

Data protection and the processing of personal data of very preterm (VPT) and very low birth weight (VLBW) children for scientific health research

A proteção de dados e o processamento de dados pessoais de crianças nascidas muito prematuramente ou com peso muito baixo para a investigação científica na área da saúde

Inês Camarinha Lopes

Invited assistant at Faculdade de Direito da Universidade do Porto (FDUP); Collaborating researcher at Centro de Investigação Jurídico Económica (CIJE)

ilopes@direito.up.pt

<https://orcid.org/0000-0001-8624-3078>

Rua dos Bragas, 223 4050-123 Porto, Portugal

Julia Doetsch

Research assistant at the EPIUnit – Instituto de Saúde Pública, Universidade do Porto
External PhD student at Maastricht University, Faculty of Health, Medicine and Life Sciences (FHML), School of Public Health and Life Sciences (CAPHRI)

jndoetsch@ispup.up.pt

<https://orcid.org/0000-0003-1388-9542>

Rua das Taipas, 135, 4050-600 Porto, Portugal

Maria Regina Redinha

Assistant Professor at Faculdade de Direito da Universidade do Porto (FDUP); Coordinator and integrated researcher at Centro de Investigação Jurídico Económica (CIJE)

redinha@direito.up.pt

<https://orcid.org/0000-0001-6216-6266>

Rua dos Bragas, 223 4050-123 Porto, Portugal

Henrique Barros

Professor of Epidemiology at Departamento de Ciências da Saúde Pública e Forenses e Educação Médica, Faculdade de Medicina, Universidade do Porto, Porto, Portugal; Director of the Instituto de Saúde Pública, Universidade do Porto

hbarros@med.up.pt

<https://orcid.org/0000-0003-4699-6571>

Rua das Taipas, 135, 4050-600 Porto, Portugal

September 2019

ABSTRACT: The present article emerges from the project 'RECAP preterm – Research on European Children and Adults Born Preterm' which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 733280.

Under this project, a report, whose objective was to describe and compare the Challenges and Opportunities of Record-Linkage Processes, was developed by an ISPUP partner and presented in September 2019.

Now, we discuss the issue focused on General Data Protection Regulation (GDPR) and national law, with a critical view as to how the legal regime for accessing routinely collected health and educational data and its subsequent processing for research purposes.

The main results of this article are the reflection on the difficulties that scientific research faces and the consideration of future legislative changes in a world where data protection is a priority policy concern.

Although scientific research in health is recognised by International, European and National law as an asset for the development of society, this article seeks to demonstrate that the possibilities for access and use of personal data, including sensitive data, are not broad.

KEY WORDS: Personal data; Sensitive data; Health data; General Data Protection Regulation; Consent of the data subject; Scientific research.

RESUMO: O presente artigo surge no âmbito do projeto 'RECAP preterm – Research on European Children and Adults Born Preterm' financiado pelo programa de investigação e inovação European Union's Horizon 2020 com acordo de financiamento N.º 733280.

No seio deste projeto, o ISPUP desenvolveu um relatório cujo objetivo foi descrever e comparar os desafios e as oportunidades do processo de recolha e ligação de dados, apresentado em Setembro 2019.

Agora, procuramos discutir o tema focando-nos no Regulamento Geral de Proteção de Dados (RGPD) e na lei nacional, analisando criticamente como é o regime legal do acesso aos dados de saúde e educacionais rotineiramente recolhidos e seu posterior uso na investigação científica.

Os principais resultados do presente artigo são a reflexão sobre as dificuldades com as quais a investigação científica se depara e a ponderação de futuras alterações legislativas, num mundo onde a proteção dos dados é uma das preocupações políticas prioritárias.

Apesar de a investigação científica na área da saúde ser reconhecida pelos Direitos Internacional, Europeu e Nacional como uma mais-valia para o desenvolvimento da sociedade, este artigo procura demonstrar que as possibilidades de acesso e uso de dados pessoais, incluindo dados sensíveis, não são amplas.

PALAVRAS-CHAVE: Dados pessoais; Dados sensíveis; Dados de saúde; Regulamento Geral de Proteção de Dados; Consentimento do titular dos dados; Investigação científica.

SUMMARY*:

1. Introduction

2. Routinely collected data (RCD)

2.1. The consent of the data subject for the access of RCD and subsequent processing of sensitive data (article 9/2/a) of GDPR) and non-sensitive data (article 6/1/a) of GDPR)

2.2. Scientific research purposes as a lawful ground to process sensitive data – article 9/2/j) of GDPR

2.3. The lawful ground - Consent versus scientific research

2.4. Coordination of the National law with the GDPR

3. Realisation of a clinical study – the provisions established by the 21/2014 act

3.1. Realisation of a clinical study with minors

4. Conclusion

References

Case law

* This article was developed under the RECAP preterm project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 733280. The authors Inês Camarinha Lopes and Julia Doetsch were hired by the RECAP preterm project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 733280.

1. Introduction

Health research is an ancient activity which began around the 5th century B. C. and increased greatly after the XIX century. It is an unquestionable fact that scientific research¹ in this area is an imperative necessity for the development of knowledge in medicine and for progress in society, preventing diseases, discovering treatments and contributing to a healthy lifestyle.

However, the possibilities for using personal data,² including sensitive data, even for scientific research purposes, which are recognised by International, European Union and National laws, exist but they are not broad.

Scientific research in the area of health (especially the study of preterm babies, the majority which have low birth weight as well), needs to process health data,³ which is considered sensitive bearing in mind the higher risk of discrimination of the subject (recital 51 of GDPR), where the risks increase when the data subject is underage, as they are considered a vulnerable data subject.⁴ Therefore, it is not an activity that is able to ignore the right of

¹ Regarding the concept of scientific research the Handbook on European Data Protection law says: "It [the GDPR] provides for the broad interpretation of the processing of personal data for scientific research purposes, including technological development and demonstration, basic research, applied research and privately funded research." EU AGENCY FOR FUNDAMENTAL RIGHTS; COUNCIL OF EUROPE; EUROPEAN DATA PROTECTION SUPERVISOR, *Handbook on European data protection law*, Edition of 2018, Publications office of the European Union, 2018, p. 340.

² Article 4(1) of GDPR adopted a wide concept of 'personal data' which signifies "any information relating to an identified or identifiable natural person ('data subject')." Reading this definition is clear that EU lawmaker gave a broader meaning to the concept of personal data, as it was recognized by the Court of Justice on the following judgements - Judgement of the Court of Justice (2nd Section) of 20-12-2017, Proc. no. C-434/16, Peter Nowak v. Data Protection Commissioner, which considered that exam answers could contain personal data; Judgement of the Court of Justice (2nd Section) of 19-10-2016, Proc. no. C -582/14, Patrick Breyner versus Bundesrepublik Deutschland, which considered the IP address a personal data. Therefore, in our opinion, it is not understandable the restriction on the concept of personal data that was made by the Portuguese "Tribunal da Relação de Lisboa" on its judgement of the 17-05-2017, Proc. no. 842/16.5T8ALQ.L1-3, Relator: Juiza Desembargadora Adelina Barradas de Oliveira.

³ Recital 35 of GDPR gives a broader meaning of "personal data concerning health". The concept provided by the previous Data protection Directive had already a wide interpretation, recognized by the Court of Justice on its judgement of the Court of Justice (1st section) of 6-11-2003, Proc. no. C-101/01, Bodil Lindqvist v. Göta Hovrätt (Suécia). The recent Recommendation CM/Rec (2019)2 of the Council of Europe, on its paragraph 3, adopt the definition of "health related data", which is broader than the concept of "medical data" adopted by the previous Recommendation No. R (97)5 of the Council of Europe, on its paragraph 1.

⁴ As GDPR says on its recital 18, "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. (...). The biggest threat to children's personal data is the digital world, where their personal data is processed oftentimes without safeguards and illegally. Transcribing Damin Park, "Of the more than 5000 apps examined over 50% of the Google Play apps meant for children under thirteen seemed to fail at protecting data. According to the study, the apps often sent "potentially sensitive information - including device serial numbers, which are often paired with location data, email address, and other personally identifiable information - to third-party advertisers. More troublingly, more than 90% of those apps were those "transmitting identifiers", which are akin to "hardware serial numbers that allow for long-term tracking and cannot be changed or deleted." Later, Damin Park described the "interactive digital toys" such as Mattel's "Hello Barbie". This new smart toy "records a child's voice, sends the recording to the Cloud, uses voice recognition software to decode the content, and learns the child's name, conversational styles, habits and interests", so it collects biometric data, which is considered sensitive data under the terms described by article 9/1 of GDPR: DAMIN PARK, *Mining for Children's Data in Today's Digital World*, 2018. Retrieved from: https://heionline.org/HOL/Page?public=true&handle=hein.journals/jnaa38&div=16&start_page=320&collection=journals&set_as_cursor=0&men_tab=srchresults (30/4/2019).

Regarding the risks of the "Digital Age" for children's data see also: KATHRYN MONTGOMERY; JEFF CHESTER, "Data Protection for Youth in the Digital Age", in *European Data Protection Law Review*, 2015. Retrieved from: https://heionline.org/HOL/Page?public=true&handle=hein.journals/edpl1&div=55&start_page=277&collection=journals&set_as_cursor=0&men_tab=srchresults (10/4/2019), which analyses the history and evolution of the Children's Online Privacy Protection Act (COPPA), of United States, whose development was influenced by EU law - "But the US government was also under increasing pressure from the European Union to establish privacy laws that would bring the United States in line with the EU's 1995 Data Protection Directive." (pp. 277 and 278).

personal data protection and the right to respect private and family life.⁵ However, a lawmaker cannot disregard its potential contribution regarding a future decrease in preterm babies, which apart from the benefits for its own life also reflects on the future costs to the National Health Service.

The birth weight of a child is defined by World Health Organisation (WHO) as “The first weight of the fetus or new born obtained after birth. For live births, birth weight should preferably be measured within the first hour of life before significant postnatal weight loss has occurred.”⁶

Categories of low birth weight (LBW), very low birth weight (VLBW) and extremely low birth weight (ELBW) are defined by WHO as less than 2500g; less than 1500g and less than 1000g, respectively.⁷ According to the *European Perinatal Health Report – Core indicators of the health and care of pregnant women and babies in Europe in 2015*, “Babies with very low birth weights, weighing less than 1500 grams, face the highest short and long term risks.”⁸

A child is born preterm when the birth occurred at the end of less than 37 completed weeks (less than 259 days) of gestation.⁹ Very preterm (VPT) babies are considered those who are born before 32 weeks of gestation, “the most vulnerable, with rates of infant mortality between 10% and 15% and of cerebral palsy between 5% and 10%.”¹⁰

Children born VPT and with LBW have increased in Portugal in the last decade. The percentage of live births with LBW (less than 2500g) was 8.3% in 2010 and increased to 8.9% in 2015.¹¹ Within 85,762 live births in 2015 in Portugal 1% were born with less than 32 weeks of gestation (VPT babies), and 7% were born between 32 to 36 weeks of gestation.¹²

⁵ The rights of personal data protection and the right to respect private and family life are considered fundamental rights constitutionally protected by articles 35 and 26/1 of Constitution of the Portuguese Republic (CRP), respectively. Another dimension of these rights is the private one, as personality rights protected by the Portuguese Civil Code (CC) on its article 70/1 and 2 and article 80. On one hand, the right of personal data protection is framed by the general personality right, predicted on article 70/1 of CC. On the other hand, article 80 of CC predicts the right to reserve on the intimacy of private life, which is particularly relevant in relation to health data that are part of the most private reserve sphere. However, the realization of this right depends on the specific case. - according to: PIRES DE LIMA; ANTUNES VARELA, *Código Civil Anotado*, Vol. I., 4th edition revised and actualised, Coimbra, Coimbra editora, 2010. However, the risks for children data subject’s rights and the benefits of the scientific research in the area of health cannot be compared to those of the digital world, where the risks are much higher and the benefits for children are small and debatable. Regarding the personality rights, especially right to reserve on the intimacy of private life and the general personality right see: ORLANDO DE CARVALHO, (COOR. BY FRANCISCO LIBERAL FERNANDES, MARIA RAQUEL GUIMARÃES, MARIA REGINA REDINHA, *Teoria geral do direito civil*, 3rd edition, Coimbra, Coimbra editora, 2012, pp. 147 ff. and CARLOS ALBERTO DA MOTA PINTO, *Teoria geral do direito civil*, 4th edition, Coimbra, Coimbra editora, 2005, pp. 199 ff.

⁶ WHO ORGANIZATION, *International statistical classification of diseases and related health problems (ICD-10)*, WHO library cataloguing-in-publication Data, 10th revision, vol. II, 2010, p. 151. Available in: https://www.who.int/classifications/icd/ICD10Volume2_en_2010.pdf.

⁷ WHO ORGANIZATION, *International statistical classification of diseases and related health problems (ICD-10)*, 2010, p. 131.

⁸ EURO-PERISTAT PROJECT, *European Perinatal Health Report – Core indicators of the health and care of pregnant women and babies in Europe in 2015*, November 2018, p. 123.

⁹ These information were retrieved from: Wh Organization, *International statistical classification of diseases and related health problems (ICD-10)*, 2010, pp. 151 and 152.

¹⁰ EURO-PERISTAT PROJECT, *European Perinatal Health Report – Core indicators of the health and care of pregnant women and babies in Europe in 2015*, November 2018, p. 131.

¹¹ EURO-PERISTAT PROJECT, *European Perinatal Health Report – Core indicators of the health and care of pregnant women and babies in Europe in 2015*, November 2018, p. 129.

¹² EURO-PERISTAT PROJECT, *European Perinatal Health Report – Core indicators of the health and care of pregnant women and babies in Europe in 2015*, November 2018, pp. 131-135.

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, known as General Data Protection Regulation (hereinafter designated GDPR) contrary to the previous data protection directive (Directive 95/46/CE), it is directly applicable over the member state's own legal system without the need to be specifically incorporated into it. However, with the flexible way as to how GDPR regulations were established, Member States still have freedom in certain aspects to define the outlines of the legal regime, in contrary to the usual harmonisation of laws under the European Union.¹³

Because of the aforementioned freedom, the Portuguese Parliament sought views from several entities that ended with the approval of the proposal of law 120/XIII. The discussion culminated on the 14 of June 2019 with the approval of the "Lei 58/2019, de 8 de Agosto" (58/2019 Act). This Act was published on the 8th August of 2019 and came into force on 9th August, the day after its publication, according to its article 68. For an Act of this importance and dimension, 24 hours between its publication and its entrance into force (its *vacatio legis*) is not satisfactory¹⁴ and may be considered a violation of the Constitution of the Portuguese Republic (CRP) that guaranteed a Democratic State of Law by its article 2.¹⁵

On the 14th June 2019 the 59/2019 Act, that incorporated the Directive (EU) 2016/680 of the European Parliament and of the council of 27 April 2016, was also approved. This Directive is related to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data. As this goes beyond our theme, we do not examine this directive and National Act.

Beyond the 58/2019 Act, there are a few other National laws that are relevant to the delicate area of scientific research in health. However, these acts were made during the time when the revoked Data Protection Directive and the "Lei 68/97, de 26 de Outubro" (68/97 Act, of the 26 of October) that incorporated it were in force. They were not modified, at least up until now, with the arrival of GDPR. Nevertheless, in case of contradiction between the

¹³ This opinion is shared by Alexandre Sousa Pinheiro, Daniel Rücker and Tobias Kugler - ALEXANDRE SOUSA PINHEIRO (COORD.); CRISTINA PIMENTA COELHO; TATIANA DUARTE; CARLOS JORGE GONÇALVES; CATARINA PINA GONÇALVES, *Comentário ao Regulamento Geral de Proteção de Dados*, Lisboa, Almedina, 2018, pp. 97 ff.; and TOBIAS KUGLER; DANIEL RÜCKER, *New General Data Protection Regulation*, C.H.Beck, Hart, Nomos, 2018, p. 2. Afonso Araújo Neto states that GDPR is an 'invisible revolution' which changed the way of doing the security of information, as the current is not enough nowadays - AFONSO ARAÚJO NETO, *RGPD: "Uma revolução invisível"*, in *Revista Luso Brasileira de Direito do Consumo*, Vol. VII, no. 27, 2017.

¹⁴ According to the article 5/2 of the Portuguese Civil Code (CC) the period of *vacatio legis* of an act is determined by the lawmaker, who have freedom to determine it, or, in his absence, it is determined by special legislation. The article 2/2 of the 74/98 act of 11 of November establishes five days until entry to force, as a subsidiary term. However, the period of *vacatio legis* should be proportional with the dimension or complexity of the act.

¹⁵ According to Gomes Canotilho and Vital Moreira, a Democratic State of Law is based on the popular sovereignty, imposes to the State the respect and effectiveness of the rights, freedoms and guarantees of the persons and prohibits its arbitrariness. - GOMES CANOTILHO; VITAL MOREIRA, *Constituição da República Portuguesa Anotada - artigos 1º a 107º*, Volume I, 4th edition revised, Coimbra, Coimbra Editora, 2007, pp. 202 ff. The principle of a Democratic State of Law imposes the legal certainty and security, which is affected by the constant changes of the laws and by its precipitated entry into force. Notice that the 58/2019 Act entered into force on the 9 of August and on the 3 of September (less than a month later...) the National Commission of Data Protection (CNPD) approved the "Deliberação 2019/494" (deliberation 2019/494) which disapply a few provisions of the 58/2019 Act on the cases that they will appreciate, considering them nonconforming with the GDPR.

regulation and National law, the law reader has to evaluate if the National law was tacitly revoked by GDPR, which prevails (article 62/1 of 58/2019 Act *a contrario*).

As a result of the foregoing, it can be considered that the European Union's law, form part of National Law and effectively are only separated artificially.¹⁶ Thus, European Union data protection rules, without losing their nature of European law, represent a significant part of the National legal system.¹⁷

Hereinafter, we will focus on the provisions established by laws regarding the access to routinely collected data.

2. Routinely collected data (RCD)

There are several databases that systematically collect personal data and, nowadays, mostly (or even all) data records are saved in an electronic form. These kinds of data records are allowed as they are covered by at least one of the legal backgrounds for the processing of personal data, according to articles 6/1 and 9/2 of GDPR.¹⁸ Article 30 of the 58/2019 Act expressly allows databases or centralised health records, if they are made under the legitimate grounds allowed by GDPR or National law.

The question is if the data routinely collected by hospitals, National Health Service, schools, Minister of Health and Minister of education, and others, can be shared and subsequently used for scientific research purposes in the area of health.

It is noteworthy that article 23/2 of the 58/2019 Act¹⁹ determines that the transmission of personal data between public entities (for example, between a public institute and a public hospital) is *exceptional*, needs to be *grounded* and be under a *protocol*, which should establish the responsibility of each intervener. Being exceptional means that for principle this transmission is not allowed.

¹⁶ Article 8/4 of the CRP establishes the principle of the primacy of the European Union Law, which means that EU law prevails over the National law. This is a classic principle of the EU, affirmed firstly by the Court of Justice of the European Communities (TJCE). – GOMES CANOTILHO; VITAL MOREIRA, *Constituição da República Portuguesa Anotada – artigos 1º a 107º*, p. 202 ff. Regarding this principle, see also MIGUEL GORJÃO HENRIQUES, *Direito da União – História, direito, cidadania, mercado interno e concorrência*, 9th Edition, Almedina, 2019, pp. 358 ff.

¹⁷ This ideia is pursued by Filipa Urbano Calvão, currently the president of the CNPD: FILIPA URBANO CALVÃO, *Direito da proteção de dados pessoais – Relatório sobre o programa os conteúdos e os métodos de ensino da disciplina*, Porto, Universidade Católica Edition, March 2018, pp. 42 and 43.

¹⁸ The Handbook on the European Data Protection Law, regarding the processing sensitive data, says: "A prominent example are electronic health file systems. Such systems permit health data, collected by health care providers in the course of treating a patient, to be made available to other health care providers of this patient on a large scale, usually nationwide", referring to the legal background "substantial public interest" provided by article 9/2/g) of GDPR. – EU AGENCY FOR FUNDAMENTAL RIGHTS; COUNCIL OF EUROPE; EUROPEAN DATA PROTECTION SUPERVISOR, *Handbook on European data protection law*, 2018, p. 163.

¹⁹ This provision, as well as the article 23/1 of 58/2019 Act, was unapplied, among others provisions, by the "Deliberação 2019/494" (Deliberation 2019/494), approved by the CNPD on the 3 of September 2019, on the data processing cases that CNPD will appreciate. This deliberation considered the article 23 of 58/2019 Act contrary to the purpose limitation principle, predicted by article 5/1/b) of the GDPR, and contrary to the article 6/4 of the GDPR. The value of this deliberation is restricted to the CNPD activity and contributes to the transparency, certainty and legal security of its task. At the moment will not be mentioned the author's opinion regarding the compatibility of this provision with the GDPR.

However, when it is accepted may have to be grounded, which requisite will be discussed below.

GDPR establishes in its article 9/1 a prohibition principle for the processing of sensitive data,²⁰ which may be considered a challenge for the controller.^{21 22} However, its article no. 2 predicts ten lawful grounds where that general prohibition is overcome, which can be considered an opportunity for the controller to process this type of data.

Article 9/2(i) of GDPR establishes that the processing of sensitive data is permitted if it is necessary for reasons of *public interest in the area of public health*. This seems to be a lawful ground that could be an opportunity in the view of the researcher to process health data for scientific research in the area of health. Common sense would suggest that scientific research in the area of health could fall under the concept of “public interest”, as it may achieve great developments in medicine and health that would benefit everyone. However, the concept of ‘public health’ in European Union law has a narrow interpretation²³ (recital 54), according to the regulation (EC) no. 1338/2008 of the European Parliament and of the Council. Its Article 3(c) defines “public health” as “all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality.” An example of the application of this ground is the protection against serious cross-border diseases. So, scientific research in the area of health are not part of the concept of public interest in the area of public health.

Now we will focus on the consent of the data subject (articles 6/1/a) and 9/2/a) of GDPR) and scientific research purposes (article 9/2/j) of GDPR) as possible grounds for data processing.

²⁰ Article 9/1 of GDPR considers sensitive the personal data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, 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. Biometric data was considered for the first time in the category of sensitive data. However, biometric data can be considered sensitive or non-sensitive, as GDPR limits biometric sensitive data where they are processed to “the purpose of uniquely identifying a natural person”. As Catherine Jasserand argues, “biometric data are not treated as sensitive by nature, but become sensitive as the result of their use.” – CATHERINE JASSERAND, “Legal Nature of Biometric Data: From generic personal data to sensitive data”, *European Data Protection Law Review*, 2016 Retrieved from: https://heinonline.org/HOL/Page?public=true&handle=hein.journals/edpl2&div=56&start_page=297&collection=journals&set_as_cursor=0&men_tab=srchresults (10/4/2019).

²¹ “Controller” is defined by the article 4/7 of GDPR as whoever determines the means and purposes of processing the personal data if several persons take this decision together they are called “joint controllers”. “Processor” is the natural or legal person that processes personal data on behalf of a controller. The processor becomes a controller if it determines the means and purposes of data processing.

²² Alexandre Libório Dias Pereira refers to the prohibition established by article 9/1 of GDPR as a data subject’s right. – ALEXANDRE LIBÓRIO DIAS PEREIRA, “Big data, E-Health e “autodeterminação informativa”: A lei 67/98, a jurisprudência e o Regulamento 2016/679 (GDPR)”, in *Lex Medicinæ – Revista Portuguesa do Direito da Saúde*, Year 15, No. 29, 2018, pp. 51-70. However, we prefer to consider it a principle that may suffer derogations, those that are predicted by article 9/2 of GDPR. Actually, the prohibition of the process of sensitive data is recognized to protect fundamental rights and freedoms of the data subject.

²³ European Union imposes the autonomous interpretation principle and the interpretation in accordance with its law and jurisprudence of the Court of Justice, which signify that the concepts of the EU are interpreted regardless its meanings on the Member States law. Regarding this principles, see MIGUEL GORJÃO HENRIQUES, *Direito da União – História, direito, cidadania, mercado interno e concorrência*, 2019, pp. 393 ff.

2.1 The consent of the data subject for the access of RCD and subsequent processing of sensitive data (article 9/2/a) of GDPR and non-sensitive data (article 6/1/a) of GDPR)

Regardless whether it is non sensitive or sensitive data, the consent of the data subject is the first lawful ground established by GDPR.²⁴

Article 4/11 of GDPR defines “consent” as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes.” In addition to these requisites, when the data subject is underaged,²⁵ as he/she does not have legal capacity, it will be for the holders of parental responsibility to give their consent.

When the data is collected through the data subject it is obvious that the controller has to seek the data subject’s consent. This task in practice is not easy, as the persons are not willing to give freely their personal data, especially health information, to contribute for scientific research. And this obstacle will only be solved when the potential participants are aware of the benefits and progresses that may be achieved in the future.

The consent given for scientific research purposes, according to the article 31/4 of 58/2019 Act may reach several areas of research or only be given for specific research projects, always respecting the ethical standards of the scientific community. This is a provision that shows the concern about making scientific research achievable, recognising that specific consent may be interpreted in a flexible way.²⁶

Another situation is where personal data was collected previously, for example by the hospital that accompanied the pregnancy and birth of a premature child, and now the researcher wants to access and subsequently process this health data for scientific research purposes. In this case, the data has been collected previously by other entities (hospitals or minister of health, for example) for a different purpose other than that for which they will now be processed.

²⁴ Despite being understood as a basic ground to process personal data, the consent is strongly criticized by Bert-Jaap Koops, who defends that it is “theoretical and has no practical meaning”, it is a ‘myth’ and defines the EU data protection law as a “zombie: it seems to live, but lacks a vital spirit.” - BERT-JAAP KOOPS, *The trouble with European Protection Law*, Vol. 4, International Data Privacy Law, 2014. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692 (24/4/2019). Likewise, Spiros Simitis criticizes the legal regime of the data processing considering the personal data protection sparse and poor. - SPIROS SIMITIS, “Privacy – An Endless Debate”, *California Law Review*, Vol. 98, 2010. Retrieved from: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1061&context=californialawreview> (24/4/2019).

²⁵ Civil law considered a person with less than 18 years old a minor (article 122 of CC). Minors did not have legal capacity to act, except under the terms described in the article 127 of CC. Article 124 of CC determines that the incapacity arising from the minority is suppressed in first place by parental responsibility and, subsidiarily, by guardianship.

²⁶ The Handbook of European Data Protection Law says: “It [the regulation] also recognises the importance of the compilation of data in registries for research purposes and the possible difficulty in fully identifying the subsequent purpose of personal data processing for scientific research purposes at the time of data collection.” EU AGENCY FOR FUNDAMENTAL RIGHTS; COUNCIL OF EUROPE; EUROPEAN DATA PROTECTION SUPERVISOR, *Handbook on European data protection law*, 2018, p. 340.

The consent that the data subjects gave before does not cover this subsequent process, thus the purpose limitation principle (article 5/b) of GDPR and, under International law, article 5/4/b) of Modernised Convention 108) implies that a new lawful ground for this subsequent data processing has to exist. However, as the researcher wants to use retrospective data, as it was collected before, in practice this means that the consent of the data subject will be now hard to obtain, as the researcher does not know who the data subjects were.

Therefore, this lawful ground to legitimate the processing of personal data is not that easy as it seems whether it was retrospective data or data collected through the data subject directly.

But, where the consent of the data subject is necessary, the processing of health data, which belongs to the category of sensitive data (article 9/1 of GDPR), requires explicit consent (article 9/2/a) of GDPR *versus* article 6/1/a) of GDPR).

The meaning of the adjective “explicit” is not clear when only reading the regulation. Albeit, its meaning is clear when we read the *GDPR consent guidance*, by the Information Commissioner’s Office, which says: “Explicit consent is not defined in the GDPR, but is not likely to be very different from the usual *high standard of consent*. (...) The key difference is likely to be that ‘explicit’ consent must be *affirmed in a clear statement* (whether it is oral or written). Explicit consent must be *expressly confirmed in words*.”²⁷ (Our italic emphasis).

Thus, firstly, GDPR does not allow: pre-ticked boxes, pre-completed forms or inactivity/silence to achieve the data subject’s consent, even if it is to process non sensitive data.²⁸ To achieve the consent of the data subject we need to have a statement (or a clear affirmative action, when it is non-sensitive data.)

Secondly, a notice that cannot be confused the requirement of an explicit consent using either the written or oral consent forms.

To explain, explicit consent can be expressed in both an oral or written form and written consent is not always explicit. Explicit consent requires an express statement of consent, such as “I consent to...”, where it is clear by this statement that the data subject gave his/her consent.²⁹ However, according to article 7/1 and recital 43 of GDPR, the controller has the burden of proof of the consent. Thus, the safest form to collect the data subject’s explicit consent is by using the written form, because that is the easiest form of proof.

²⁷ Available in: <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent-1-0.pdf> (p. 30).

²⁸ As it is clear reading the recital 32 of GDPR. EU AGENCY FOR FUNDAMENTAL RIGHTS; COUNCIL OF EUROPE; EUROPEAN DATA PROTECTION SUPERVISOR, *Handbook on European data protection law*, 2018, p. 113 and TOBIAS KUGLER; DANIEL RÜCKER, *New General Data Protection Regulation*, C.H.Beck, Hart, Nomos, 2018, p. 92.

²⁹ Regarding this point, see the document “Grupo de trabalho do artigo 29º - Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679”, retrieved from: https://www.cnpd.pt/bin/rqpd/docs/wp259rev0.1_PT.pdf.

2.2. Scientific research purposes as a lawful ground to process sensitive data (article 9/2/j) of GDPR)

Article 9/2/j) of GDPR says: " Paragraph 2 shall not apply if one of the following applies:

(...)

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89(1) based on 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 interests of the data subject."

Article 89/1 of GDPR, whose epigraph is "Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes", says: "Processing for archiving purposes in the public interest, scientific research or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of the data subjects, those purposes shall be fulfilled in that manner."

There is no doubt that scientific research may be considered an activity recognised by the European Union's law as a legitimate aim to process sensitive data. This understanding is also shared by International law and National law.

Reading the articles 89/2 of GDPR and 31/2 of 58/2019 Act we can conclude that this purposes are considered difficult to achieve by the European Union's law maker, with all the principles and rights of the data subjects recognised by GDPR. To make it achievable, those articles provide derogations of the rights of the data subjects to access,³⁰ to rectification, to restriction of processing and to object³¹ which can be considered as an opportunity for the researcher to process this type of personal data.

Despite the right to erasure (also known as 'right to be forgotten'³²) does not listed on article 89/2 of GDPR, the article 17/3 excludes it where the processing is necessary: "(...) (c) for

³⁰ Regarding the right of the patient to access and copy his medical records see the judgement of the European Court of the Human Rights (4th section) of 7-04-2009, K.H. and Others v. Slovakia. The applicants alleged that articles 6, 8 and 13 of the European Convention of the Human Rights were violated. The court considered that only the first two were violated.

³¹ For a brief description and analysis of the data subject's rights enshrined by the GDPR see: RUI MANUEL SOARES, "RGPD - Revisitando os direitos individuais", *Cyberlaw*, Vol. I, No. 5, 2018. Retrieved from: <https://blook.pt/publications/publication/969204b109e3/> (30/3/2019).

³² The right to erasure or right to be forgotten was recognized for the first time by GDPR. However, it is not new, as the Court of Justice affirmed this right on the judgement of the Court of Justice (Grand Section) of 13-05-2014, Proc. no. C- 131/12, Google Spain e Google Inc. versus Agencia espanhola de proteção de dados (AEPD) e Mario Costeja González. In this controversial case the Court created a new right from the interpretation of the articles 12 and 14 of the Previous Data Protection Directive. Many of the "innovations" that GDPR brought us are the result of the Court of Justice case law - this opinion is also shared by ALEXANDRE

archiving purposes in public interest, *scientific or historical research purposes* or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to *render impossible* or *seriously impair* the achievement of the objectives of that processing.”

The difference between those provisions of GDPR is that article 89/2 allows EU law or Member State’s law to provide exceptionally derogations of the rights to access, to rectification, to restriction of processing and to object, whose derogations are established by article 31/2 of 58/2019 Act, and article 17/3 of GDPR predicts itself the list of the situations where the right to erasure shall not apply, provision that is directly applicable to the Member States.

When the personal data is going to be processed for scientific research purposes, article 31/1 of 58/2019 Act to reinforce the necessary respect for the minimisation principle and, when the purpose may be achieved that way, determines the anonymisation or pseudonymisation of the data. This provision is nothing more than what is a concretization of article 89/1 of GDPR when it talks about “organisation and technical measures” that need to be provided.

The storage limitation principle (article 5/1/e) of GDPR) has a soft interpretation concerning when the data will be processed for scientific research purposes. According to article 21/2 of the 58/2019 Act, where it is not possible to know previously the storage time needed to reach the purpose, the storage of the personal data is lawful, if organisational and technical measures are in place to ensure the rights of the data subject.

These provisions, amongst others, demonstrate how GDPR and, consequently, National law support scientific research purposes.

2.3. The lawful ground - Consent *versus* scientific research

Notice that article 9/2 of GDPR says: “Paragraph 1 shall not apply if *one of the following* applies:” and article 6/1 of GDPR says: “Processing shall be lawful only if and to the extent that *at least one of the following applies*:” (our italic emphasis). Thus, it is clear that there is only need to verify at least one of the provisions established by GDPR.³³

However, Tatiana Duarte, who commented on article 9 of GDPR,³⁴ says that some hypotheses established by article 9/2 of GDPR are not legal grounds but admissible purposes for the data processing. The author concludes by saying that in data processing for scientific

LIBÓRIO DIAS PEREIRA, “Big data, E-Health e “autodeterminação informativa”: A lei 67/98, a jurisprudência e o Regulamento 2016/679 (GDPR)”, 2018, pp. 51-70.

³³ Actually, according to the article 8/2 of the Charter of Fundamental Rights of the European Union, the consent “or *some other legitimate basis* laid down by law” may ground the process of personal data. Therefore, as António Menezes Cordeiro states, the consent is one of the main guarantees of protection of data subject’s interests but *it is not an utter requirement*. - ANTÓNIO BARRETO MENEZES CORDEIRO, *O consentimento do titular dos dados no RGPD*, 2018. Retrieved from <https://blook.pt/publications/publication/e772e2d8f7b4/> (30/3/2019).

³⁴ ALEXANDRE SOUSA PINHEIRO (COORD.), CRISTINA PIMENTA COELHO, TATIANA DUARTE, CARLOS JORGE GONÇALVES, CATARINA PINA GONÇALVES, *Comentário ao Regulamento Geral de Proteção de Dados*, Lisboa, Almedina, 2018, pp. 235 ff.

research the consent of the data subject is still required and the circumstances that the European law maker have listed as admissible purposes for data processing does not make them into legal grounds because these purposes still need the balancing of interests by the data subject through his/her consent. This narrow interpretation of GDPR contradicts its own literal interpretation and the reasoning of the EU law maker.³⁵

To sustain the literal interpretation of the Regulation, *Handbook on European Data Protection law* says: "For this reason, the regulation allows the processing of data for these purposes [archiving purposes in the public interest, scientific or historical research purposes or statistical purposes], *without the data subjects' consent*, provided the relevant safeguards are in place."³⁶ (Our italic emphasis)

2.4. Coordination of the National law with the GDPR

Assuming that scientific research purposes are the lawful ground of the processing, now we will see what National laws say about it.

On one hand, the "Lei 12/2005, de 26 de Janeiro" (12/2005 Act, of the 29 of January) stipulates, in article 4/3, that health information can only be used by the health system under the terms and conditions expressed in written consent by the data subject or his representative. Thus, if the patient, as the data subject, gave his consent, the hospital can share health information with the researcher for data processing for scientific research purposes, respecting all the principles and rights of the data subject provided by GDPR. On the other hand, regardless of the consent of the data subject, article 4/4 of the 12/2005 Act determines that the access to health information may be provided for scientific research purposes, *if the information is anonymised*.

³⁵ Regarding the possibilities allowed by the article 8/4 of the previous Data Protection Directive to use health data for scientific research purposes without consent Ian Brown, Lindsey Brown and Douwe Korff have a very narrow interpretation of that provision – "In our opinion, this means that the law, or any decision under the law, *should not just allow the use of patient data without the latter's consent for certain generally-defined types of research*. Rather, such use of such data can only ever be allowed on a *case-by-case basis*, and only if the *particular research that proposed serves a particularly important public interest*. This allows, for instance, the compulsory reporting of *certain very serious infectious diseases in order to protect the general public*, and use of reporting data for statistical purposes and for research into measures to counter such a disease. It will *not allow* the use of patient data without consent for research into *less serious diseases*." (our italic emphasis) – IAN BROWN; LINDSEY BROWN, DOUWE KORFF, *Using NHS [national health service] Patient Data for Research without consent*, 2010. Retrieved from: https://heinonline.org/HOL/Page?public=true&handle=hein.journals/linovte2&div=12&start_page=219&collecton=journals&set_as_cursor=0&men_tab=srchresults (10/4/2019). This interpretation, agreeing with it or not, is in accordance with the recital 34 of Data Protection Directive - which allowed the processing of sensitive data if it was justified by "grounds of important public interest (...) in areas such as (...) scientific research (...) - and its article 8/4 - which used the expression "important or substantial public interest". But, nowadays the GDPR is clear predicting and distinguish two different grounds: scientific research purposes (article 9/2/j) of GDPR) and "reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medicinal devices (...)" (article 9/2/i) of GDPR).

³⁶ EU AGENCY FOR FUNDAMENTAL RIGHTS; COUNCIL OF EUROPE; EUROPEAN DATA PROTECTION SUPERVISOR, *Handbook on European data protection law*, 2018, p. 340.

First of all, we have to stress that anonymised information means that we cannot link the information to the person, unlike what happens with pseudonymisation, where the data subject is not immediately identified but it is possible to (re)identify he/she.³⁷ Thus, anonymous information is not considered personal data (regarding the concept of personal data, see foot note no. 2).

Despite it not being completely useless, anonymised information is not always fit for research projects. Thinking on research projects that follow up the evolution of a cohort for example, we conclude that anonymised information is not enough.

Second of all, anonymised information is not personal data, as the concept of personal data, according to article 4/1 of GDPR, implies an identified or identifiable natural person. Therefore, when the data processing uses anonymised information, the 'controller' does not even have to comply with GDPR.³⁸ GDPR is clear in its recital 26 on the following transcription: "This regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes." On the contrary, as previously shown, GDPR allows the process of sensitive personal data for scientific research purposes, ensuring appropriate safeguards. So, GDPR allows the processing of sensitive data for scientific research, at least with pseudonymised information.³⁹

In our point of view, this provision of article 4/4 of the 12/2005 Act could be modified following the GDPR.

Under the terms described in article 62/1 of the 58/2019 Act "The provisions related to data protection established by specific laws remain in force in all that does not contradict the GDPR and the present law, without prejudice of the next number". Comparing the article 4/4 of the 12/2015 Act with article 31/1 of the 58/2019 Act, the first one does not contradict the last one. As referred to above, article 31/1 of the 57/2019 Act, after reaffirming the data minimisation principle, determines that, *when the purpose may be achieved that way*, the data must be anonymised or pseudonymised. So, article 4/4 of the 12/2005 Act, which handles the specific situation of the access of health information for scientific research purposes, requires the anonymisation of the health data, which measure is contemplated by article 31/1 of the 58/2019 Act.

³⁷ The Handbook of Data Protection law says: "Data subject to pseudonymisation remain subject to the General Data Protection Regulation, unlike anonymous data.", according to the recital 26 of GDPR as well. - *Handbook of Data Protection law*, Luxembourg, Publications Office of the European Union, 2018, p. 340. Regarding the concept of identified and identifiable information consult: ANTÓNIO BARRETO MENEZES CORDEIRO, "Dados pessoais: conceito, extensão e limites", *in Revista de Direito Civil*, Year 3, no. 2, point 6.

³⁸ The first assumption of the application of Data Protection Rules is the presence of personal data. If the controller conclude that the purpose can be achieved with anonymised information GDPR is not applicable, but Regulation (EU) 2018/1807 of the European Parliament and of the Council of the 14 November 2018 may be applicable as it establishes the framework of the free flow of non-personal data in the European Union.

³⁹ A similar question was placed by Jorge Bacelar Gouveia related to the article 11/2 of the revoked 10/91 Act. This provision established that the computerized processing of 'sensitive' data was allowed for statistics and research *if the person could not be identified*. This Author argued that there was an incompatible contradiction because the concept of personal data presupposes the identification or identifiability of the data subject. The Author defended an interpretation that disregards that provision or that it may be considered unconstitutional, as it limits, in violation of the article 18/2 of CRP, the right predicted by article 35/3 of CRP. - JORGE BACELAR GOUVEIA, "Os direitos fundamentais à proteção dos dados pessoais informatizados", *in Revista da Ordem dos Advogados*, Year 51, III, 2015, pp. 726 and 727.

Looking to GDPR and article 4/4 of the 12/2005 Act, cannot be considered that this provision was tacitly revoked with the entry into force of the GDPR, because article 4/4 does not contradict the provisions of GDPR, whose articles 9/2/j) and 89 give rise to the members' state law to define the outlines of the legal regime, including the processing of sensitive data (as affirmed by recital 10) and its recital 28 stipulates that "(...) The explicit introduction 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection."

However, article 9/2/j) of the European regulation requires that the members' state law has to be: proportional to the objective pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

Imposing data anonymisation without exceptions seems to be an excessively guaranteeing measure, broadly protecting the data subject and blocking the processing for scientific research. Where the purpose cannot be obtained without personal data, such as an anonymised one, pseudonymisation⁴⁰ should be the adequate measure to safeguard the fundamental rights of the data subject. In this way there is a balance between the rights of the data subject and scientific research aims.

Another provision to be analysed is the "Despacho n.º 6742/2019", published on Diário da República, 2nd serie, by the State Secretary of Health, on the 29th July 2019, which came into force on the day after (30th July 2019). This repealed its antecedent "Despacho n.º 4354-A/2017", published on Diário da República, 2nd serie, no. 97, by the State Secretary of Health, on the 17th May 2017, which came into force on the 18th May 2017.

Therefore, the publication and application of both started after the entrance into force of the GDPR (whose date is 24th May 2016, according to article 99/1), which differs from its application (whose date is 25th May 2018, according to article 99/2), so the dispositions of the Regulation should had been taken into account.

The previous "Despacho n.º 4354-A/2017" established the following dispositions about the transmission of *health information* by the public entities in the area of health:

- The prior authorisation by the member of government responsible for health area needed for the transmission of data for third entities is dismissed, if that transmission is justified and grounded, under a *research protocol* or under the realisation of analyses or studies requested by the National Health Service and *as long as it does not involve transference of personal data identified or identifiable* (no. 1).

⁴⁰ Regarding the pseudonymisation measure, Daniel Rücker and Tobias Kugler say: "Consequently, also under the GDPR, pseudonymisation at least reduces risks of being identified by unauthorised persons and is therefore a way of designing data processing in a less invasive and therefore data protection friendly way. Pseudonymisation reduces the risks for data subjects (which, for instance is relevant in the process of balancing interests: see section C.I.3.b), increase data security and helps controllers and processors to meet their data protection obligations. For the effectiveness of the pseudonymisation procedure, for example, it is decisive at what stage it is used, how secure it is against reverse tracing and the size of the population in which population the individual is concealed." - TOBIAS KUGLER; DANIEL RÜCKER, *New General Data Protection Regulation*, 2018, p. 20. A classic example of a pseudonymisation measure is the encrypted data (or key-coded data).

- The transference, for free or at a cost, of personal data to third entities by entities that are part of the National Health Service, *if it does not fit with the previous provision has to be previously and expressly authorised* by the member of government responsible for the health area (no. 3).

To summarise, there was two relevant options: if between the intervening entities (the researcher and the public hospital, for example) a protocol existed, then the transmission of personal information unidentified or unidentifiable (thus, not personal data) did not need the previous authorisation of the member of government responsible for health area.

Otherwise, if the transmission involved personal information that was not personal data, as the anonymised ones are, where between the intervening entities there did not exist a protocol, then the transmission needed the previous and express authorisation of the member of government responsible for the health area.

Matching these provisions with article 4/4 of the 12/2005 Act, the access to health information, even if it is anonymised, where there is no protocol between entities (no. 1 *a contrario sensu*), must needed the authorisation of the member of the government responsible for the health area.

In the same way as was stated previously above, according to no. 3 of the antecedent "Despacho n.º 4354-A/2017", if the transmission involved personal data, as the pseudonymised one does, the transmission needed the previous and express authorisation by the member of government responsible for the health area.

Currently is into force the "Despacho n.º 6742/2019", which lays down the transmission of *statistic data of production and consumption* by entities integrated on the Minister of Health. This provision aimed to simplify the process, saying that the previous required authorization for the transmission of *statistic data of production and consumption* where there was not a protocol between the intervening entities implied a *lagging and bureaucratic procedure*, that does not added value to the process, in comparison with the analysis made by the entities of the National Health Services that should be carried out in each case.

To analyse this provisions, the first problem to be solved is the definition of its extent, namely which is the information concerned.

Several provisions succeeded between 2017 and 2019. Firstly, the "Despacho n.º 913-A/2017", published on the 19th of January 2017, which prohibited the transmission of *health information*, without authorization by the member of the State in the area of health. However, the difficulties on its application motivated the emergence, less than a month later, of the "Despacho n.º 1612/2017", published on 17th of February 2017, which aimed to clarify the scope and the *type of data* concerned. Bearing in mind these objectives, the "Despacho n.º 1612/2017" was restricted to the transmission of *statistic data of production and consumption*. As was mentioned above, the following "Despacho n.º 4354A-2017" of the 17th of May 2017 referred to the communication of *health information*, thus using the broader expression. Nevertheless, the scope of this provision was to regulate the transmission of a

specific type of information, the statistic data of production and consumption, notwithstanding its unclear letter. This interpretation is confirmed by the recent “Despacho n. 6742/2019”, which refers to the predecessor restricting its scope to the transmission of statistic data of production and consumption.

Therefore, as the transmission of health information other than statistic data of production and consumption by public entities that are integrated in the Minister of health is not covered by the “Despacho n. 6742/2019”, its access and transmission must have to be legitimated by the GDPR and the 12/2005 Act.⁴¹

However, the access of personal data, as the pseudonymised one, is not foreseen on the 12/2005 Act, unless with the consent of the patient. As previously stated, it cannot be considered that article 4/4 of that Act contradicts GDPR or that the 58/2019 Act, whose article 31/1 stipulates the anonymisation measure, but can be considered excessively limited, making the use of personal data for scientific research purposes unfeasible.

This obstacle, may be overcome if article 4/4 of the 12/2005 Act is read with an actualised interpretation compatible with GDPR, whose article 9/2/j) allows the processing of sensitive personal data for scientific research purposes and imposes the proportionality of the Members’ state law, and article 31/1 of the 58/2019 Act, which stipulates anonymisation or pseudonymisation *if the purpose can be achieved that way*. So, where the purpose cannot be achieved by using anonymous information the use of pseudonymised data is permitted.

When the process involves a large amount of sensitive data a Data Protection Officer must be designated, who ensures the compliance with data protection rules (article 37/1/c) of GDPR) and a previous data protection impact assessment is necessary to evaluate the risks of the process (article 35/3/b) of GDPR) as well.

3. Realisation of a clinical study – the provisions established by 21/2014 Act

“Lei 21/2014, de 16 de Abril” (21/2014 Act of the 16th April) establishes the legal regime for clinical research. That Act is regulated by the “Decreto-lei 131/2014, de 29 de Agosto” (131/2014 Decree-Law of the 26th January), which determines the legal regime of protection and confidentiality of genetic information. Therefore, both rules were made during the term

⁴¹ The importance of the 26/2016 Act of 22 of August 2016, published on “Diário da República n.º 160/2016, 1st serie of the 22nd of August 2016, which predicts the legal regime of the access of administrative and environmental information and the re-use of the administrative documents is not rejected. However, its article 7, which establishes the regime of the access and transmission of health data, sends the reader to the provisions of the 12/2005 Act, despite the few conditions that it imposes. Furthermore, article 3 of 12/2005 Act establishes that health information belongs to the person, so it is his/her property and the health services are only the keepers. Therefore, health information cannot be considered administrative information, according to the opinion of Sérgio Deodato. SÉRGIO DEODATO, *A proteção de dados pessoais de Saúde*, Lisboa, Argumento, 2017. For these reasons, the 26/2016 Act was not mentioned.

of the previous Data Protection Directive and the Portuguese correspondent Act (67/98 Act), and did not change with GDPR, at least, up until the present.

Genetic data, which are considered sensitive as health data, has a specific regime that differs from the legal regime of health data in certain respects, hence we shall only focus on the 21/2014 Act.

“Clinical research” is defined in article 1/1 as “every systematic study that aim to discover or verify the distribution or effect of factors of health, health states or results, health or diseases processes, the performance, the safety of an intervention or health care services. Therefore, this broader meaning may include scientific research on the area of health.

Article 2/p) of the 21/2014 Act defines “clinical study” as any systematic study that takes on a human being or *through individual health data*, aimed to discover or verify the distribution or effect of health factors, states or results in health, health or illness processes, the performance, or the security of interventions or health services, through biological aspects, behavioural, social or organisational. Thus, scientific research that analyse personal health data may be considered, under the terms described, a clinical study, predicted by National Law.

The realisation of a clinical study is subject to several requisites that are imposed, some of them described in article 6 of the 21/2014 Act, whose epigraph is “minimum protection conditions for participants”.

From previous interviews with the researcher (article 6/1/a)), who has to give to the participant extensive information, and the existence of the previous informed consent of the participant (article 6/1/d) and article 2/l)) and a liability insurance (article 6/1/e)), to the authorisation of the competent ethics committee (article 16/1 of 21/2014 act), between others.

It is noteworthy, that article 6/1/d) determines the requirement for the researcher to obtain the informed consent of the participant. However, this consent is not always needed because, according to article 6/2, the competent ethics committee may, *exceptionally and properly grounded*, dismiss it on the clinical studies *without intervention*, as well as the interview and the information to the participant. Naturally, clinical studies with intervention, which concept is defined by article 2/s) of the 21/2014 Act, need the informed consent of the participant, respecting the dignity of the human person and his self-determination.

Therefore, we conclude again that according to the provisions established by this Act, it is possible to process health data without the consent of the data subject, a process that is lawful as it is grounded by scientific research purposes, stipulated by article 9/2/j) of GDPR and article 31 of the 58/2019 Act.

However, observe that this opportunity for the researcher is narrow, as the dismissal of the consent given by the competent ethics committee has to be *exceptional* and *properly grounded*. So, the dismissal of the consent is at the discretion of the competent ethics

committee and for principle the consent is needed, only in exceptional cases may it be exempted.

Obviously, in these cases where the consent was not needed, it is necessary to observe the appropriate safeguards to protect the right of the personal data protection and, as health data is concerned, the right to respect the private and family life. Those safeguards should be anonymised where the purpose may be satisfied with anonymous information or pseudonymisation if personal data are needed.

The requisites exposed above are imposed by the 21/2014 Act, interpreted as exposed, to protect the data subjects and does not compromise the feasibility of scientific research, thus they may be considered compatible and proportional with GDPR scope and the 58/2019 Act provisions as well.

3.1. Realisation of a clinical study with minors

When the participants are under-aged, article 7 of the 21/2014 Act establishes additional requisites, in order to protect the participant as they are considered vulnerable data subjects.

One of the requisites established is the informed consent (article 7 of the 21/2014 Act). It has to be distinguished where the participant is sixteen years old or more – in this case the minor and the holders of parental responsibility have to give their consent - and where the participant is less than sixteen years old – here the consent has to be given only by the holders of parental responsibility, which must reflect the presumed will of the minor.

Even in this particular case, article 7/3 stipulates the same provision established by article 6/2. Thereby, the competent ethics committee may dismiss the consent on the clinical studies without intervention when the participants are minors.

Regarding this provision, we have to conclude that the researcher has an opportunity to process health data of VPT or VLBW children if the competent ethics committee gives their favourable feedback, however taking into account that now we are considering vulnerable data subjects, as they are minors, the reservations of the competent ethics committee may be, understandably, higher. Therefore, the opportunity for the researcher is even tighter. Nevertheless, a balance between the benefits of the clinical study and the protection of the data subject must be made, considering that those purposes cannot always be achieved with anonymous data. Thus, we stress again that pseudonymisation in a higher level, where the risks for the rights of the data subject are reduced to the minimum if the data subject is difficult to identify or even reidentify, is the adequate safeguard to be taken when the purpose to be achieved needs personal data.

4. Conclusion

Within the world, the European Union has one of the highest standards of privacy protection and in the last decades this has been increased. The previous Data Protection Directive of 1995 established a lacking regime in comparison with GDPR, which is consistent and dense. Thus, EU citizens benefit of several rights and guarantees in order to ensure their right of personal data protection.

One of the scopes of GDPR is the harmonisation of the legal regime into the Member states as these discrepancies are an obstacle to the free flow of personal data within the European Union (recital 9 of GDPR). However, under the European Union the consensus among all its Members is not easy, which results in a regulation that requires autonomy with its members to regulate certain aspects.

Besides GDPR is already regulated by the 58/2019 Act, several previous laws have some provisions related to data processing and they were not modified yet in accordance with that regulation.

However, regardless of the legislative changes, it has to be considered whether the previous National provisions were tacitly revoked, insofar as they contradict GDPR or the 58/2019 Act (article 62º/1 of the 58/2019 Act).

The provisions analysed cannot be considered tacitly revoked. However, as they provide a higher protection for the data subjects, scientific research in the area of health, where personal data is needed, has to overcome several difficulties in prejudice for this noble activity.

The concerns naturally increase when the data process involves health data of the VPT and VLBW children. Firstly, because this data belongs to the category of sensitive data, which process is prohibited for principle (article 9/1 of GDPR) but allowed under the terms described by article 9/2 of GDPR. Secondly, the subjects do not have legal capacity, thus their incapacity has to be suppressed by the holders of parental responsibility. Comprehensively the safeguards provided by law and by the applicator of the law increase when the process has these delicate factors to consider.

The difficulties faced by scientific research are not only legal, they exist in practice as well, bearing in mind the poor adherence to these projects, because the persons are not aware of its potential benefits.

To conclude, as recital 4 of GDPR establishes, "The processing of personal data should be designed *to serve mankind*. The right to the protection of personal data *is not an absolute right*; it must be considered in relation to its function in society and be *balanced against other fundamental rights*, in accordance with the principle of proportionality. (...)". Thus, in our opinion, what is needed in National law is a better balance between the right of personal

data protection and the right of the respect of private and family life and the use of personal data, including sensitive data, for scientific research purposes.

References

BROWN, IAN; BROWN, LINDSEY; KORFF, DOUWE, *Using NHS [national health service] Patient Data for Research without consent*, 2010. Retrieved from: https://heinonline.org/HOL/Page?public=true&handle=hein.journals/linovte2&div=12&start_page=219&collection=journals&set_as_cursor=0&men_tab=srchresults (10/4/2019)

CALVÃO, FILIPA URBANO, *Direito da proteção de dados pessoais – Relatório sobre o programa os conteúdos e os métodos de ensino da disciplina*, Porto, Universidade Católica Editora, March 2018

CANOTILHO, GOMES, E MOREIRA, VITAL, *Constituição da República Portuguesa Anotada*, Vol. I, 4th ed. revised, Coimbra, Coimbra Editora, 2014

CARVALHO, ORLANDO DE, (COOR. by FRANCISCO LIBERAL FERNANDES, MARIA RAQUEL GUIMARÃES, MARIA REGINA REDINHA), *Teoria geral do direito civil*, Coimbra, Coimbra editora, 2012

CORDEIRO, ANTÓNIO BARRETO MENEZES, "Dados pessoais: conceito, extensão e limites", in *Revista de Direito Civil*, Year 3, No. 2, pp. 297-321

CORDEIRO, ANTÓNIO BARRETO MENEZES, *O consentimento do titular dos dados no RGPD*, 2018. Retrieved from <https://blook.pt/publications/publication/e772e2d8f7b4/> (30/3/2019)

DEODATO, SÉRGIO, *A proteção de dados pessoais de Saúde*, Lisboa, Argumento, 2017

EU AGENCY FOR FUNDAMENTAL RIGHTS; COUNCIL OF EUROPE; EUROPEAN DATA PROTECTION SUPERVISOR, *Handbook on European data protection law*, Edition of 2018, Publications office of the European Union, 2018

EURO-PERISTAT PROJECT, *European Perinatal Health Report – Core indicators of the health and care of pregnant women and babies in Europe in 2015*, November 2018

GOUVEIA, JORGE BACELAR, "Os direitos Fundamentais à proteção dos dados pessoais informatizados", in *Revista da Ordem dos Advogados*. Year 51, III, 2015, pp. 699 e ss.

HENRIQUES, MIGUEL GORJÃO, *Direito da União – História, direito, cidadania, mercado interno e concorrência*, 9th Edition, Coimbra, Almedina, 2019

JASSERAND, CATHERINE, *Legal Nature of Biometric Data: From generic personal data to sensitive data*, 2016 Retrieved from: https://heinonline.org/HOL/Page?public=true&handle=hein.journals/edpl2&div=56&start_page=297&collection=journals&set_as_cursor=0&men_tab=srchresults (10/4/2019)

KOOPS, BERT-JAAP, *The trouble with European Protection Law*. Vol. 4. International Data Privacy Law, 2014. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692 (24/4/2019)

KUGLER, TOBIAS; RÜCKER, DANIEL, *New General Data Protection Regulation*, C.H.Beck, Hart, Nomos, 2018

LIMA, PIRES DE; VARELA, ANTUNES, *Código Civil Anotado*, Vol. I., 4th edition revised and actualised, Coimbra, Coimbra Editora, 2010

MONTGOMERY, KATHRYN C.; CHESTER JEFF, *Data Protection for Youth in the Digital Age*, European Data Protection Law Review, 2015. Retrieved from: https://heinonline.org/HOL/Page?public=true&handle=hein.journals/edpl1&div=55&start_page=277&collection=journals&set_as_cursor=0&men_tab=srchresults (10/4/2019)

NETO, AFONSO ARAÚJO, "RGPD: Uma revolução invisível", in *Revista Luso Brasileira de Direito do Consumo*, Vol. VII, no. 27, 2017

ORGANIZATION, WH, *International statistical classification of diseases and related health problems (ICD-10)*, WHO library cataloguing-in-publication Data, 10TH revision, vol. II, 2010

PARK, DAMIN, *Mining for Children's Data in Today's Digital World*, 2018. Retrieved from: https://heinonline.org/HOL/Page?public=true&handle=hein.journals/jnaa38&div=16&start_page=320&collection=journals&set_as_cursor=0&men_tab=srchresults (30/4/2019)

PEREIRA, ALEXANDRE LIBÓRIO DIAS, "Big data, E-Health e "autodeterminação informativa": A lei 67/98, a jurisprudência e o Regulamento 2016/679 (GDPR)", in *Lex Medicinæ - Revista Portuguesa do Direito da Saúde*, Year 15, No. 29, 2018, pp. 51-70

PINHEIRO, ALEXANDRE SOUSA (COOR.); COELHO, CRISTINA PIMENTA; DUARTE, TATIANA; GONÇALVES, CARLOS JORGE; GONÇALVES, CATARINA PINA, *Comentário ao Regulamento Geral de Proteção de Dados*, Lisboa, Almedina, 2018.

PINTO, CARLOS ALBERTO DA MOTA, *Teoria geral do direito civil*, 4th edition, Coimbra, Coimbra editora, 2005

SIMITIS, SPIROS, "Privacy - An Endless Debate", in *California Law Review*, Vol. 98, 2010. Retrieved from: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1061&context=californialawreview> (24/4/2019)

SOARES, RUI MANUEL, "RGPD - Revisitando os direitos individuais", in *Cyberlaw*, Vol. I, No. 5, 2018. Retrieved from: <https://blook.pt/publications/publication/969204b109e3/> (30/3/2019)

Case law

Judgement of the Court of Justice (1st section) of 6-11-2003, Proc. no. C-101/01, *Bodil Lindqvist v. Göta Hovrätt (Suécia)*

Judgement of the European Court of the Human Rights (4th section) of 7-04-2009, *K.H. and Others v. Slovakia*

Judgement of the Court of Justice (Grand Section) of 13-05-2014, Proc. no. C- 131/12, *Google Spain e Google Inc. versus Agencia espanhola de proteção de dados (AEPD) e Mario Costeja González*

Judgement of the Court of Justice (2nd Section) of 19-10-2016, Proc. no. C -582/14 - *Patrick Breyner versus Bundesrepublik Deutschland*

Judgement of the Tribunal da Relação de Lisboa of 17-05-2017, Proc. no. 842/16.5T8ALQ.L1-3, Relator: Juiza Desembargadora Adelina Barradas de Oliveira

Judgement of the Court of Justice (2nd Section) of 20-12-2017, Proc. no. C-434/16, *Peter Nowak v. Data Protection Commissioner*

(texto submetido a 10.09.2019 e aceite para publicação a 18.09.2019)