject the data subject request (Article 21.6).

The scope of application of the exemption set by Article 21.6 is particularly limited. Indeed not all research projects can qualify *as necessary for a task of public interest*. So, instead of facilitating research, this provision even broadens the scope of research participants' right to object. On the other hand Article 89.2 provides additional legal basis for an exemption from the right to object with a wider scope than Article 21.6.

Paragraph 2 of Article 89 states that Union and Member State Law may provide for derogation from the rights to object, the right to access, the right to rectification and the right to restriction of processing. These rights are regulated by correspondent Article 21,15, 16 and 18 of the GDPR. [37] It's notable that the Union or Member State Law don't have to, but they « may » provide these exemptions. Moreover Article 89.2 doesn't give blanket authority to derogate from these rights, since derogations can be implemented as far as adequate safeguards referred to paragraph 1 of Article 89 are provided and in so far as such rights are « likely to render impossible or seriously impair the achievement» of the scientific specific purposes and such derogation is necessary for the fulfillment of those purposes.

In conclusion, despite exemptions set by Article 17.3.e) and Article 21.1 are directly imposed by the GDPR, the codes of conduct or the same implementing law may opt to specify when the request to

[35] Art 21.1 permits controller to reject the objection of the data subject also if he or she demonstrates a compelling interest for the establishment of a legal claim.

[36] These are the cases of processing that is necessary the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6.1.e) and of processing necessary for the legitimate interest pursued by the controller (Article 6.1. f). Additionally the right to object can also exercised against processing for direct marketing purposes.

[37] The right to access (Article 15) is the right of data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and to a series of additional information including the purpose of processing, the categories of personal data concerned, the recipients and other specified in paragraph 1 of Article 15. The right to rectification (Article 16) is the right to obtain without undue delay the rectification of inaccurate personal data and to have incomplete personal data completed. The right to restriction of processing (Article 18) which may be based on the ground of an unlawful processing or on the lack of accuracy of data, consists in preventing the processing of the data, with the exception of storage, without the data subject's consent.

erasure is « likely to render impossible or seriously impair the achievement of the objectives of the processing», and when a processing for scientific purposes qualify as «processing necessary for the performance of a task carried out of public interest» to permit the controller to reject the objection by the research participant.

2.5. Scope of Application of the Facilitating Regime

The GDPR doesn't define "scientific research" in its provisions, but only in Recital 159, where it states that «for the purposes of this Regulation, 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».
This definition of scientific research certainly encompasses both public and private entities, and regardless of how the research is financed, whether by public or private funding. However it remains unclear how far the facilitating regime will extend, and in particular as regard to data processing for purposes of scientific research but with a commercial goal. Indeed it is not uncommon that scientific research has some commercial element or perspective.
A stricter interpretation of the "*scientific research purposes*", which doesn't encompass research with immediate commercial goals, would be suggested by the Recitals of the Regulation and the aims that motivated the European Commission to its 2012 proposal for a Data Protection Reform. Indeed the GDPR is intended to strengthen data subjects' rights while the facilitating regime determines a relaxation of data protection rules and thus a detriment to data subjects rights. Such detriment is justified by the social benefits of scientific research, in term of increase of public knowledge and improvement of public policies contributed by the research outcomes. Expanding the scope of application of the facilitating regime to include also research with commercial goals would result in a disproportionate detriment of the research participants' rights. [38] On those grounds, we can also question whether the regime should apply to data processing for the so called "me too drugs" development. Me-too drugs are products which largely duplicate the action of existing drugs, and have more or less identical clinical outcomes to pre-existing drugs without even providing much benefit for price competition. To the extent that they are similar to pre-existing drugs, they can be considered a waste of R&D resources and lacking of social benefits. However more they differentiate from pioneering drugs and greater their benefits for citizens. Thus depending on the meaning ascribed to the term me-too drugs we can include or not in the definition of scientific research.[39]
An other key issue is how to deal with scientific projects pursued by consortia or temporary partnership which include research entities (such University faculties and centers of research) as well as private companies (including spin-off). More and more often scientific consortia include a business enti-

[38] On the Principle of Proportionality and its application in the EU see W. SAUTER , *Proportionality in EU Law: A Balancing Act?*, *op.cit*., pp.1-31.

[39] On the application of the facilitating regime to me-too drugs development see J.M.M. RUMBOLD AND B. PIERSCIONEK, *The effect of the General Data Protection on Medical Research*, in *J Med Internet Res*, Vol.19, No 2, Feb. 2017, e 47. On the so-called "me-too drugs", see generally B. GYAWALI, B. PRASAD, *Health Policy: Me-too drugs with limited benefits- the tale of regorafenib for HCC*, in *Nat. Rev. Clin. Oncol.*, 14(11), 2017, pp. 653-654; I. HERNANDEZ, ZHANG Y, *Comparing Adoption of Breakthrough and "Mee-too" drugs among Medical Beneficiaries: A Case Study of Dipeptidyl Peptidase-4 Inhibitors*, in *J Pharm Innov*., 12(2), 2017, pp. 105-109.

ties to provide insight on the market needs, prototyping and exploitation strategies. The facilitating regime should apply in such cases, regardless the nature and business purposes pursued by some of the consortia entities involved in the scientific project. Moreover we cannot exclude that datasets collected as a result of the scientific project can then be further processed for commercial goals, however the further processing will be subject to the general rule of the GDPR and not to the facilitating regime.[40]

Under the Directive 95/46, both private and public entities have been admitted to the facilitating regime, but Member States were free to establish different requirements for public and private entities. Most restrictive legislations have defined the scope of the facilitating regime relying on both objective and subjective requirements. The Italian Code of Conduct of 2004 can be counted among the latter. It establishes that the regime applies only for entities, both private and public, whose scientific research purposes result from the institution or organization objectives (in general from the statute of the organization) and whose scientific activities are documentable. Additionally it requires that the research project is carried out pursuant to the relevant sector-related methodological standards. In order to prove that the processing is made for research purposes, the data controller is required to deposit the project with the designated university or research body or scientific society, and these will need to keep it at least for 5 years after the planned completion of the research.[41] The GDPR doesn't refer to any subjective requirement and therefore an interpretation of the scope of facilitating regime such as the one of the Italian Code would be too restrictive and not validated by the new Regulation.

According to an even more rigorous interpretative approach, scientific research should include only that scientific research which is subject to specific obligations of dissemination. Recital 159 specifies such requirement with respect to processing for archiving purposes: processing for archiving purposes is subject to the facilitating regime of the GDPR only when made by bodies that are under a legal obligation «to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest». Such interpretation is however not supported by the text of the GDPR that doesn't recall same duty of dissemination with respect to scientific research. Moreover in Europe duties of dissemination are seen as a responsibility shared by both funding bodies and researchers, and so in absence of an applicable policy, that specifies the content of the dissemination's duties and specifically includes dataset sharing duties, researchers cannot be considered obliged to disseminate and sharing the research outcomes. [42] There-

[40] For H2020 Programs, the funding body and the consortia stipulate a grant agreement in compliance with *European Regulation No 1290/2013 of the European Parliament and of the Council* (OJ L 347 20/12/2013 p. 81-103). The Regulation provides rules for exploitation of the research results, however it must be distinguished between the exploitation of the results from the exploitation of the dataset. If the commercial use of the dataset is allowed by the Grant Agreements and/or any other governing rule or policy applied by the European Commission, it doesn't follow that further commercial use can enjoy relaxation of rules for data protection.

[41] *Italian Code of Conduct for Data Processing for Research and Statistical Purpose,* En Version doc. web. n. 1115480. For an analysis of implementation of the Directive by Member States, D. KORFF, *op.cit.,*114.

[42] Differently from the GDPR, the *Italian Code of Conduct* of 2004 mentions the principle of "*universal access to all analytical bona fide users*" (Recital 7), according to which when data are the result of research activities which have been funded with public resources, rules on no-discrimination and impartiality should apply to ensure access to all researchers. Recital 7 states that « Entities and bodies applying this Code shall abide by the

fore there is no rational basis to link the GDPR definition of scientific research to the enforceability of duties of dissemination.

Finally, with respect to the scope of the facilitating regime in the context of health-research, it is worth remembering that, under the Directive 95/46, the facilitating regime didn't apply to health-research studies that are directly related to the health-care activities carried out by health-care professionals and entities, but only to scientific studies that only *indirectly* serve and/or are related to provide healthcare services. For the first category of studies the GDPR in Recital 161 states that «for the purpose of consenting to the participation in scientific research activities in clinical trials, the Relevant Provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council should apply.».[43]

3. Safeguards for Data Processing in the context of Research

All the derogations provided by the GDPR for scientific research contain an explicit reference to the «appropriate safeguards» set by Article 89(1), to make it clear that exemptions can be lawfully provided as far as the research participants are adequately safeguarded.

Article 89(1) is construed as an open clause to be further implemented. However it provides some directions to those called to implement the data protection regime for research.

First, these safeguards should be established «in view of this Regulation» which means that the general protections for data subjects of the GDPR should be adapted to fit with the specific needs of the research context.

The concept of "appropriateness" of the safeguards also recalls that margin of manoeuvre left to Member States to adapt safeguards for research participants in view of the likelihood and severity of the risks for research participants, the type of data processed (with possible additional safeguards for sensitive data) and other factors.

Article 89.1 clause also contains some more specific requirements: the safeguards cannot be limited to organizational measures but must include technical measures, at least to ensure compliance with the principle of data minimization. This clarification is consistent with the two principles of «privacy by design» and «privacy by default » which have been introduced in the Regulation, but were already elaborated by the WP29 in many advisory opinions under the Directive 95/46/EC. Privacy by design expresses the requirement that organizations consider data protection issues early, during the planning phases of the processing operations. The processing operations should be designed, planned and then implemented in order to ensure that data protection is guaranteed during the whole data

impartiality and non-discrimination principle with regard to any other entities that process the data for statistical and/or scientific purposes. In undersigning this Code, special attention shall be paid, in particular, to the importance of said principle in connection with communications for statistical and/or scientific purposes of data that have been either deposited with public archives or processed on the basis of public funds ». See also on duties of dissemination and in particular to dataset: P. ARZBERGER, P. SCHROEDER, A. BEAULIEU, G. BOWKER, K. CASEY, L. LAAKSONEN, D. MOORMAN, P. UHLIR, P. WOUTERS, *Promoting Access to Public Research Data for Scientific, Economic, and Social Development*, in *Data Science Journal*, Volume 3, 29 November 2004, 135.

[43] *Regulation (EU) No 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* (OJ L 158, 27.5.2014, p. 1).

life cycle by the adoption of the most adequate technologies of the state of the art. The designing of processing operations should be such as to ensure compliance with data protection rules without need of human interaction (Privacy by default). (Recital 78 and Article 25)

In particular, technical measures should be in place «to ensure respect for the principle of data minimization». Processing operations should be designed and proper technical solutions should be adopted, as to guarantee that only data necessary for the specific purpose of research are processed (Article 89.1).[44]

Technical measures «may include pseudonymisation provided that those purposes can be fulfilled in that manner», and «where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner» (Article 89.1). Pseudonymisation is strongly encouraged by several GDPR provisions, not merely in the context of scientific research. According to the new definition of the GDPR, pseudonymisation means «the 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» (Article 4.3 b).

Pseudonymized data typically have their identifiers removed and replaced with a unique key code, and the key code can be used to track back to an individual, enabling future verification of data.[45]

Personal data that have been pseudonymised are still personal data and therefore the GDPR applies to their processing. By contrast data protection rules don't apply to anonymous information, «namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable »(Recital 26).

GDPR's dividing line between pseudonymised data and anonymised data is particularly relevant because it defines the scope of the Regulation. Organizations, including research organizations, have an obvious and justifiable interested in avoiding, if possible, the regulatory and administrative (and now also technology) burdens deriving from the application of data protection rules. However, they may now find difficult to determine when they processes truly anonymised data since the definition of anonymous or anonymised data in the GDPR relies on a complex fact-specific scrutiny that leaves a margin of uncertainty.

In order to establish whether pseudonymised data can be considered also truly anonymised, the data subjects should be « no longer identifiable». More specifically to determine whether the data subject

[44] The concept of "privacy enabling technologies" or "privacy enhancing technologies" or "PET" is a consequences of the privacy by design and by default approaches. They represent the idea that the processing operations should be designed through the adoption of adequate technologies, so that data protection is ensured in the engineering phase. See G.DANEZIS, J. DOMINGO-FERRER, M. HANSEN, J.H. HOEPMAN, D. LE METAYER, R. TIRTEA, S. SCHIFFNER, *Privacy and Data Protection by Design - From policy to engineering*, ENISA report, 2015, available at http://dx.doi.org/10.2824/38623 (last visited 26/10/2017).

[45] S. STALLA-BOURDILLON A.KNIGHT, *Anonymous Data v. Personal Data—A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, in *Wisconsin International Law Journal*, 2017 Available at SSRN: https://ssrn.com/abstract=2927945.

is still identifiable, account should be taken on «all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. (Recital 26)

The most notable defect of this definition is the wording «either by the controller or by another person» because it wrongly conflates two different data protection issues. Indeed according to the GDPR in order to ascertain if the data subject is still identifiable, account should be taken also on all reasonable means likely to be used by a *third party* to identify the data subject. In this way the category of anonymised data encompasses also the case a researcher who has no ability to re-identify, but, due to a breach, a third party can re-identify the data subject. The two aspects should however be considered and ruled separately: the way the pseudonymisation should be made is an issue of privacy enabling technology, while the breach by third party is a vulnerability issue, which should be addressed by the rules on security and on measures against unauthorized access.

Another flow of the GDPR test for anonymization is related to the wording «such as singling out». Indeed it is not clear the meaning of singling out within the Recital 26. All data subjects in research databases may need to be *singled out*, but in the sense of being discerned one from the other, not in the sense of being evaluated as it happens, for example, in personalized advertisement. Research and statistics make a collective use of data to find pattern and general rules and a participant can be "evaluated" together with many other participants. [46] In scientific research there is no risk of personalized evaluation as it happens in personalized advertisement. However if the "singling out" expression is interpreted also to cover the type of evaluation that is likely in the research context, then the test pursuant to Recital 26 would have the effect to unreasonably restrict the cases where data can qualify as truly anonymised. [47]

A third relevant issue on the definition of anonymised data within the GDPR is that it doesn't distinguish between cases of pseudonymised data where the data subject is identifiable at the source from those cases where the data subject is yet identifiable at the source but not at the recipient. Thus GDPR may bring 2 way-pseudonymised data to the category of personal data (because not truly anonymised). In the WP29 Opinion 4/2007 the personal data which undergone 2-way-pseudonymisation are qualified as anonymous because, despite being identifiable at the source, they

[46] U. TRIVELLATO, *op.cit,* page 631. The Author recalls the words of the *Explanatory Memorandum to the Recommendation R(97)18* according to which: « Scientific research uses statistics as one of a variety of means of promoting the advance of knowledge. Indeed, scientific knowledge consists in establishing permanent principles, laws of behavior or patterns of causality, which transcend all the individuals to whom they apply. Thus it is aimed at characterizing collective phenomena, this being the very definition of statistical results. It could be said, therefore, that research becomes statistical at a certain stage in its development.» (*Council of Europe, 1997b, Explanatory memorandum*, p. 30).

[47] E.B.,VAN VEEN, *GDPR facts and comments; LIBE and research*, *op. cit*., 6: «The pseudonymisation is applied in a data chain. The source or a Trusted Third Party replaces the direct identifiers of the subject by a pseudonym. The recipient cannot reach the subject through that pseudonym. The data attached to the pseudonym will in general be filtered to prevent all too easy re-identification through those data. In the meaning of ISO 25237 (nt. 5) of pseudonymised data, they should even be anonymous then.»; see also E.B.VAN VEEN, *Patient data for health research, a discussion paper on anonymisation procedures for the use of patient data for health research*, MedLawConsult, Den Haag, 2011.

are anonymous at the recipient.[48] If this interpretation of GDPR is correct, this will have effect on certain on-going European research projects, which have relied on a less restrictive definition of anonymised data, bringing them to the scope of the GDPR and to the consent system, with the resulting difficulties of seeking re-consent by research participants. [49]

In conclusion, the GDPR while encourages data pseudonymisation, it doesn't encourage controllers to go down the road of anonymising data to escape compliance burdens.[50] On the other side the issue of anonymisation of data before the data reach the research domain is, in most of the cases, vain and irrelevant. Sufficiently detailed data are indeed fundamental for research.[51] Truly anonymised data cannot be linked back to an individual, so preventing verification of data by any mean. Re-identification is particularly relevant in Medical Science and Life Science. Examples in Medical Science demonstrated that «interesting correlations that lead to breakthroughs only become apparent after the initial results suggest the implications of new variables that were not taken into consideration at the time of the study design. Discovery of new phenomena occurs only after going back to the original patient files and stratifying them according to the new variables. This type of analysis would not have been possible under data protection rules that prevent re-linking data and individuals».[52]

4. General rules of the GDPR applying to Scientific Research

Article 89.1, when mentioning the need for adequate safeguards for data processing in the field of research, specifies that these safeguards should be implemented «in view of this Regulation», suggesting that rules on general application of the GDPR (consisting in safeguards for the data subjects)

[48] Also ISO norm 25237 (2008) considers anonymous data those which undergone 2 way pseudonymisation. However there have been different interpretations of the WP29 Opinion and according to other interpreters that Opinion, not differently from the GDPR, considers 2 way pseudonymised data as personal data (pseudonymised but not truly anonymised data).

[49] J.M.M. RUMBOLD AND B. PIERSCIONEK, *op.cit.*, p. 2, indicates that the UK Information Commissioner's Office treats pseudonomyzed data as anonymous when they are used by a third party who doesn't possess the key code.

[50] As a matter of fact there is still one challenge with truly anonymisation of data in the medical research domain and it is merely a technology challenge. Certain solutions (based on blockchain technology) can be used to allow data anonymization and, at the same time, re-identification procedures that ensure compliance with rules on transparency, confidentiality and integrity of data. These solutions are not yet in the state of the art, but some are being developed and tested these days. See Q. XIA, E. BOATENG SIFAH, A. SMAHI, S. AMOFA, Z. ZHANG, *BBDS: Blockchain-based Data Sharing for Electronic Medical Records in Cloud Environments*, in *Secure Data Storage and Sharing Techniques in Cloud*, 8(2), 2017, p.44; A.EKBLAW, A.AZARIA, J. D. HALAMKA, A.LIPPMAN, *A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data*, White Paper, 2016, available at http://dci.mit.edu/assets/papers/eckblaw.pdf (last visited 26/10/2017).

[51] According to Van Veen «Instead of assuring that data reach the research domain anonymously (also if with a pseudonym attached)» emphasis should be rather placed to avoid "that they will not be re-identified within the research domain», E.B.VAN VEEN, *GDPR facts and comments; LIBE and research*, cit., page 21.

[52] Science Europe, *Position Statement on the Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*), available at www.scienceeurope.org (last visited 26/10/2017). See also generally S. STALLA-BOURDILLON A.KNIGHT, *Anonymous Data v. Personal Data—A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, in *Wisconsin International Law Journal*, 2017 Available at SSRN: https://ssrn.com/abstract=2927945.

should be *adapted* for scientific research and not applied as such. By contrast Recital 159 states that «where personal data are processed for scientific research purposes, this Regulation should also apply to that processing», implying that rules of general application should also apply to scientific research as such, without adaptation. Regardless of which of the two interpretations is the right one, there cannot be doubt that certain principles and rules of general application shall also apply to processing for scientific research purposes.

Principles of integrity and of confidentiality certainly apply also to scientific research. Despite not being explicitly stated by Article 89.1, controllers shall implement appropriate security measures, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. Security of the processing and the environment within which the processing takes place are particularly relevant in the context of scientific research; indeed a potentially large amount of personal data, including sensitive data, can be stored longer than necessary for the purposes for which they were first collected or processed. Security is also relevant for ensuring quality and integrity of the data, and thus reliable and verifiable results.[53]

Processing for research purposes is also subject to the principle of accountability, which was introduced by the Directive but has been clarified and associated with implementation procedures by the GDPR. Accountability means that the controller is deemed responsible for, and should be able to demonstrate, compliance with the rules and general principles of the GDPR (Article 5.2). The controller, or where applicable its representative in EU, and the processor will need to organize and maintain records of all processing activities performed under their responsibility to demonstrate compliance. These records will be made available to the Supervisory Authority, at request, to permit the monitoring of the processing operation.

Furthermore, scientific research organizations will be required to comply with GDPR rules on Breach Notification and Communication, in case of 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 (Articles 12.4, 33, 34).

An other group of rules applying to research are those provisions that concretize the risk-based approach of the GDPR. The Regulation requires organizations to get a clear understanding and to monitor their processing operations, and evaluate the severity level and likelihood of the risks for data subjects posed by their processing activities. In certain cases a special form of risk assessment called Data Protection Impact Assessment ("DPIA") is required. More specifically the controller have to conduct a DPIA for one, or more similar, processing where the type of the processing, «in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons» (Article 35.1)

To help controllers to identify the scope of this provision, the National Supervisory Authority ("NSA")

[53] Data Integrity and quality are also relevant in relation with the need of making dataset available for other researchers, when a data sharing policy applies. See also G. Chassang, *The impact of the EU general data protection regulation on scientific research,* available at https://doi.org/10.3332/ecancer.2017.709 (last visited 26/10/2017).

will publish a list of the type of processing operations that are subject to the DPIA requirement, after approval of the European Data Protection Board ("EDPB").[54]

Then Article 35.3 indicates certain situations for which the DPIA «shall in particular be required». Among these cases, two may be relevant in the context of research:

- 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 (Article 35.3 a);
- in case of processing on a large scale of special categories of data such as genetic, biometric, data concerning health and other sensitive data referred to in article 9 Par.1 (Article 35.3 b).

The second situation may be represented by bio-banking, consisting in an organized collection of human samples and associated information (specimen) which are routinely collected and stored for multiple future research purposes. Bio-banking poses several ethical and legal issues, including the issue of the ownership to the sample. However there is not a common view on the risks posed by bio-banks to individuals compared to other studies of medical intervention and therefore the evidence collected by research organizations may be of help in individuating whether the DPIA requirement applies. [55]

NSA will need also to identify when a DPIA is necessary for Whole-Genome Sequencing.[56] Indeed in consideration of the technology used and the large-scale of data stored and processed it may fit in cases provided for in Article 35.1 and 35.3.[57]

---

[54] «A DPIA is not a singular and linear process, but rather has to be repeated to ensure continuous supervision over the lifetime of a project. Accordingly, Article 35(11) GDPR calls for a review at least when there are changes in the risks posed by the processing of data. Such changes may occur whenever organizational or legal conditions change or new risks for data protection in general are identified. It then has to be ensured that the safeguards chosen are able to adapt to these changes. », F. BIEKER, M. FRIEDEWALD, M. HANSEN, H. OBERSTELLER, M. ROST, *A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation, Privacy Technologies and Policy*, 4th Annual Privacy Forum, S. Schiffner et al. (eds.), Frankfurt, 2016, pp. 21–37.

[55] On the risks posed by bio-banking and those posed by medical intervention, see J.M.M. RUMBOLD AND B.PIERSCIONEK, *op.cit.,* p.3; see also G. LAURIE, KH. JONES, L. STEVENS AND C. DOBBS, *A review of evidence relating to harm resulting from uses of health and biomedical data,* 2015, London, Nuffield Council on Bioethics, p.210. See also, on the different degree of risk posed by interventional research compared to epidemiological research that makes use of registries and bio-banks, M.G. HANSSON, G.J.V. OMMEN, R. CHADWICK, J. DILLNER, *op.cit,* p. 451.

[56] WSG means the process of determining the complete DNA sequence of an organism's genome at a single time and it is necessarily sequencing on large scale. It is also done by means of hi-tech machines. Ethical and privacy concerns arising from WSG are described in A. L. MCGUIRE, T. CAULFIELD, AND M- K. CHO, *Research ethics and the challenge of whole-genome sequencing*, in *Nat. Rev. Genet*. 2008; 9(2): 152–1.

[57] The text of the GDPR approved by the Parliament in 2014 defined the criterion of "large scale" with specific parameters, while the text of the enacted version of GDPR provides only some directions in recital 91; the WP29 on 4 April 2017 issued an Opinion on DPIA which doesn't address specifically research, and it recommended that the following factors, in particular, should be considered to determining whether the processing is carried out on a large scale: the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity. If sensitive data are not processed systematically and on a large scale, the processing does not auto-

ISSN 2284-4503

Guidance on the identification of the risk related to the processing will be also provided through the code of conducts, approved certifications, guidelines provided by the EDPB and the data protection officer (Recital 77).

The designation of a Data Protection Officer, with mainly advisory role, is also mandatory upon to Article 37 in case of processing of large scale, in particular when the processing in large scale concerns sensitive data (Articles 37 and 39).[58]

Research entities that have participated in Horizon 2020 (or ERC programs) will find the DPIA as something not so different from the Data Management Assessment required by those funding programs. In Horizon 2020 the Data Management Assessment is a part of the ethic assessment and requires the research organizations to describe the whole data life cycle, and assess if there are specific ethics or privacy concerns or risks for research participants. The Data Management Plan should be then structured accordingly. When the GDPR will enter into force in May 2018 this assessment will become a specific obligation for all researchers and research institutions, independently from the source of project funding and from the policy applied by the funding body. However ethical issues, which are part of the assessment under H2020 or ERC, will not be part of the DPIA as ethics and deontology issues are not covered by GDPR.[59]

Since the DPIA is not always mandatory, the question arises to what further function should be assigned, in the context of research, to the risk-based approach. One may wonder if the risk-based approach represents that solution to the well-known conflict between right-based nature of data protection, implied by the fundamental right' nature of data protection, and the need for a flexible approach to compliance on the side of researchers. Indeed the risk-based approach can be interpreted

matically presents high risks for the rights and freedoms of data subjects; thus processing of special categories of data by a medical doctor in a one-person practice should not be considered "large scale". WP29 also listed some examples where DPIA is mandatory: in case of an hospital processing its patients' genetic and health data (hospital information system) the relevant parameter to consider are that sensitive data and data concerning vulnerable data subjects are processed, and also in large scale so a DPIA is obligatory. See *WP 248 – Guidelines on Data Protection Impact Assessment (DPIA).*

[58] The designation of the DPO is mandatory upon to article 37 when (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

[59] With respect to ethic rules we should mention the *European Code of conduct for research integrity* drawn up by the European Science Foundation (ESF) and the Federation of all European Academies (ALLEA), which brings together 53 national academies from 43 states. The European Code of Conduct for Research Integrity is considered one of the most authoritative codes on the subject in the European Union and has been adopted by several institutions. The principle of integrity in research applies in particular to: honesty in presenting goals and intentions; reliability of research; fairness in communication; objectivity; independent and impartial communication with other researchers and with the public; duty of care for humans, animals, the environment; fairness in providing references and giving credit for the work of others; responsibility for future generations in the supervision of young scientists and scholars. European Science Foundation (ESF), All European Academies (ALLEA). *A European code of conduct for research integrity.* 2011, available at www.esf.org/fileadmin/Public_documents/Publications/Code_Conduct_ResearchIn tegrity.pdf. (Last visited 26/10/2017).

as to justify that "scalability" or "granularity" of compliance to the legal requirements of data protection based on the degree of risks for participants, which representatives of the Scientific Community have championed during the work on the preparation of the GDPR. For the Art 29 Working Party this interpretation is not supported by the text of the GDPR and the risk-based approach cannot be presented as an alternative to well-established data protection rights and principles.[60] The likelihood and severity of risks posed by the processing operations to the data subjects, according to the WP29, cannot justify a different level of compliance to the rules of the GDPR. Nevertheless if this may be true in general, a strong "harm-based approach" would be surely beneficial for accelerating scientific research, because it would serve to avoid harmful and useless compliance work when there are no relevant risks for research participants and at the same time to protect them when required. [61]

5. Rules on Data Transfer to Non-EU Countries and International Organizations

In principle, any transfer of personal data to third countries (which are Non-EU Countries) and international organizations is forbidden, unless one of the exceptions of Chapter V of the GDPR applies.
Researchers ordinarily collaborate with third countries academies and research organizations, and the rules on transfer of personal data are especially relevant, since there is no exception or more lenient regime when the data to be transferred are pseudonymized. Moreover since the GDPR reduces the possibilities to consider pseudonymized data as anonymous, transfer of data for research purposes is now more likely to be subject to rules on data protection than under the Directive. Therefore research organizations need to ensure that at least one the following legal grounds applies if they process personal data and a transfer to third countries is likely.
While establishing the exceptions to the ban on transfer, the EU legislator warned that these exceptions require not a formalistic but a functional interpretation in order to substantially ensure that the level of protection of natural persons guaranteed by the Regulation is not undermined (Article 44.1).
The main exception to the ban, which also results as the most comfortable option to controllers and processors, is the transfer to the countries or international organizations with respect to which the Commission has deliberated that they ensure adequate level of protection (Article 45.1). By implementing act, the Commission may also assess the adequacy of the level of protection of only a territory or one or more specified sectors within a third country or the international organization (Art 45.3). The adequacy decisions of the Commission will be periodically reviewed and could be amended or repealed upon to paragraph 4, 5 and 9 of Article 45 and they will be published in the Official Journal of the European Union and on the website of the Commission.
When the Commission has made no decision, the transfer to the country or organization is permitted only if the controller or processor has provided appropriate safeguards and on condition that data subjects rights and effective legal remedies are available (Art 46).

[60] WP29 Opinion 2014 on *Statement on the role of a risk-based approach in data protection legal frameworks*, WP 218 Adopted on 30 May 2014.
[61] R. GELLERT, *op.cit,* p. 4; the Author well analyzed the uncertainty surrounding the notion of risk and risk-based approach within the GDPR, the position of the WP29 in the mentioned Opinion of 2014 as well as the different dimension of the risk-based approach as it was envisaged in early documents of the Working Party.

Such safeguards can be represented, alternatively, by binding corporate rules in compliance with Article 47 (Article 46.2 letter b); or by «a legally binding and enforceable instrument between public authorities or bodies» (46.2 letter a); or by an approved Code of Conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply appropriate safeguards, including as regards data subjects rights (Article 46.2 e).

The GDPR also provides for further derogations from the general ban for transfer, in the absence of an adequacy decision by the Commission or of appropriate safeguards upon to Article 46 and 47, in particular:

- when the data subjects give their explicit consent to the transfer, after having been properly informed of risks due to the absence of adequate safeguards (Article 49 Par 1 letter a);
- when the transfer is necessary for important reasons of public interest (Article 49 Par 1 letter d);
- in case of transfer for the purpose of «compelling legitimate interests» pursued by the controller , unless these interests are not overridden by the interests and freedoms of data subjects (Article 49.2).

The concept of legitimate interest is of difficult application in the absence of an implementing legislation. The legitimate interest of the controller can be a legal ground for processing for the purpose of scientific research pursuant to Article 6.1 f). It can also be the ground for the transfer of data outside EU pursuant to Article 49.2, in the absence of an adequacy decision of the Commission. The controller is required to assess «all the circumstances surrounding the data transfer» and on the basis of that assessment the controller should be provide suitable safeguards. However, a transfer on this ground is lawful only if it's not repetitive and concerns a limited number of data subjects, which makes this provision of very rare application in the context of research.

The other option, consisting in seeking the consent of the data subject to the transfer, finds the difficulties already analyzed in scientific research. It's not easy to forecast, at the time of the collection of personal data for a scientific research project, if the dataset proves later to be useful for a new research project involving third countries or international research organizations. Obtaining the "re-consent" of research participant when the need of transfer arises would be even less feasible.

Consequently, in the research context, if a transfer of research participants' data is necessary and it has to be done to a third country that according to the Commission doesn't offer adequate level of protection or for which the Commission didn't express its evaluation, the whole research cohort may opt to adopt and approve a Code of Conduct and to commit to apply safeguards and data subjects right in the third country upon to Article 46.1.e).

Given the mandate to the European Commission by the Treaty of Lisbon (Article 180) to complement the activities carried out by Member States to promote cooperation in the field of research, which includes cooperation with third countries, we expect an implementing act by the Commission to establish harmonized rules which facilitates transfer of personal data for scientific research purposes. The GDPR itself doesn't contain any derogation from the ban on transfer specifically applicable for scientific research, and therefore rules of general application should apply. The absence of an exemption at least guarantees that there won't be divergent national rules on transfer for research purposes.

Essays

6. Conclusions

The final chapters of the GDPR confirm that the Directive 95/46 will be repealed once the new Regulation will be fully enforceable. During the two-years transition period any on-going processing authorized under the previous regime remain valid, while new processing should refer to the GDPR. [62]
With respect to exhaustively regulated provisions, Member States may, but are not required to, enact new laws to repeal past legislation and to make the Regulation provisions more comprehensible. [63] Rules on scientific research, by contrast, need to be implemented by law and then, possibly, specified in a code of conduct.[64]
Under the Directive 95/46, Member States had enacted specific legislation and some of them adopted a code of conduct to comply with the Directive and other European legislation in the field of scientific research and statistics.[65] Some of these codes of conduct contain adjustment clauses to ensure that they are updated, to comply with new international or EU instruments adopted in connection with the protection of personal data for statistical and scientific research purposes. However, considering the impact of the rules of general application (in particular the institutional novelties) and also of some new rules specific for scientific research introduced by the GDPR, new codes will need to be drafted and adopted.
In the meaning of the GDPR, the codes of conduct don't represent ethics and deontological duties, but proper rules of law; indeed despite several references in the GDPR to the ethics, the ethic rules are outside the scope of the Regulation. They are delegated legislation and, in consideration of the multilevel governance system of EU, in the field of Scientific Research, each National Parliament will need to enact delegating legislation for their adoption. But the drafting of the rules is up to the research organizations and associations, which will involve and consult also relevant stakeholders when possible. The National Supervisory Authority will approve the Code only if it finds that it provides suf-

[62] Recital 171 clarifies that where processing is based on consent under the current Data Protection Directive, it is not necessary for the individual to give their consent again if the way the consent was given is consistent with the conditions of the GDPR.
[63] The 27 April 2017 Germany Parliament passed the BDSG to replace predecessor legislation which has been in force for the last 40 years and with effective date of 25th May 2018 the new BSDG will be the basis for the adaption of further Germany Privacy acts to implement the other provisions of the GDPR on special processing situations, such as the provisions on processing for scientific and statistical research. Most of remaining Member States indicate through their officials, members of their parliament or other parties how their jurisdictions intends to deal with laws supplementing the GDPR, but they didn't enact new legislation. On April 28 2017, the Italian Data Protection Authority (Garante) released its first set of guidelines on the upcoming General Data Protection Regulation, which also takes into account the recent opinions issued of the Article 29 Working Party available at http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali.
[64] See footnote 9.
[65] Specific rules on scientific research and statistics were contained in: *Convention for the protection of the individual with regard to the automatic processing of personal data,* (Council of Europe, 1981), *Recommendation R(97)18 on the protection of personal data collected and processed for statistical purposes,*(Council of Europe, 1997b). For health data: the *Recommendation R(97)5 on the protection of medical data* (Council of Europe, 1997a). On Statistics and Research also: *Regulation n. 322/97* (Council of Europe, 1997) and *Regulation n. 831/2002*(Commission 2002) for the implementation of the Regulation n.322 and related to the access to data for scientific purposes.

ficient appropriate safeguards and then transmits it to the EDPB, which will take care of the publicity of all codes approved. (Articles 40.5 and 40.11)

These codes are intended to contribute to the proper application of the Regulation «taking into account of the specific features of the various processing sectors» (Article 40.1). The rules of the Regulation will be there specified in particular as regard to the pseudonymisation measures, information provided to the public and data subject, security measures, notification of data breach, transfer outside the EU and dispute resolution procedures can be introduced (Article 40.2.). The code of conduct for scientific research will include also the exemptions of the facilitating regime. The need for an adaptation of the Regulation rules is shared by other sectors, in addition to scientific research, and in particular by small and medium enterprises or entities which can hardly sustain certain regulatory and administrative burdens (Recital 98).

Codes of conduct also serve to demonstrate and facilitate compliance to the GDPR by the processor and controller (Recital 81 and Article 24. 3).

It is still unclear how and if, in the next months, the EU will address States implementation activities for the scientific research regime. The TFEU makes clear that EU has only support competence in the field of Scientific Research, but this includes supporting the cooperation between Member States «aiming notably at permitting researchers to cooperate freely across borders » and in «the definition of common standards and the removal of legal and fiscal obstacles to that cooperation» (Article 179 TFEU ex 163 TEC); furthermore «the Union and the Members shall coordinate their research and technology activities so as to ensure that national policies and Union policy are mutually consistent » (Article 181 ex 165 TEC).

The powers of the European Commission are further disciplined in the GDPR according to which «the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in order to fulfill the objective of the regulation and in particular in respect of criteria and requirements for certification mechanisms, information to be presented by standardized icons and procedures for providing such icons » (Recital 166 and Article 12.5).[66] There is no express reference to implementing acts in the field of scientific research in the GDPR.

Much of the work on policy harmonization is left to the "consistency mechanism" designed in Chapter VII, which requires a cooperation between supervisory authorities first and then between them and the Commission (Article 63).

Under the GDPR, the WP29, bringing together the European Union's National data protection authorities, will become the EDPB. The EDPB will maintain its role of issuing opinions on matters related

[66] Chapter X of the GDPR (containing Art 92 and 93) grants the Commission the power of adopt delegated acts, but such power can be revoked by the Parliament or the Council at any time. The Commission will be assisted by a committee in accordance with *Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers* (OJ L. 55, 28.2.2011, pp. 13–18). Additionally, according to Art 12.8 of the GDPR «The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardized icons.»; upon to Art 43.8 of the GDPR the Commission may adopt implementing acts laying down technical standards for certification mechanism and data protection seals and marks, and mechanism to promote and recognize those certification mechanism, seals and marks in accordance with the procedure referred to in Article 93. 2.

to the interpretation of the rule of the GDPR. In its action plan issued the 6th of February 2016 and the accompanying supplementary statement, the WP29 illustrated the important institutional implications of the GDPR and laid out seven substantive topics to be covered with forthcoming advisory opinions. The opinions issued on these topics under the Directive will be re-examined in light of the GDPR to hammer out any inconsistencies.

On 4 April 2017 the WP29 issued the guidelines on DPIA and on June 8, 2017 new guidance on data processing in the context of employment. The WP29 has no yet issued an opinion on processing for scientific and statistical purposes in the light of the GDPR and we expect that Member States will be waiting its advisory opinion before implementing the scientific research regime and working on the codes of conduct. [67]

[67] The French Government for example has created a taskforce led by the Ministry of Justice to reshape the existing FDPA according to a report published on 22 February 2017 and announced that they will be following the Art 29 Working Group guidelines emphasizing in the report that «Several Concepts referred to in the Regulation will have to be clarified by the Art29 Working Party in order to allow a uniform application of the Regulation among Member States of the European Union ». However according to some commentators of the GDPR, the new role of the EDPB has some governance issues, in particular E. B. VAN VEEN «With by-laws by the Commission there is some system of oversight, as regulated in the TFEU and following decisions. For implementing acts the Commission must consult an expert group. Delegated acts can even be repealed by the EP or the Council (member states). There is non of that governance system with the EDPB. In its present form, the Art. 29 WP, the Opinions are not discussed beforehand with relevant stakeholders. EDPB will be composed of the DPA's of the member states, just like the present art. 29 WP. » E.B. VAN VEEN, *GDPR facts and comments; LIBE and research*, cit., p.9.