The new european regulation on personal data protection: significant aspects for data processing for scientific research purposes

Francesca Preite [1], Silvia Salardi [2], Rosaria Gesuita [3], Simona Villani [4], Paolo Trerotoli [5], Vincenzo Guardabasso [6], Antonella Zambon [7] and the SISMEC "Observational Studies" working group

(1) MediNeos S.U.R.L, Modena, Italy. Senior partner in the Law Firm of Miari-Preite, Reggio Emilia, Italy
(2) Assistant Professor of Philosophy of Law and Bioethics, School of Law, University of Milan-Bicocca
(3) Centre of Epidemiology, Biostatistics and medical Information Technology, Polytechnic University of Marche, Ancona, Italy
(4) Department of Public Health, Experimental and Forensic Medicine, Unit of Biostatistics and Clinical epidemiology, University of Pavia, Pavia, Italy
(5) Department of Biomedical Science and Human Oncology, University of Bari Aldo Moro, Italy
(6) University Teaching Hospital "Policlinico-Vittorio Emanuele", Catania, Italy
(7) Department of Statistics and Quantitative Methods, Unit of Biostatistics, Epidemiology and Public Health, University of Milan-Bicocca, Milan, Italy

CORRESPONDING AUTHOR: *A. Zambon, Department of Statistics and Quantitative Methods, University of Milano-Bicocca, via Bicocca degli Arcimboldi, 8, Edificio U7, 20126 Milano, Italy. Email: antonella.zambon@unimib.com*

DOI: 10.2427/12286
Accepted on March 27, 2017

ABSTRACT

Aim The paper investigates the new European Data Protection Regulation released in 2016.
It highlights the data protection principles inspiring the Regulation and outlines its main innovative as well as critical aspects as regards the use of personal data for research purposes.
Results: As far as scientific research is concerned, the new Regulation provides some interesting novelties in relation to informed consent and to use of personal data without consent.
Conclusion: It is still early for the consideration of the new Regulation, in relation to which the transition period before it definitively comes into force in 2018 will be useful for making a complete and detailed assessment of its adequacy. However, it is precisely with reference to the collection of retrospective personal data that the greatest innovations are seen. It will therefore be interesting to follow the interpretative evolution of the principle of compatibility of purposes which renders – in fact – personal data already collected usable, even in the absence of consent from the data subject.

Key words: Data Protection Regulation, informed consent, Data Protection Officer, Right to privacy, personal data for research purposes

INTRODUCTION

On 27 April 2016, after a troubled gestation,, Regulation 2016/679 [1] of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data was finally published.

The Regulation is to have a two-year transitional period, meaning it will actually enter into force in the first half of 2018.

The wide-ranging and heated debate that accompanied the development of the Regulation, particularly with regard to certain aspects, along with numerous revisions caused a severe delay in the presentation of the draft. One crucial aspect was the clash over the responsibilities and burdens of the Providers, as well as the rights of the data subjects, with regard to data processing on the internet.

The most obvious innovation, however, relates to the legal instrument chosen by the EU Institutions. This is a Regulation and not a Directive. Indeed, the European Directive 95/46/EC will be abrogated upon the entry into force of the Regulation. The Regulation – by its very nature, immediately self-executing in all member states - was preferred over the Directive, which, by contrast, for implementation requires transposition into the national law of member states, which, within the limits of the European framework, may amend and/or define individual provisions.

We are thus faced with a normative act that is binding, in a uniform manner, on all member states.

The objectives were clearly set out in the preamble to the Draft Regulation in its final version dated 28 January 2016 and described in Figure 1.

However – in an apparent contradiction– both the Draft and the published Regulation provide that member states shall be free to maintain or introduce national rules that clarify and specify the provisions of the Regulation.

This means that the Union is clearly deciding to make a compromise between the imposition of a homogeneous rule for all member states and the possibility of a broad space for manoeuvre by individual states.

It is expected that such an approach will only have the effect of partly neutralising the intended uniformity, equality and coherence of processing, which is enthusiastically proclaimed in the first 15 "Whereas…" recitals -the Regulation consists of 173 recitals explaining the regulated matters and 99 articles- and which pervades the document.

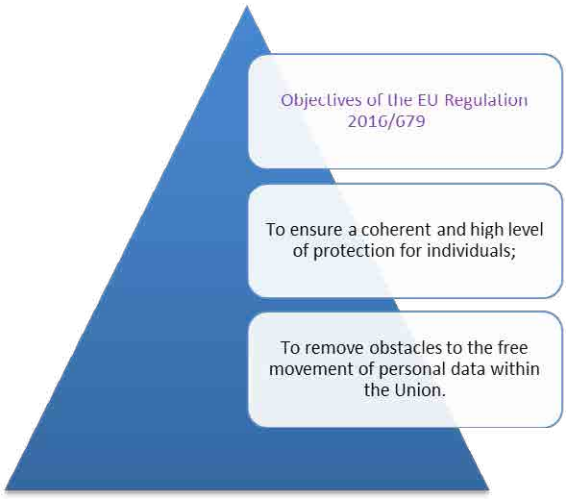
It is the aim of this paper to critically approach this new EU Regulation in order to analyse the implications of its provisions for scientific research and to offer a first overview of its possible impact on national rules.

BACKGROUND

The new Regulation in the context of the framework for data protection principles at European level

Personal data protection has acquired a central role in the European legal context. That centrality is directly related to the evolution of the concept of *privacy*. This concept was originally an expression of the right to be let alone; it then had the function of excluding interference by others in an individual's private sphere. However, from the second half of the last century when technological and scientific development started to penetrate, pressingly and invasively, into the private sphere of individuals, it became necessary to redefine the concept of *privacy*. [2-4] In this regard, in the 1970s the concept of *privacy* expanded to include within its sphere of action an individual's right to control the use that others make of his or her information. [5-8] This definition is not the point of arrival, but rather the point of departure for further definitions of that right, which can be summarised in the words of Stefano Rodotà as follows: *privacy* is "the right to retain control over your information and to determine the methods of construction

FIGURE 1. Objectives of the EU Regulation 2016/679.



of your private sphere" [3] and, in the broader sense, of your personality and identity. *Privacy*, understood in the sense of the aspects briefly analysed here, is not only important from an ethical and deontological perspective, but it is also a legally guaranteed right. [9] It is explicitly formalised in various normative documents that lay down the framework of principles underlying the European legal system. In particular, the protection of *privacy*, in the specific sense of personal data protection, assumes the nature of a fundamental constitutional right protected both nationally and at the highest levels of the European legal system. With particular reference to this field, and before reviewing the *framework rules* that protect the right to confidentiality of personal data in the different contexts in which it may be used by third parties, we ought to clarify opposing rights for which a balancing process is needed. In the case of the right to *privacy* in the senses referred to earlier, the right of the natural person is balanced against the right of biomedical research to perform necessary trials and to publish the results, and also against the interest of the community in using those results to improve the quality of community life. That right thus requires the development of methods for acquiring informed consent with a view to ensuring the effectiveness and practicability of the right. Balancing as mentioned above is rendered necessary in light of the structure of the European legal system, founded on the protection of fundamental rights and therefore on the protection of the values that those rights express. This means that when a new piece of legislation, whether it be a Regulation or a Directive, is developed, it must respect not only the correct procedures of legislative production provided by the system, i.e. be produced by and derived from the authority with jurisdiction to do so, [10] but it must also be in accordance with the principles and values expressed at the highest levels of the legal system (*axiological consistency*) [11].

In the specific case of the Regulation considered in this paper, its suitability to protect not only the natural person's *privacy*, but also the interests of the other interested parties , will therefore be demonstrated by its consistency with the principles expressed in the legislative acts that will be analysed below, i.e. the provisions of the Charter of Fundamental Rights of the European Union (the Charter of Nice), [12] the Convention on Human Rights and Biomedicine, and the respective Protocols [13].

The Charter of Fundamental Rights of the European Union at Article 8, and the Treaty on the Functioning of the European Union (TFEU) [14] at Article 16, both ratify the protection of personal data processing of natural persons as a fundamental right. Article 16 TFEU provides that "Everyone has the right to the protection of personal data concerning them. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities".

This article specifies that the right to protection of data of a personal nature must be subject to ad hoc regulation by the Parliament, by the Council, and by the member states. Assigning control of regulation to an independent authority points the way for the implementation of a regulation aimed, on the one hand, at guaranteeing the private sphere from external interference and, on the other, not entrusting control over the data of natural persons exclusively to legislative and government power.

Article 8 of the Charter of Nice, [12] entitled "Protection of Personal Data", provides that everyone has the right to the protection of his/her own personal data; that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law; that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; finally that compliance with these rules shall be subject to control by an independent authority. For the purposes of this discussion, the relevant aspects of this article are that the right to the protection of personal data is provided as an autonomous right compared to that provided by Article 7 relating to respect for private and family life. This separation of the right to the protection of personal data serves precisely to emphasise the transition from negative protection of *privacy* as the '*right to be let alone*' to active protection, coming to fruition in the power of control over and intervention on one's data. In addition, "the powers of control and intervention are not attributed only to the direct data subjects, but are also entrusted to an independent authority (Art. 8.3): protection is no longer just individualistic, but involves a specific public responsibility. We are thus faced with a redistribution of social and legal powers" [4].

The Convention on Human Rights and Biomedicine [13] (Oviedo Convention) also refers to the right to know information concerning a certain individual at Article 10 entitled "Private life and right to information". That article provides that everyone has the right to respect for private life in relation to information about his or her health; everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed. The article in question supplements the provisions of Article 10 of the Charter of Nice [12] on the other facet of the right to know one's information, i.e. the right not to know it. [15] This aspect is of particular importance with regard to u*nexpected findings*. [16] Needless to say, this term refers to "findings, data, information not sought, but resulting randomly from a clinical examination (not only in the genetic field, but, for example, also in diagnostic

imaging or commonly during an autopsy), particularly frequent in scientific research. With reference to the cases of biobanks and human genetics studies, the possibility of using biological samples, given with a specific research project in mind, for a new and different purpose brings with it, obviously, the discovery of "additional", information thereby raising the question of notification to the person to whom it refers.16 Recently, both Recommendation 6 (2016) relating to the use of biological samples of human origin, replacing Recommendation 4 (2006), and the National Bioethics Committee in its opinion of March 2016 entitled *Managing "incidental findings" in genomic investigations with new technology platforms"* have also taken a stance on the issue.

Articles 16 and 26 of the Additional Protocol to the Oviedo Convention [17] on genetic testing and biomedical research, respectively, provide for the right to respect for private life and the right to know the existence of information collected about the individual. It should also be noted that Article 2 of the Oviedo Convention [13] provides that the interests and welfare of the human being shall prevail over the sole interest of science and society.

After the brief examination of the principles that act as a framework for the Regulation which is the subject of this paper, we can ask ourselves if the provisions on the protection of personal data contained in the new Regulation are consistent with them, specifically regarding the processing of such data for the purposes of scientific research.

It is evident that it is the declared intention of the European legislator to safeguard the right to the protection of personal data, as ratified by Article 8 of the Charter of Nice, [12] through a Regulation, i.e. a *self-executing tool*, and, as such, with a view to guaranteeing harmonisation of the different national rules. That article provides the basis for the adoption of a Regulation aimed at ensuring both the same level of protection of data throughout the Union and the protection of personal data with reference to cross-border flows to third countries or international organisations.

It is emphasised in several ways that the Regulation is intended to strengthen the rights of the data subject so that the active control over his or her data is highly effective, using different actions such as deletion, rectification, objection and so on. Many specifications within the Regulation are oriented in this direction, particularly those that base the lawfulness of data processing on informed consent. Informed consent is not, however, an absolute requirement, but represents one of the conditions that Article 6 stipulates for the lawfulness of processing. As clarified in recital 26, the Regulation applies only to information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation should be considered to be information on an identifiable natural person. To ascertain whether means are 'reasonably' likely to be used to identify the natural person, all objective factors, such as the costs of and the amount of time required for identification, should be taken into account. The available technology at the time of the processing and technological developments must also be taken into account. In light of these considerations, the non-application of the Regulation to cases of anonymous information, including for statistical and research purposes, is understandable.

The so-called "purpose limitation" provided at Article 5, 1b contributes to strengthening the impression that the Regulation is intended to guarantee effective control over one's data by the data subject. In that regard, the data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In other words, the general rule is maintained, in line with the fundamental principles imposed to protect personal information. This means that further use of personal data must be compatible with the purposes for which the data was originally collected and further processing of personal data for the purposes of scientific research is considered compatible with the initial purposes. Even where data processing is not based upon the consent of the data subject, the processing controller must make a general check on whether the processing for further purposes is compatible with the purpose for which the data was initially collected (Article 6, 4). It is noted, in recital 50, that "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations." A series of derogations with regard to informed consent and the related rights are also moving in this direction, which we will comment upon in the paragraph focusing on the issue of consent.

In the balance between the rights of the data subject to the protection of his or her data and archiving in the public interest,scientific, historical or statistical research, the Regulation provides further derogations in favour of the latter activities. With reference to the processing of particular categories of sensitive data (Article 9, j), prohibition on processing "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" is liable to be waived, inter alia, in the case where the sensitive data, used for health-related purposes, is processed for the purposes of archiving in the public interest, or for scientific, historical or statistical research. Of particular interest for scientific research is the Regulation's provision of derogations from the obligation to provide information to the data subject, where the data has not been obtained directly from the same (Article 14, 5b), and from the obligation to communicate a violation of the personal data of the data subject (Article 32).

Article 14, 5b provides that where the communication to the data subject of information regarding his or her data is impossible or would involve a disproportionate effort, in particular for archiving purposes in the public interest or for scientific research purposes, that obligation is no longer in place, subject to the safeguards referred to in Article 89 [1], and particularly as regards the minimisation of the data. That derogation is justified in relation to the disproportionate effort required from the data controller to trace the data subject.

That disproportion could occur, in particular, "where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration", as literally specified in recital 62 of the Regulation.

On the other hand, Articles 45 and 46 provide the general limits for the transfer of data to a third country or to an international organisation. These concern, respectively, transfers of personal data on the basis of an adequacy (of protection) decision and transfers subject to appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. That stated however, Article 49 provides for specific derogations from the cited articles. That article is relevant with regard to archiving in the public interest or for scientific, historical or statistical research, as it allows the transfer of data towards a third country or an international organisation, if it is not a repetitive transfer regarding a limited number of data subjects, and where that operation is necessary to pursue the legitimate overriding interests of the processing controller, which are not overridden by the interests or rights and freedoms of the data subject. In that regard, recital 113 focuses attention on the fact that "for scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer". It seems clear from the latter specification that the European legislator is opening the doors to a balance between the right of the data subject to the protection of his or her data and the controller's overriding interests, in the cases specifically indicated, leaning more towards the latter. This, however, is not a position free from criticism, particularly in light of the above-cited Article 2 of the Oviedo Convention, which rejects the proposition that the sole interest of society or science can justify overriding the rights of the individual.

It should be noted that, as regulated by Article 30, the processing controller or the controller's representative must maintain a record of processing activities under its responsibility. Despite this article not even indicating how far the number of data subjects must be limited so that the cross-border transfer of data can be carried out, it is requested that, in addition to the contact details of the processing controller or controller's representative and the purposes of the processing, the records should also indicate a description of the categories of data subjects and the categories of personal data along with the categories of recipients to which the personal data has been or will be communicated, including third country recipients.

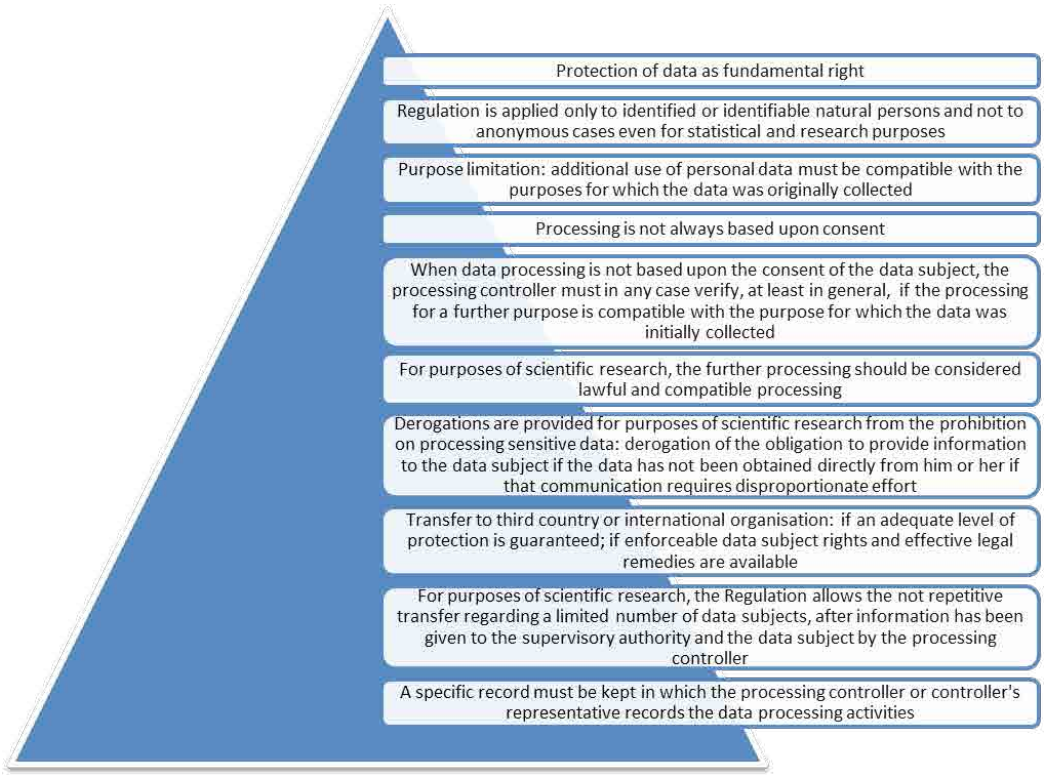
The Regulation specifies that processing for archiving purposes in the public interest, scientific, historical research or statistical purposes, shall be subject to appropriate safeguards to protect the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place to give effect, in particular, to the principle of "data minimisation". However, there are possible derogations from the rights of the data subjects, provided in particular in the articles that allow for direct power of control over the data by the data subject, as will be analysed in more detail in the paragraph focusing on informed consent. What is worth noting here is that the provision of those derogations is under the remit of the national law of individual member states or the Union, a fact that could lead, as noted above, to critical issues for harmonisation of the rules.

In light of the framework of provisions analysed thus far, it is possible to draw some intermediate conclusions regarding their compatibility with the safeguarding of the right to protection of data in the sense intended by the rules at the heart of the European system, a compatibility of an essentially *axiological-value* nature. This is an evaluation of an ethical-legal nature which does not principally concern the methods of production of the rules but, rather, the consistency of their content with the values underlying the principles and fundamental rights.

While it is true that the adoption of a *self-executing* Regulation should guarantee harmonisation between the various national legal systems and that this should be advantageous for the safeguarding of the fundamental right to the protection of personal data, it is also true that through the numerous references to additional national or possibly European regulations made in various articles, there is the risk that substantial differences will remain in place between the various legal systems. In this sense, therefore, the Regulation does not appear to be able to achieve the purpose set by the European legislator. These references risk creating uncertainties regarding the application and enforcement of safeguards for the right to the protection of personal data and confusion between those who need to use the data. Such legal uncertainty is an important defect, as it creates serious difficulties for the system itself, being unable to guarantee continuity, effectiveness and overall stability with respect to the values on which the so-called (constitutional) *social contract* is based.

In precise relation to the uses of personal data for purposes of archiving in the public interest, scientific, historical or statistical research, Article 89 allows derogations from the Regulation's articles that govern, for example, the

FIGURE 2. Protection of data as fundamental right.



right of access to data by the data subject (Article 15) and the right to rectification (Article 16), through generic references to national or European rules which are not however specifically identified. In so doing, effectiveness of protection as well as identification and management of sanctioning mechanisms will be very difficult.

All this will complicate the work of researchers, who will no longer know with certainty whether the use they are making of information and data of third parties is lawful.

Taking into account the framework of principles of reference as referred to earlier, with particular reference to Article 2 of the Oviedo Convention, [13] another critical aspect is the provision of derogations, for example, from the right to be let alone, the right to object or to use particular categories of data that carry a high risk of discrimination (Article 9 of the Regulation). These are, in fact, rights included in the broad sense of the protection of *privacy*, as outlined above, whose balance with 'the public interest', also for the purposes of archiving, would require a specific assessment, almost case by case, which does not appear to have been taken into consideration by the Regulation (see Figure 2).

The regulation on data protection: analysis and prospects for scientific research

Examining the Regulation in order to grasp its scope and the prospects in relation to scientific research involves a laborious task of analysing the details and "twists" hidden between one provision and the next, devoid essentially of a coherence. Despite this, the document devotes many provisions to scientific research and acknowledges explicitly that "By coupling information from registries, researchers can obtain new knowledge of great value … On the basis of registries, research results can be enhanced, as they draw on a larger population … Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people …".

In any case, we must identify - above all in the preamble, but also in the main body of the Regulation - the provisions that may be found to be applicable in the field of clinical-scientific research and patiently connect them to each other (see Figure 3).

Firstly, with a view to clearing up any lingering doubt, the legislator in the initial pages of the Regulation, clarifies the issue of anonymity of encoded data, through which the identity of the data subject can be traced - directly or indirectly with reasonable means - which must be considered personal data to all effects. That principle, now fully consolidated in Italy following the Guidelines of the Data Protection Authority18 (24 July 2008), was still being debated in some EU member states at that time, generating significant legal-operational difficulties in *multi-*

country clinical studies.

As already specified, reasonableness, used as a parameter in assessing the possibility of identifying the subject, is included in the set of factors - including mainly cost and time – necessary for the identification operations, taking account of the available technologies at the time of processing.

The data encoding operation is given the new name of "pseudonymisation", thereby referring to the moment that the personal data cannot be attributed to a certain person, other than with the use of additional information (to be stored separately and with the support of every necessary security measure).

In the aforementioned provisions we find the typical flow of data collected and processed for the purpose of clinical research: full identification of the subject in the original source accessible by the Investigator (for example, in the medical records), data transfer with elimination of direct identifiers onto a new medium (for example on electronic-Case Report Form), accessibility to the new database also by other persons involved in the research (for example CRO, Sponsor).

In this respect, there is nothing new in Italy.

There is also nothing new regarding the data subject's consent. In fact, the centrality of consent as a requirement for the legitimacy of data processing, also in the field of research, is still confirmed in general, and the need to respect what is established in EU Regulation no. 536/2014 is explicitly cited in that regard.

Consent – informed, relating to the purposes and always revocable - of the patient involved in clinical research is reiterated as the main basic criterion on which to "measure" the lawfulness of the processing operations.

However, it is precisely in relation to consent that the main "snags" in normative rigidity are found. These open up prospects of greater freedom in the processing of personal data for research purposes.

The first innovation, introduced in recital 27, concerns the non-applicability of the personal data processing regulation to data of deceased persons.

Considering to the 2009-2012 period and the numerous authorisations of the Italian Data Protection Authority in relation to the issue of processing the data of deceased persons with exemption from consent and the general authorisation of the Italian Data Protection Authority in December 201219 (n. 85, 2012, January 1), the scope of the provision is immediately grasped (Authorisation to IEO, April 16, 2009; Authorisation to University Bodeaux, April 27, 2010; Authorisation to ISS, November 11, 2010; Authorisation to ISS, January 19, 2011; Authorisation to Roche, September 16, 2010; Authorisation to IRCSS Istituto Naz. Tumori Milano on July 14, 2011; Authorisation to Az. Serv. San. Trento on February 9, 2011; Authorisation to Celgene July 21, 2011; Authorisation to IRCCSS San Matteo Pavia, September 22, 2011; Authorisation to AIOM September 22, 2011; Authorisation to Az. Osp. RE, October 11, 2011; Authorisation to Bayer December 1, 2011; Authorisation to Az. Osp. Univ. Pisa January 20, 2012; Authorisation to Az. Osp. S. Orsola Bologna January 25, 2012; Authorisation Boheringer Ingelhaim January 25, 2012; Authorisation to Celgene Febraury 2, 2012).

Another important provision regarding clinical research is found in the preamble of recital 33, also a final addition, concerning the recommendation that, at the time of collecting data for treatment purposes, patients are permitted to express their consent to some fields of scientific research, provided that the ethical standards issued in that regard are respected. The general authorisation of the Italian Data Protection Authority, no. 85/2012 (and subsequently renewed) already contained such guidelines, but they had only been half-heartedly accepted as they appeared to be inconsistent with the principle of relevance of consent to the specified purpose. The Regulation, on the other hand, states and clarifies that "it is often not possible to fully identify the purpose of personal data processing for scientific research at the time of data collection."

It is, therefore, foreseeable that clinical centres will take steps - where they have not already done so - to implement *templates* of data processing consent, including in them also the general purpose of clinical-scientific research, albeit with reference to certain fields of research.

The possibility of consent expressed for a general purpose is a prelude to a further clarification contained in the Regulation (set out in recital 50), regarding the possibility of using the data subject's consent for purposes other than those for which the data was initially collected. This is so where such action is "compatible" with the purposes initially declared, albeit with reference to the possibility for the individual member states to specify the duties on those who are performing the processing. The proposition goes even further, stating that further processing for scientific research should in any case be considered "compatible lawful processing" and that, in any case, to assess compatibility with the initial purposes, consideration must be given to the following: any link between the initial purposes and the purposes of the intended further processing; the context in which the personal data have been collected; the reasonable expectations of data subjects based on their relationship with the controller as to the further use; the nature of the personal data; the consequences of the intended further processing; and, finally, the existence of appropriate safeguards during all processing.

The common thread running through this part of the preamble is found in the provision set out in Art. 14, Paragraph 5, Letter b) of the Regulation (consistent with what is set out above although not of identical content): the provision of information to the data subject is not necessary where communicating the information proves impossible or would involve a disproportionate effort and, particularly in the field of scientific research, if it risks rendering impossible

or seriously impairing the achievement of the purpose of the research (on this point, we find full continuity of and consistency with the current Italian *Privacy* Law, the Code of Ethics [20] in relation to processing for the purposes of scientific research and the measures of our Data Protection Authority in relation to clinical research).

The above interpretation is, if anything, confirmed by the provision inserted into recital 53, according to which special categories of personal data meriting a higher level of protection (such as health data) should be processed for health-related purposes, also understood as being to the "benefit of natural persons or society as a whole", since, by express provision, those purposes connected to health also include scientific research, useful for achieving objectives in the public interest.

Ultimately, the following appear to be the European responses to the requirements expressed in a harmonised manner by the world of clinical research (including users of administrative databases and private research funders – recitals 157-159):

- no need for consent for processing of data of deceased persons;
- possible use of consent expressed at the time of data collection in the clinical centre with reference to the purpose of general sectors of scientific research, irrespective of the assessment of compatibility;
- possible use of data with subsequent purposes different from those initially declared, subject to assessment of compatibility between initial and subsequent purposes;
- no need for consent where the communication risks rendering impossible or seriously impairing the achievement of the purposes.

As against these possibilities, with the objectives of consistency of the normative rules and the freedom of movement of data, the system of obligations and responsibilities imposed upon data processing operators (Data Controller and Data Processor) is, however, strengthened and the sanction system is tightened.

With the system of notifications to the control authority abandoned, as it was found to be ineffective, data processing controllers and processors (also for the purpose of scientific research) must:

- adopt internal policies or measures that are designed to satisfy the principles of data protection, with a view to ensuring respect of the principles of pseudonymisation and minimisation of processing ("*protection by design*");
- implement adequate technical and organisational measures, with a view to ensuring that only personal data necessary for each specific purpose is processed ("*protection by default*");
- ensure the continuous confidentiality, integrity, availability and resilience of the systems;
- adopt procedures for the prompt recovery of data in the event of deletion or loss;
- adopt procedures to prove, verify and regularly assess the effectiveness of the aforementioned security measures.

In this regard, systems of certification, seals and security labels are encouraged, as elements that may facilitate the demonstration of conformity with the above-mentioned requirements, along with the adoption of codes of conduct.

In addition, entities that systematically process data must keep a record of the processing activities performed under their responsibility. They will also be required to appoint a data processing officer ("*Privacy Officer*"), with proven expertise and reliability, not subject to hierarchical powers and equipped with the power of expenditure.

The control authorities will prepare a list of the types of processing subject to the precondition of the drafting of a document entitled "Assessment of the impact of planned processing on the protection of personal data".

Lastly, the controllers and processors must ensure the effectiveness of the right to data portability, i.e. the possibility of the data subject to receive his or her data in a "structured, commonly used and machine-readable format" and to obtain its transfer to another processing controller, without impediments.

It seems clear that the requirements placed on the processing controllers and processors are much more demanding and that, depending on the complexity of the business, it will be necessary to employ fully-fledged "*Privacy* Managers".

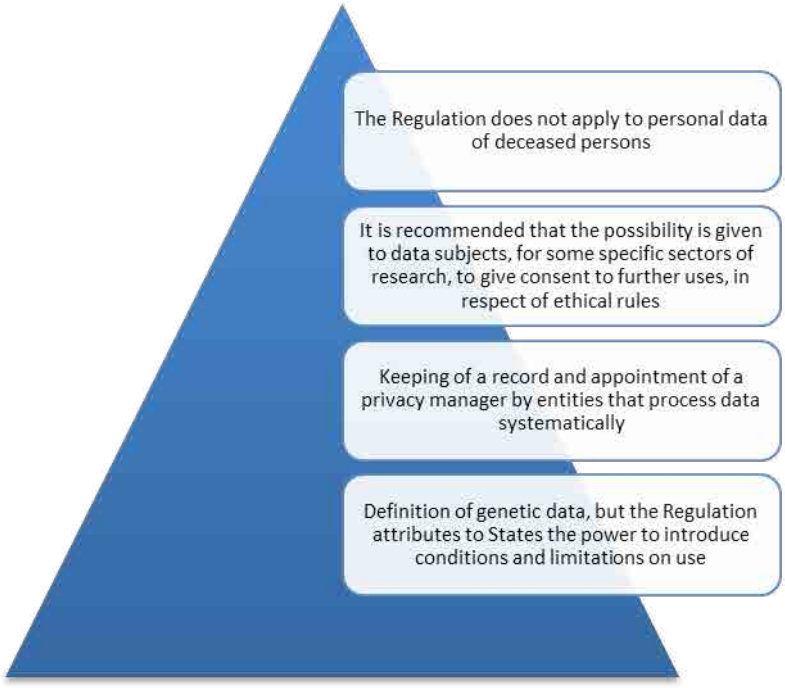
In the event of infringements, these are subject to the application of the administrative pecuniary sanctions provided by Art. 83 of the Regulation at a fixed or proportional amount parameterized according to the company's total annual global turnover; it is not clear if this is of the individual company or the group). Infringements must be reported by the perpetrator within 72 hours, where feasible (Art. 33).

The aforementioned administrative sanctions are without prejudice to civil liability for compensation for damages, with respect to which is established that the controller and the processor should compensate the entire damages sufferend by the person, and criminal liability, whose determination is entrusted to the individual member states.

Lastly, in the Draft Regulation, responding to a generalised requirement for clarity and uniformity, the European Union defines the category of genetic data, as that "relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained" (recital 34).

Probably aware of the risks entailed in, and the unpredictability of the consequences of the processing of

FIGURE 3. Use of personal data.



genetic data, the European legislator lacks the courage to go further: thus the power to introduce conditions and limitations with regard to the processing of genetic and biometric data is left to the various member states, albeit with a recommendation not to hinder the free movement of data within the Union.

Therefore, the taboo subject surrounding the processing of genetic data is not broken and a "middle way" solution is adopted which seems to lay a real trap at the frontiers of scientific research in the genetic field.

RESULTS

Informed consent and the collection of data for scientific research purposes

Informed consent is a legal requirement today. In particular, it represents the means by which concrete implementation is given to the fundamental right to individual self-determination (see Figure 4).4 There are various areas in which informed consent must be requested from the data subject by those intending to use his or her data and information. If we consider, by way of example, the area of scientific research, human trials and clinical practice, we see that informed consent has become an essential requirement before involving persons in scientific research or trials, or for performing surgery or administering therapeutic treatments. The consent from those in question in these cases is a consent to participate in specific research or trials whose peculiarities, risks and benefits are broadly specified to the participant who, therefore, by way of his/her informed consent, expresses his or her informed and free will to participate in the study. Consent to therapeutic and/or surgical treatment is moving in the same direction, where a person decides whether or not to undergo the same after the doctor has provided adequate information. The completeness and non-manipulation of the information is, in these cases, fundamental to forming the sufficient awareness, understood as the prerequisite for exercising full self-determination.3 With regard to the Italian legal system, the Constitutional Court clarified this point in ruling no. 438/2008: "The fact that the informed consent finds its basis in Articles 2, 13 and 32 of the Constitution highlights its function as a synthesis of two fundamental rights of the person: that of self-determination and that of health, as, while it is true that every individual has the right to be treated, he has, also, the right to receive the necessary information in relation to the nature and possible developments of the therapeutic course to which he is subjected, as well as any alternative therapies; information that must be as comprehensive as possible, precisely for the purpose of ensuring the free and informed decision by the patient and, as such, his personal freedom, in accordance with the second paragraph of Art. 32 of the Constitution."

In the case of processing data collected for the purposes of research and trials, the informed consent, necessary so that those obtaining the data of the data subject can use it legitimately, should not be confused with the consent referred to above. This is in fact a different

moment with respect to the consent to participate in research or to undergo therapies, which therefore requires the provision of a separate form, clarifying the purposes for which the data will be used, the duration of its storage and the criteria for ensuring data security. In relation to the distinction between the types of consent, recital 161 of the Regulation refers to the provisions of (EU) Regulation no. 536/2014 of the European Parliament and Council, for the purposes of consent to the participation in and the activity of scientific research as part of clinical trials. That regulation entered into force in May 2016.

Based upon the last issue highlighted, i.e. the need for a distinction between consent to the processing of data and other types of consent, for example, to participation in a trial, it is specified at article 7 of the Regulation: *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2.If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3.The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4.When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.* If the consent is given in the context of a written declaration which also concerns other matters, the request for said consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Article 7 again specifies, at paragraph 3, the right to withdraw consent to the use of the data at any time, as the expression of the effective power of control of the data subject who provides the data. As regards this point, the same article underlines that both giving or withdrawing consent to the use of personal data ought to be two equally simple procedures, that is, not burdensome for individuals providing their data to third parties. This specification in Article 7 is the final outcome of a heated debate about the need for simplification of the procedure of withdrawing cosent, as in many cases it was excessively and unjustly onerous for the data subject.

It is also stated that before consent is given, the data subject is informed that his or her withdrawal will not have negative implications on the lawfulness of the data processing based upon the consent given prior to the withdrawal.

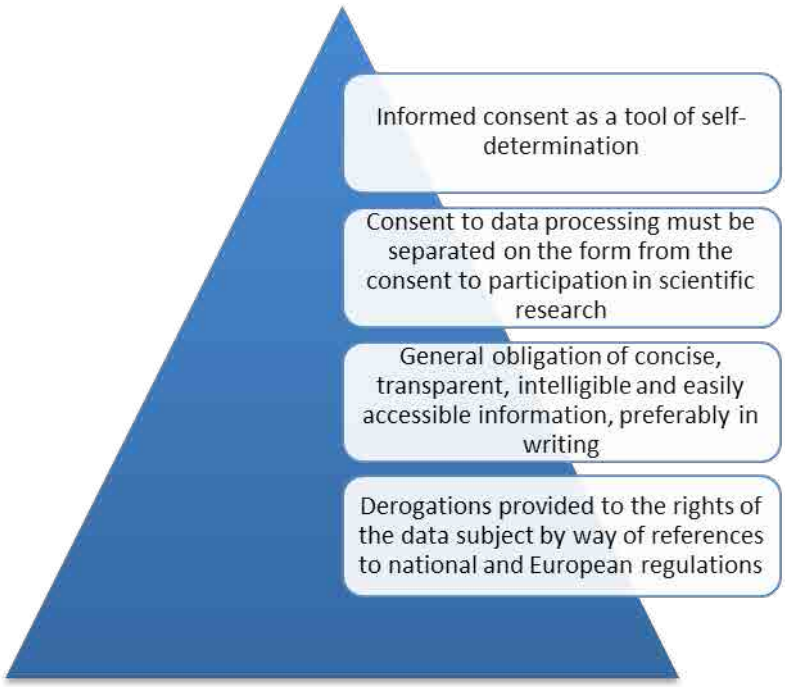
It can, therefore, be stated that the Regulation generally respects the objective - upheld over time - of ensuring the exercise of the right to self-determination, to the greatest possible extent, through the effective control of one's data and respective information. However, certain derogations provided for the activities subject to analysis in this paper are not free of crtical issues. Before focusing attention on this aspect, it is necessary to complete the round-up of the articles that guarantee active control of data, at least generally. Chapter III of the Regulation is entitled "Rights of the Data Subject" and it opens with a direct reference to transparent information and communication. In order to achieve these objectives, Article 12 imposes upon the data controller the duty to take appropriate measures to allow the rights provided by subsequent articles to be given effect. In particular, measures should be taken to ensure that the information is concise, transparent, intelligible and easily accessible, preferably provided in writing. In addition, the processing controller must take steps to facilitate the exercising of the right of access to data (Article 15), the right to rectification (Article 16), the right to erasure (Article 17), the right to objection (Article 21).

This framework of rules confirms the intention of the European legislator – expressed a number of times - to ensure facilitated access to the data and better information regarding the fate of the personal data once it has been shared.

While all this is true, it should, however, be noted that the very effectiveness of the power of control over one's data is flawed or, at least open to criticism with regard to the use of data for archiving in the public interest, for purposes of scientific, historical and statistical research. Given that the Regulation includes the consent of the data subject among the requirements for the lawful processing of the data (Article 6), it does not, however, make it a requirement that is due at all times. It provides, in fact, that the processing of data may be considered lawful if and to the extent that at least one (alternatively and not simultaneously) of the requirements listed in the mentioned article is present.

The processing necessary for conducting an activity in the public interest (Article 6, 1e) is therefore lawful, irrespective of the informed consent. However, in the case of processing data for the purposes of archiving in the public interest, it seems that ab origine there must be consent by the data subject, but then Article 89, 3 provides the possibility for European or national law to prescribe derogations to the rights intrinsically connected with the informed consent previously acknowledged, i.e. those provided by Articles 15, 16, 17, 18 and 19. The very derogation of those rights renders control over one's information ineffective. The question arises as to why, in the case of the archiving of data - an activity in which public interest plays a predominant role - the Regulation has chosen to take such a contorted path, dotted with derogations by way of reference to national regulations,

FIGURE 4. Informed consent and self-determination.



only then to give prevalence to public interest over the rights of the data subject, when the reference to Article 6, 1e could actually have been sufficient.

Similar comments must be made with reference to data processing for scientific, historical and statistical purposes. In this case too, given informed consent as a prerequisite, there is the prospect of the derogation of rights provided for the direct control of one's information, mostly by way of reference to national or European rules, which are not identified in detail, when such rights apparently protected by the aforesaid provisions of the Regulation "are likely to render impossible or seriously impair the achievement of the specific [public interest] purposes and such derogations are necessary for the fulfilment of those purposes."

CONCLUSIONS

It is still early for the consideration of the new Regulation, in relation to which the transition period before it definitively comes into force in 2018 will be useful for making a complete and detailed assessment of its adequacy. However, it is reasonable to envisage that there will be no innovations of particular significance for scientific research operators in relation to personal data processing, other than in the area of governance (with an increase in organisational and security obligations).

Consent remains the main criterion to "measure" the legitimacy of processing, subject to exceptions where there may be.

In particular, research on administrative databases is regulated in the same manner as processing for the purposes of retrospective observational research. However, it is precisely with reference to the collection of retrospective personal data that the greatest innovations are seen. It will therefore be interesting to follow the interpretative evolution of the principle of compatibility of purposes which renders – in fact – personal data already collected usable, even in the absence of consent from the data subject.

For the time being, any comprehensive response should be deferred, as this is non-exhaustive legislation that has intentionally left broad discretional space for concrete decisions to the national authorities and to European board dealing with multi-country issues.

It is entirely likely that a second level legislative production will soon start (for example, specific authorisations of data protection authorities and guidelines), similar to that already inaugurated and trialled successfully by the Italian Data Protection Authority. This will represent an adequate way to respond to the requirements of rapid change that science requires.

SISMEC "Observational Studies" working group members. Coordinators. Gesuita Rosaria (Polytechnic University of Marche, Italy) Villani Simona (University of Pavia, Italy), Zambon Antonella (University of Milan-Bicocca, Italy). Members. Montomoli Cristina, Morandi Anna, Stendardo Antonietta († Deceased); Accordini Simone (University of Verona, Italy); Banfi Francesco, Patarnello Francesca (Amgen, Milano, Italy), Pitrelli Andrea (GlaxoSmithKline Italia, Verona, Italy); Biasi Valeria

Schematic summary of relevant changes introduced by the EU Regulation compared to the current legal situation.

OBLIGATIONS	ITALIAN LEGISLATIVE DECREE 196/2003[21]	EU REGULATION 2016/679
Notification to the Authority	YES	NO
Information to the data subject	YES	YES
Consent of the data subject	YES	YES
Minimal security standards	YES	NO
Adequate security measures	YES	YES
Data Protection Officier	NO	YES
Data Protection Impact Assessment	NO	YES
Prior consultation of the supervisory authority	NO	YES
Protection by design/ default	NO	YES
Records of processing activities	NO	YES
Certification mechanism	NO	YES (optional)
Notification of a personal data breach to the supervisory authority	NO	YES

(University Hospital of Verona, Italy); Baldi Ileana, Gregori Dario, Frigo Annachiara (University of Padua, Italy), Volpato Sandra (Self-employed, Padova, Italy); Campari Cinzia, Vicentini Massimo (Local Health Unit of Reggio Emilia, Italy); Preite Francesca, (Law Firm of Miari-Preite, Reggio Emilia, Italy - MediNNeos S.u.r.l., Modena, Italy); Simoni Lucia (MediNeos S.u.r.l., Modena, Italy); Molinaro Sabrina (National Research Council, Pisa, Italy); Galassi Gianmichele (University of Siena, Italy); Flavia Carle, Ferrante Luigi (Polytechnic University of Marche, Italy); Vestri Annarita (University of Rome "La Sapienza", Italy); Chiodini Paolo (Second University of Naples, Italy); Trerotoli Paolo (University of Bari, Italy); Guardabasso Vincenzo (University Hospital of Catania, Italy); Minerba Luigi (University of Cagliari, Italy); Palmas Maria Antonietta (Healthcare Department of Region Sardinia, Italy); Solinas Giuliana, Sotgiu Giovanni (University of Sassari, Italy).

References

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)
2. Rodotà S., Tecnologie e diritti. Bologna: Il Mulino 1995
3. Rodotà S., La vita e le regole, Milan: Feltrinelli, 2007
4. Rodotà S., Il diritto di avere diritti. Rome-Bari: Laterza, 2012
5. Borsellino P. Bioetica tra 'morali' e diritto. Milan: Raffaello Cortina, 2009
6. Beachamp T.L, Childress J.F., Principles of Biomedical Ethics. New York: Oxford University Press, 2013
7. Buttarelli G., Banche dati e tutela della riservatezza. Milan: Giuffré, 1997
8. Westin A., Privacy and Freedom, New York: Atheneum, 1970
9. Scarpelli U., Diritti positivi, diritti naturali: un'analisi semiotica, in S. Caprioli, F. Treggiari (ed), Diritti umani e civiltà giuridica,, Perugia: Centro Studi Giuridici e Politici, 1992
10. Kelsen H., Lineamenti di dottrina pura del diritto. Turin: Einaudi, 1952
11. Ferrajoli L., Principia Juris. Rome-Naples: Laterza Editori, 2007
12. The Charter of Fundamental Rights of the European Union (Charter of Nice) 2000
13. Convention on Human Rights and Biomedicine (Oviedo Convention) 1997
14. Treaty on the Functioning of the European Union (TFUE) 2007
15. Salardi S., Test genetici tra determinismo e libertà. Turin: Giappichelli, 2010.
16. Piga A. Comunicare o non comunicare: il problema degli incidental o unexpected findings, in Notizie di Politeia, 2012, 108.
17. Additional Protocol to the Convention on Human Rights and Biomedicine on biomedical research 2005
18. Guidelines of Italian Data Protection Authority on clinical trials 2008
19. General Authorization of Italian Data Protection n. 85/2012
20. Code of Ethics in relation to processing for scientific and statistic purposes 2004
21. Italian Legislative Decree N. 196 /2003