INTERNATIONAL
HELLENIC
UNIVERSITY

Protection of Personal Data in the Era of COVID-19

OLGA TSIPTSE

SCHOOL OF HUMANITIES, SOCIAL SCIENCES & ECONOMICS

A thesis submitted for the degree of

Master of Laws (LL.M.) in Transnational & European Commercial Law, Banking Law, Arbitration/Mediation

December 2020

Thessaloniki – Greece

Student Name: OLGA TSIPTSE

SID: 1104180029

Supervisor: Prof. Komninos Komnios

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

December, 2020
Thessaloniki - Greece

Abstract

This dissertation was written as part of the LL.M. in Transnational & European Commercial Law, Banking Law, Arbitration/Mediation at the International Hellenic University.
The COVID-19 pandemic (more commonly known as Coronavirus) poses unprecedented threats and challenges for individuals and countries around the world. The need to stop its spread and cure those who are suffering is a prominent goal shared by nations globally. Moreover, COVID-19 caused shock to individuals and countries, initiating from the speed of the transmission of this Coronavirus, that finally there was no possibility to be dealt this emergency even by the most advanced health systems. In the effort of curbing the number of new contaminations, governments have had to resort to extraordinary measures, including the declaration of a state of emergency in many cases. However, the exercise of human rights, like the right to Data Protection, is applicable and cannot be suspended but only derogated or restricted by law, to the extent strictly required by the exigencies of the situation while respecting the essence of the fundamental rights and freedoms.
The present dissertation aims at addressing the impact of COVID-19 on the protection of personal data, even in those emergency and extraordinary cases. More specifically, an effort will be made in order to face the above issue, focusing on the following points:
-Processing of health-related data, forming the special category data, during the pandemic
-Data processing by employers (remote work) or by students (distance education)
-Digital epidemic surveillance (e.g. contact tracking, mobile tracing)
The issue to be faced is, whether GDPR conform processing is still possible.

Special Honor and Gratitude to my supervisor Ass.Professor Komninos Komnios.
Honor to the authors, that are mentioned in the end of the writing, who provide me all the information needed for my effort.

Special Dedicated to my parents and mostly to my Mom, Vasiliki Tsiptse,
responsible for my life and
my Husband, Matthaios Gkaros, responsible for my good life,
without them I wouldn't/couldn't have done much.

Keywords: Pandemic COVID-19, protection of personal data&privacy, remote work, distant learning/education, contact tracking, devices tracing

Student Name: Olga N. Tsiptse
Date: September - December 2020

Contents

Introduction

"All human beings have three lives: public, private, and secret."
— Gabriel García Márquez"

Protection of personal data[1] is absolutely a human right, but it is not an absolute human right. Data protection is considered as high priority for, at least, European Nations and that is the reason, for the increasing concerns about how retaining personal data protection against the need to suppress pandemic SARS-CoV-2 (hereafter COVID-19 or coronavirus). Despite these concerns, data protection, through these tough pandemic years, is not taken for granted. The changes of the data process worldwide, are radical, also the speed of these changes is vertiginous and the humanity was not ready for such eventuality.

Referring to a human right as a non absolute right, indicates, and therefore highlights, the difficulties in its protection. The difficulties protecting personal data tends to peak in emergencies and force majeure situations, when other individual rights such as public health and safety, and in general public interest, must be protected as well. When these emergencies are faced, and while considering personal data protection not being an absolute human right, it shall be balanced in and for every separate case that arises. There is no general rule. The duty of balancing this top priority right[2] with others, shall be "in accordance with the Principle of Proportionality", a cornerstone Principle that is diffused in the legislation of Regulation (EU) 2016/679 of European

---

[1] See the relevant definitions in Article 4 of the Regulation (EU) 2016/679 and especially: Article 4 (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (…) etc".

[2] Quite contradictory, on writer's opinion, because this priority is finally on the surface and not substantial.

Parliament and Council of 27th April 2016[3] (hereafter the Regulation or GDPR), it is also mentioned in all relevant legislation, guidelines, opinions, statements etc[4].

At this point, a separation of concepts must be realized. Protection of personal data is only an area of the broader concept of privacy. In fact, data protection right serves more purposes than privacy, and in that sense it is broader than privacy[5]. On the other hand though, privacy is broader than data protection, because it is consisted by other elements, as the right to be alone, the right to respect private or family life[6]. Consequently, the above two concepts, data protection and privacy, are not the same but still both are connected and interacting[7]. The data protection right depends on privacy and, at a certain level, it secures privacy. It is not only protected when it is violated, but it obligates all the processors to be organized to a certain regulatory field. And that leads to a conclusion, that though it is a non absolute right - and therefore it shall be balanced with other rights, in order the legal purposes of data processing to be indicated against the legitimate intrusion of that right - data protection seems to be a "constitutionalized" right, that is volatile depending on the purposes that is needed to protect[8].

Another topic, that shall be examined in the new COVID-19 era, is the lawful processing of data, especially of the special categories of personal data. Lawful processing is one

---

[3] GDPR Recital 4 "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. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity. "

[4] Article 9A Constitution of Greece, Guidelines and opinions of EDPB (European Data Protection Board) and national DPA's (Data Protection Authorities) that are going to be analyzed below.

[5] Mitrou L, The Personal Data Protection Right, 2012, pp.42-47.

[6] Article 8 ECHR (European Charter for Human Rights).

[7] Akrivopoulou X., "The Data Protection Right through the lens of Privacy', Theory & Praxis of Public Law Journal Session 7, 2011, <http://www.nomikospoudastirio.gr/δημοσιεύσεις-–νομικές-μελέτες/1300-χ-ακριβοπούλου,-το-δικαίωμα-στην-προστασία-των-προσωπικών-δεδομένων-μέσα-από-το-φακό-του-δικαιώματος-στην-ιδιωτική-ζωή> (accessed: 20.01.2021).

[8] Mitrou L., The Personal Data Protection Right, 2012, pp. 42-47, Akrivopoulou X., "In Between Autonomy & Intimacy - Self-defining the right to privacy", 2009, p. 422, https://thesis.ekt.gr/thesisBookReader/id/20504#page/1/mode/2up (accessed: 20.01.2021).

of the principles, that are relating to process of any category of data[9]. The GDPR repeats the implication of the previous Directive 95/46[10], and imposes the lawful processing of personal data. This principle is not defined exactly in the provisions, but it is implied in recital 40 GDPR, where a reference to lawful processing of data is also made[11]. More specifically, entities shall not process data, and mostly special categories of data, unless there is a legal basis for that action, a legitimate ground[12]. And to that point, the above prohibition must be seen as an exception. This exception, that also consists one of the principles in protecting data, leads to the reduction of personal data protection[13]. Data protection limitation is also recognized in Article 52 (1) of the European Charter of Human Rights (ECHR)[14]. After all, some other severe rights, like the health right and the duty of the governments to take care of the citizens' health, is also constitutionalized[15]. Therefore, in case of conflicting rights, some are limited and some prevail.

The aim of this paper is the examination whether the COVID-19 pandemic is the reason for the limitation of a non absolute but fundamental right, as data protection, invoking the meaning of public interest or health right?

In case of a positive answer to the above question, up to what level shall be occurred this limitation of personal data protection - balancing the rights that have to be

---

[9] Other principles are the processing of personal data shall be Fair, Transparent, Limited in purpose, in storage and in quantity, Accurate, and finally Confidential.

[10] Article 6 (1)(a) GDPR.

[11] Rücker D./Kugler T., New European General Data Protection Regulation, 2018, pp. 50-51.

[12] Legitimate grounds for processing data are restrictively referred to Article 6 GDPR, and for special categories of data, to Article 9 GDPR. Also are referred to national laws following GDPR.

[13] "The right to personal data protection is not an absolute right; it may be limited if necessary for an objective of general interest or to protect the rights and freedoms of others." (See, for example, CJEU, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 9 November 2010, para. 48), Handbook on European data protection law - 2018 edition, FRA/ EctHR/EDPS, p.35

[14] "As long as those limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others."

[15] Article 21 para. 3 Greek Constitution.

protected as well. Up to what level the limitation is not considered as an abuse of the data protection right?

Following this brief invocation of concepts, that have to be considered, an also brief historical reference, will be presented in the First Chapter, about the legislation surrounding personal data protection. In the Second Chapter, the issue that will be discussed is the presentation of the COVID-19 case and what happened in the field of legislation. The Third Chapter is focusing on what are COVID-19 case's pillars, what are the specific processes of personal data that create the danger of breach of data protection right, what are the legal grounds of those processes, if any. How the new Schrems II decision affects the processes when there is conducted data transfer to third countries. The Fourth Chapter is dealing with the balancing test of the before mentioned findings and the Principle of Proportionality and finally, the Last Chapter, is dedicated to author's personal opinion about the questions set above and a general conclusion.

Chapter One: Brief Historical Reference

Though GDPR is -up to now- a commonly known Regulation, with a worldwide reputation, useful is a brief reference about its route and significant information about its ratio. It will not be overviewed as a whole, but only in relation to the certain topic of how GDPR and any other Guideline related to Regulation, contributes to the protection of data. And of course, in particular in extraordinary and crucial circumstances, as COVID-19 or any other emergency situation, that may be faced in the future.

1.1 Primarily set of standards for the data protection right

Personal data protection was underlined mostly by GDPR, because of -unfortunately- the high administrative fines that threatens. Extremely high fines for the violation of GDPR provisions, was the reason for such popularity, though as a legal text, there are more important and substantial provisions than fines. Nevertheless, this right had been existed decades before. Protection of personal data and special categories of data (known as "sensitive"), though, was not introduced primarily by GDPR.

Looking back, regarding that right, it is necessary to acknowledge the **Convention 108** in the year 1981 (and the renewed and modernized version in 2018, **Convention 108+)**[16]. Also, we have to consider Article 8 (1) of the Charter of Fundamental Rights of the European Union (ECHR)[17], where it is stated explicitly the legal basis of any text issued about data protection[18].

Convention 108 and ECHR were a milestone. Technology started moving forward with maximum speed, gaining many steps in a small time and connecting human beings with an aggressive manner. The use of the word aggressive is chosen, because

---

[16] <https://rm.coe.int/1680078b37>

[17] Rücker D./Kugler T., New European General Data Protection Regulation, 2018, p. 5.

[18] "1. Everyone has the right to the protection of personal data concerning him or her.
2. 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. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority."
Source:Official Journal of the European Union C 303/17 - 14.12.2007

processing data lead to an abusing penetration to the field of privacy, especially online, without respecting the data subject's right and the limits of any data processing. This abuse caused also the reduction of subject's reactions and lack of their reflexes. Subjects started to easily provide data and that had to cease.

1.2 Data protection before GDPR

The European Member States noticed the technological evolution early enough and the enormous danger of exposing personal data from the subjects and the abuse from the data controllers and processors, in 1995. There was a need of publishing an innovative legislation and that was the Directive 95/46/EU. The purpose was one: the mitigation of personal data breach or loss[19] and protection of certain rights that any physical person should be free to enjoy.

The above ambitious Directive was adopted and ratified by almost all EU members at that time[20], however failed to provide the absolute protection needed, against the careless data processing by entities. That negative outcome was caused, because of the lack of uniformity, of tight connection and of interaction between the Member States (MS), in the same time of such speedy evaluation of technology information. A drastic change was needed, and an improved Regulation this time, was on its way after 20 years of Directive's life and after the explosion of the third and fourth industrial revolution.

A Regulation was needed because of its legal nature. Regulations directly apply with the same manner, at the same time, through all MS. To be coherence between MS and especially between their Data Protection Authorities (DPAs), under the umbrella of the a supervisor authority, the European Data Protection Board (EDPB).

During the application of Directive, plenty of Guidelines were issued by the Working Party of article 29 (WP29)[21], which are still used nowadays, even with slight revisions

---

[19] And in general actions and incidents that would affect the confidentiality, integrity and availability of the personal data, which consists the principle of data security.

[20] The Directive was transposed into Greek law by Law 2472/97.

[21] https://edpb.europa.eu/our-work-tools/article-29-working-party_el

from EDPB. Many Guidelines were also published by MS's DPAs[22]. The above material consists the treasure in the field of personal data protection.

1.3 The high time for direct application of a Regulation.

After years of preparation, the GDPR issued in the year of 2016 without changing many granted provisions, but bringing in a few substantial points[23]. The key point for the existence of a Regulation, was the direct and uniform application of a binding legal text in all MS. The structure of supervising actions, relating to the data protection, was renovated by GDPR and all MS's DPAs. This supervision and control started to be centralized, by EDPB. That Board is considered as a new organ. EDPB is where all representatives from national DPAs shall collaborate and from where guidelines are issued and must be implied homogeneously. Also, national DPAs introduced to the public and private entities, the notion of Data Protection Officer (DPO), who should be DPAs extension, in order to controlling organizations and undertakings, whether they adopt the GDPR compliance, serving the rights of physical persons and securing their data.

This was an administrative change implied by GDPR, because the control should be remained centrally. But it was not the only innovation.

- Enormous and threatening administrative fines were introduced, for not being compliant towards the Regulation.
- More rights[24] were implied from the entities in favor of human beings, the data subjects.
- New notions as the privacy by design and by default were faced, binding for entities both in private and public sector.
- Notifications to the national DPAs ceased, and the responsibilities shifted to entities.

GDPR had a two years period, from 2016 when it was issued to 2018 when it should be in action, to be known by all the entities founded in MS but also by the entities of the third (to EU) countries that process EU citizens' data. When 25th of May 2018, time for

---

[22] http://www.dpa.gr, www.dataprotection.gov.cy, www.cnil.fr, www.agpd.es, and other MS's DPAs , with special contribution of United Kingdom's and Ireland's DPA, before BREXIT but also up to nowadays, https://ico.org.uk & www.dataprotection.ie.

[23] In Greece the national law that was issued, for the issues that was authorized to be supplemented, was Law 4624/2019.

[24] The right to be forgotten & the right for portability.

being set in action approached, GDPR was faced as an Armageddon and caused huge "noise". Uncountable mails were sent to every EU (and not only) data subject, seeking for consent for subject's data processing, while in fact this action was itself a breach of GDPR provisions in many cases.

1.4 "Automated individual decision-making, including profiling"

GDPR is considered a very complex text, with 99 articles and almost duplicated recitals, up to 173, where the ratio of this legislation is analyzed. In fact, all the substantial interpretation of the Regulation is located in these recitals. One of the most important article, though, is the article, that will decisively affect the new practices coming in the future. Especially, will affect the effort in controlling pandemic COVID-19, when the use of some artificial intelligence (AI) or smart devices and applications, is necessary. That is the article 22 GDPR[25].

When we talk about "automated decision making" and "profiling"[26], we consider a contribution to a no-turn back situation: "the development of automated decision making, without human intervention". This decision making is based upon artificial intelligence algorithms, and will replace fully the process by humans. It is self-evident how dangerous this operation can be. It is a tool but with wrong handlings, it may also be a weapon. Algorithms may fully replace human resources and all the process will be conducted by the process of data by AI devices.

In risk management, such as pandemic treatment, is already decided that some applications as contact tracing and mobile tracking and monitoring or mass mapping and demographic quarantining, are promoted[27]. The profiling and decision making by AI devices is unavoidable. In fact, that process has been absolute relied on profiling.

---

[25] "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

[26] The constitutive elements are: a) profiling must be automated, b) profiling must be performed on personal data, c) the goal of the profiling must be to evaluate certain personal aspects of the individual.

[27] Singapore case study "s73 of the Infectious Diseases Act34 (hereinafter referred to as "the IDA"). This includes an individual who: enters Singapore (by land, sea or air) from a country or territory outside Singapore during the control period; before or during the control period, comes into contact or has come into contact with any other individual who is, or is suspected to be, infected with COVID-19; …"

The ethical challenges[28], that have been caused by the effort and the purpose to save mankind, have many parameters. In particular challenges about:

a.whether is accepted the prevalence of public interest towards privacy and personal data protection. The high need of controlling pandemic has lead to the closest surveillance and use of AI, for decision making and profiling. There is framework in GDPR for lawful process of data, especially health data, in the context of pandemic. Article 9 GDPR implies "the processing of personal data for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health," as long as that kind of process is proportionate and for a certain purpose. That means, that, while lacking of time, authorities have to provide a - to the depth - impact assessment.

b.whether the human dignity can be protected equally, towards the coveted public interest. There is a stigma threatening humans, who share health data, a discrimination that exceeds to the family, children even parents or further relatives of the diseased victims[29]. Governments shall cover dignity with a solid protection shield. Together with dignity, it shall be examined the challenge, whether there is data bias, that could lead to discrimination upon race and gender

c.whether there is transparency in collecting data. Transparency is connected with the duty to disclose to humans what data are collected, for what purpose and where are they transmitted. Transparency is very important especially when Governments dominate private entities[30].

---

[28] Findlay M., Jia Yuan Loke, Remolina N, Tham B, Research Paper No. 2020/02, "ETHICS, AI, MASS DATA AND PANDEMIC CHALLENGES: RESPONSIBLE DATA USE AND INFRASTRUCTURE APPLICATION FOR SURVEILLANCE AND PRE-EMPTIVE TRACING POST- CRISIS" Singapore Management University, Centre for AI and Data Governance, pp.29-42.

[29] Example given people with HIV in South Africa and the United States faced discrimination and have problems getting jobs or attending school, also the stigma against survivors of Ebola in West Africa.

[30] "Apple and Google are jointly developing technology to alert people if they have recently come into contact with others found to be infected with coronavirus. Their contact-tracing method would work by using a smartphone's Bluetooth signals to determine to whom the owner had recently been in proximity for long enough to have established contagion a risk. See Leo Kelion, "Coronavirus: Apple and Google team up to contact trace Covid-19", *BBC News* (10 April 2020) <https://www.bbc.com/news/technology-52246319> (accessed 27 April 2020); Patrick Howell O'Neill, "How Apple and Google are tackling their covid privacy problem", *MIT Technology Review* (14 April 2020) <https://www.technologyreview.com/2020/04/14/999472/how-apple-and-google-are-tackling-their- covid-privacy-problem/> (accessed 27 April 2020).

d.also the challenge whether the data will be expired after emergencies, which is not self-evident, and the challenge of explainability[31].

Among the securities offered by the 99 articles of GDPR, for personal data protection, this unique article 22 is the cornerstone, protecting the absolute surrender of human rights, related to data, to the Rubicon of AI[32]. This anxiety that is hidden behind article 22 GDPR, leads to the conclusion that our lives are finally digitized and privacy is transcendent.

Still, we shall not ignore, nor underestimate, the value of the principles of GDPR in Articles 5 (1)(a)- (3), 6 or 9[33], that are guardians for data subjects. In particular, the principles of lawful data processing[34] and transparency. For instance, for lawful process of special categories of data, we shall consider the conditions set in article 9 (2) together with article 22 (2) and (4)[35].

Pandemic though, cast a strong doubt about the protection provided by the above mentioned legal basis. After all, the legal frame is not a panacea for abusing human rights.

---

[31] Article 13 (2) (f) stipulates that "the controller must provide additional information if the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".

[32] Below, will be presented the ways that will cause such an intervention to subject's rights and the excessive introduction of smart devices or apps into our lives that may trigger GDPR article 22. "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

[33] "Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law". "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law".

[34] Convention 108 Article 5 (3) & the Charter article 8 (2). Also, GDPR recital 40.

[35] Granic M.-Antunovic K., Journal of Swiss Chinese Law Review Issue No.1, pp.14-17.

Chapter Two: COVID-19 case and the legal treatment

The year 2020, is historically marked by the dominance of COVID-19, worldwide. An extreme situation that changed the flow of history, normality and routine of physical and legal persons globally. It is considered as a force majeure situation and in those situations the balancing for everyday's decision gains ground. The World Health Organization (WHO) faced a holistic health threat, that still is highly contagious after almost one year, and is declared, from the beginning, to be as a pandemic[36].

2.1 What was the data protection problem that COVID-19 caused?

Something had to be done, for facing the emergency. There were two levels that should be faced: the prevention of disease's spread and the treatment of data protection during that pandemic. COVID-19 health case, became easily a political case and a great challenge for the Governments, that had the heavy duty to control the spread of the disease, a spread with high speed and protect the health of citizens. Governments though, had the duty to respect democracy and of course the duty to respect the data protection right, which right was highly affected[37] by the actions decided against the spread of pandemic.

As is commonly accepted, no human right is superior than life. No human right can prevent saving lives, when have to be adopted measures that cause derogation of these rights. This derogation, though, applies, regarding the below severe and tight conditions:

a. The restriction shall a be short-term situation and

b. only to the minimum level needed[38], in order not leading to abuse of human rights.

The puzzle to be solved is, as a matter of fact, acrobatics in a tightrope: The fully without suspension respect of personal data protection, especially the "sensitive"

---

[36] https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/

[37] In the next Chapter, the data processes are analyzed and how that processing affects data protection right.

[38] https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter?fbclid=IwAR0geAAqTdil0d7oKYjpJp53BZkN0JI9RM_vz-0pnb5srEn4wDg5MawZpyM

ones, against the uncontrolled flow/situation of a definitely contagious and potentially fatal disease. And the resolution of this problem is given legislatively.

2.2 The Legal Treatment, the prediction in general

In all legal texts regarding personal data protection, that are already mentioned above, is declared, that the data process shall be achieved "only if necessary, specified, proportionate and with legitimate purpose pursued". Otherwise, if these principles are ignored, the victims of the pandemic will be two, in the end of the day: both human beings and privacy and data protection rights.

The question that comes first is what kind of data is crucial for facing and dealing with COVID-19. Answering to that question, we have to examine two GDPR principles:

a. the purpose limitation, together with

b. the minimization of data processing[39].

Throughout this thesis, the reference to data includes both simple and special categories data. But, COVID-19 data are, certainly, health data, meaning mostly special category data. These kinds of data concern authorities at the most, trying to find solution for mitigating the risk from COVID-19 collection and process that is needed. Health data is not the only category that is processed in that health battle. Also, geolocation data about patients, human contacts, data for movement, maybe data generated and exported from small devices of their owner like device's IP, emails etc, are collected and being processed.

All these data, either simple or special category, need to be lawfully and transparently processed. The reason and purpose of the process shall be stated to data subjects and when the purpose has been served, data, mostly health, have to be deleted, due to certain protocol, or anonymized for medical or scientific reason. Though, it is declared in GDPR that, special data in particular, can by no means be processed, there is a limitation to that right.

---

[39] Purpose Limitation implies "data collected for specified, explicit and legitimate purposes… further processing for archiving purposes in the public interest…".
Data minimization implies that only "adequate, relevant & limited to what is necessary to the purposes for which they are processed"
Rücker D./Kugler T., New European General Data Protection Regulation, 2018, BECK-HART-NOMOS, pp. 49-67.

The prediction of suspension data protection right, is first faced in 1966. The International Covenant on Civil and Political Rights[40] , in Article 4, predicted that "1 . In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations…". The same direction follows the European Convention on Human Rights[41], which in the article 15 are mentioned the derogations on human rights that shall be occurred in time of emergency. Also, the ECHR implies, in article 35, the high level of human life protection.

In all those cases, the conditions for suspension of human rights are:

a.the short-term application of the derogation from obligations,

b.the proportionate derogations in order to be only the minimum needed for the case of emergency.

Finally, in GDPR recitals 46 and 52, it is directly referred to data processing necessary for "humanitarian purposes, including for monitoring epidemics and their spread" and also directly referred to "Derogating from the prohibition on processing special categories of data" and how this is allowed. Also, in recital 159 GDPR is implied, that data process is allowed for scientific and research reasons, as long as this process follows protocols and good practices and always in relation with the article 89 GDPR[42]. After all, the core GDPR principles lead to the major Principle of Accountability of data controller (and processor).

2.3 Specific Legal Treatment in COVID-19 era

The evolution of COVID-19 and the "ruins" that has left globally, has triggered the legislative machinery of new legislation. All States, from the appearance of the disease, have issued specific legal texts, joint decisions, newly issued laws facing and trying to control the outrageous COVID-19 case. All these legal texts rely on the technological assistance, meaning AI methods, through which authorities are able to collect and process data, as an interim measure, for facing emergency, until a rescue vaccine will be found.

---

[40] https://www.ohchr.org/Documents/Professionalinterest/ccpr.pdf

[41] https://www.echr.coe.int/documents/convention_eng.pdf

[42] GDPR Chapter 9 - Art. 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Below, will be analyzed some of the new "COVID-19" methods that are conducted, Methods that are implied by laws, as the contact tracing, the collection of health data, the messages sent to the authorities in order humans to be permitted to do basic duties like going to market or for a walk in quarantine days etc. These methods that help authorities to their effort mitigating COVID-19 health risks, have two faces: effort for the mankind rescue, on the one side, and their "bad face" is the conceal of dangers for breach of data protection right, either by human intervention or by the States themselves.

Apart from the above mentioned general provisions of GDPR or other legal frameworks, the permission of suspension and the limitation of data protection right is directed by specific guidelines and statements from EDPB and from national DPAs, that have been released. These institutions after all, showed their worries about the present unprecedented situation, from the first time of the health out bushed.

On 19th of March 2020, EDPB released a "Statement on the processing of personal data in the context of the COVID-19 outbreak"[43]. In that Statement is declared, that protection of data is not an obstacle for prevention of that contagious disease, which prevention consists high level priority, after all. Despite that, the Statement underlines the necessity of data controller (and data processor, or any other form as joint controllers/processors), to process data due to the **principle of lawfulness**. Moreover, it underlines, that **GDPR offers legal basis for data processing during the emergency, referring to a specific cases as health data processing by public health sectors due to articles 6 and 9 GDPR**, as employees' data processing by the employers, as data process by telecommunications due to **article 15 of the relevant, and Lex Specialis, e-Privacy Directive** and as the "mobile location data". That Statement also, seeks the answer to the question, whether MS's governments "can use personal data related to individuals' mobile phones, in efforts to monitor, contain or mitigate the spread of COVID-19" and reminds the core principles of GDPR[44].

This Statement is considered, by the author of this writing, as an ultimate cry out for not breaching GDPR, in the name of the effort controlling COVID-19. Ultimate and vain, author could add, because it is a common secret that no Laws can satisfactory protect

---

[43] https://epdb.europa.eu/our-documents/outros/statement-processing-personal-data-context-covid-19-outbreak_en.

[44] article 5 (3)-(4), article 7 and 10 GDRP.

any kind of data, during such emergencies. It is also a reminder and an anxiety, that there is only a tiny red line that divides the permitted and lawful process of data (simple and special category) from the data breach, that cannot be finally avoided.

A month after publishing the above Statement, EDPB issued two more Guidelines, for specific processes. The first Guideline is 03/2020, "on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak", and the second is 04/2020 "on the use of location data and contact tracing tools in the context of the COVID-19 outbreak", both were adopted at the same date, on 21 April 2020[45] and are considered crucial Guidelines for process "sensitive" data and simple data.

As it was expected, similar Statements were issued, at the same time, by the national DPAs. For instance, in Greece on 18th of March 2020, the Greek DPA issued Guidelines for personal data process during COVID-19[46]. These Guidelines is a remind to the data controllers, that GDPR is in action and is not suspended because of pandemic. That data processing shall obey certain lawful purposes, data protection right is not absolute and for that reason must be balanced when needed due to proportionality test, and finally offer some instructions for employers and journalists for data process. Greek DPA in fact, retains a very active role, in data protection during the spread of COVID-19, and has already published many texts. Worth mentioning is, the on 04 of April 2020 decision no 05/2020[47] and on 15th of April 2020 Guidelines for remote working, the creation of a special portal[48] in Hellenic DPA site, for issues arising from data process in COVID-19 era, and has examined practices as the Passenger Locator Form (PLF)[49] or the thermal cameras that measure temperature of train passengers or the contact tracing

---

45 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf & https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

46 www.dpa.gr/APDPXPortlets/htdocs/doccumentSDisplay.jsp?docid=163,39,44,101,194,223,3,99Portlets/htdocs/

47 https://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=88,14,167,167,62,175,11,248

48 www.dpa.gr/portal/page?_pageid=33,269264&_dad=portal&_schema=PORTAL

49 https://travel.gov.gr/#/

applications. Of course, in every country, DPAs manage to issue relevant Guidelines and Statements[50].

Remarkable is the "Statement on derogations from the Covenant in connection with the COVID-19 pandemic" that Human Rights Committee of United Nations released on 24th of April 2020[51] and also the previous one, in the beginning of pandemic article of

---

[50] https://lsts.research.vub.be/en/data-protection-law-and-the-covid-19-outbreak-archive?fbclid=IwAR1X_MGiJ-cvFlnBAMBduLb6NEQpRO68nerm9Ce0W1bfpD3XhNJP9D6ox7I

[51] "The Committee is of the view that in the face of the COVID-19 pandemic, States parties must take effective measures to protect the right to life and health of all individuals within their territory and all those subject to their jurisdiction, and it recognizes that such measures may result in certain circumstances in restrictions on the enjoyment of individual rights guaranteed by the Covenant. Furthermore, the Committee acknowledges that States parties confronting the threat of widespread contagion may resort, on a temporary basis, to exceptional emergency powers and invoke their right of derogation from the Covenant under article 4, provided this is required to protect the life of the nation. Still, the Committee wishes to remind States parties of the requirements and conditions laid down in article 4 of the Covenant and explained in the Committee's General Comments, most notably in General Comment 29 on States of Emergency (2001), which provides guidance on the following aspects of derogations: (1) official proclamation of a state of emergency; (2) formal notification to the Secretary General of the UN; (3) strict necessity and proportionality of any derogating measure taken; (4) conformity of measures taken with other international obligations; (5) non-discrimination; and (6) the prohibition on derogating from certain non-derogable rights. In particular, States parties must observe the following requirements and conditions when exercising emergency powers in connection with the COVID-19 pandemic:
(a)Where measures derogating from the obligations of States parties under the Covenant are taken, the provisions derogated from and the reasons for the derogation must be communicated immediately to the other States parties through the Secretary-General of the UN (…)
(b)Derogating measures can deviate from the obligations set out by the Covenant only to the extent strictly required by the exigencies of the public health situation (…)
(c)States parties should not derogate from Covenant rights or rely on a derogation made when they can attain their public health or other public policy objectives through invoking the possibility to restrict certain rights, such as article 12 (freedom of movement), article 19 (freedom of expression) or article 21(the right to peaceful assembly), in conformity with the provisions for such restrictions set out in the Covenant, or through invoking the possibility of introducing reasonable limitations on certain rights, such as article 9 (right to personal liberty) and article 17 (right to privacy), in accordance with their provisions.
(d)States parties cannot resort to emergency powers or implement derogating measures in a manner that is discriminatory, or which violates other obligations they have undertaken under international law, including under other international human rights treaties from which no derogation is allowed. Nor can States parties deviate from the non-derogable provisions of the Covenant - i.e., article 6 (right to life), article 7 (prohibition of torture or cruel, inhuman or degrading punishment, or of medical or scientific experimentation without consent), article 8, paragraphs 1 and 2 (prohibition of slavery, slave-trade and servitude), article 11 (prohibition of imprisonment because of inability to fulfil a contractual obligation), article 15 (the principle of legality in the field of criminal law), article 16 (the recognition of everyone as a person before the law), and article 18 (freedom of thought, conscience and religion) - or from other rights which are essential for upholding the non-derogable rights found in the aforementioned provisions and for ensuring respect for the rule of law and the principle of legality even in times of public emergency, including the right of access to court, due process guarantees and the right of victims to obtain an effective remedy.
(e)In addition, States parties cannot derogate from their duty to treat all persons, including persons deprived of their liberty, with humanity and respect for their human dignity, and they must pay special attention to the adequacy of health conditions and health services in places of incarceration, as well as to the rights of individuals in situations of confinement, and to the aggravated threat of domestic violence arising in such situations.(…)
(f) Freedom of expression, access to information and a civic space where a public debate can be held constitute important safeguards for ensuring that States parties resorting to emergency powers in connection with the COVID-19 pandemic comply with their obligations under the Covenant.

UN experts (United Nation of Human Rights) with the title “COVID-19: States should not abuse emergency measures to suppress human rights”[52].

Chapter Three: COVID-19 case’s pillars: the specific processes of personal and their legal grounds. How the new Schrems II decision affects the processes.

In the first two Chapters, we had the opportunity to review the topic in general, in reference to a lawful limitation of data protection right. This Chapter is dedicated to a further analysis of specific processes, in order to recognize the processes that were selected from experts, by laws, due to the effort controlling the pandemic. To find out what is the exact problem and estimate legal basis, if any. Since we have derogation and limitation of human rights, at least it shall be lawful. Because even in this era, GDPR continue to be in force[53]. Finally, we have to consider a new entry issue: we depend our jobs or educational system on internet and we use cloud methods, so many data transfers are conducted, especially towards third countries. On the other hand we have Schrems II decision, that revoked Privacy Shield in data transfer outside EU umbrella, so we have to consider whether this decision affects these data processes. Are the platforms that we use safe or/and legal? What we should do to supplement the gabs created?

3.1 The tools that selected against COVID-19 spread and their legal basis

The tools, against pandemic, are outlined as follows:

a.Remote work, in order to mitigate the risk of the disease spread

---

[52] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E

[53] IAPP member site, Fazlioglu M., “Privacy in the Wake of COVID-19: Remote Work, Employee Health Monitoring and Data Sharing”.

b.Contact tracing / Mobile tracking, in order to find out, where is the most infected environment.

c.Distant education and

d.Health data process for the same reasons as above.

The processed data during the usage of these tools, are mostly health data, meaning special category. For examination whether GDPR is applied, data shall be either automated processed or be part of filing system[54].

In general, the legal basis of these data processes, regarding their nature, can be found[55]:

a. either in Article 9 par. 2, GDPR[56]

b. or -for simple data - in Article 6 para. 1, GDPR[57].

These extended methods may need high assessment before selection. Assessment and balancing between privacy, data and other rights' protection, e.g. the right and free of movement, and the public interest and public health protection. Finally, we have always to pay extremely attention to the not always granted principle of data and purpose minimization, which shall be dominated.

---

[54] Article 2 para.1 GDPR.

[55] Tintzoglidou N., "Practical GDPR Guide", 2020, p.228

[56] b.processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; e.processing relates to personal data which are manifestly made public by the data subject; h.processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; i.processing is necessary for 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 medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

[57] c.processing is necessary for compliance with a legal obligation to which the controller is subject; d. processing is necessary in order to protect the vital interests of the data subject or of another natural person; e.processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

a. REMOTE WORK

To mitigate the spread of disease, humanity globally was set in a quarantine period. Private and public sector, more than 90% of them, started the use of the unique and ultimate choice, to work remotely, from home mostly. The subsequence of that was the extremely high amount of distant data process, which enlarge the danger of incidents.

In Europe at least, all public organizations and private undertakings started considering the provisions of GDPR, examining the purpose limitation and the lawful principle. Questions arose, as which is the right purpose for the selected measure or whether existed an other - safer measure they had to consider, whether teleworking was adequate, proper, specific measure.

Teleworking is considered a work plan[58], through technological devices and information technology systems, in the field of a work contract in distance, meaning without physical appearance to the working place that should be offered[59]. But what really is the risk taken, working from home? Why this way of working might be considered as extremely hazard in data protection field?

Working from home may be dangerous for the protection of personal data, not only employees' or employers' data, but also the data of clients, vendors etc. Data are totally unfenced, because COVID-19 was an unexpected fact and the procedures were not set. Only a few enormous, and multinational entities have the ability to mitigate the risk of any kind of data breach incident, that would cause harm to integrity, availability and confidentiality of data processed at home, remotely. Special categories of data also are exposed.

From what? First of all, from the violation and hacking through internet provider, because at home there is no professional internet connection, that is costly. The lines are unprotected and any hacker would intrude to the line stealing precious files.

---

[58] Koronaios Ai., Taxheaven, Article for Remote Working in pandemic era- Cybercrime and personal data, https://www.taxheaven.gr/circulars/33745/arora-thlergasia-en-kairw-pandhmias-kybernoegklhma-kai-proswpika-dedomena

[59] Koukiadis I., "Labour Law", version 8th, 2017, Sakkoulas,pp. 304-307.

Remote work also may means paper work, not only web work. Paper work means also many precious data accessible by the whole family.

It is worth mentioning that, in case of cybercrime, all the three principles of cybersecurity -integrity/ availability / confidentiality- are violated. For that reason, articles 24 (1), 28 and 32 GDPR shall be strictly followed, and "appropriate technical and organizational measures" shall be applied[60].

A protected and with standards remote work[61] prerequisites huge amount of expenses for building a strong VPN system, customized for each employee, back-ups regularly, encryption and locked systems that can be unlocked only using dual authentication, good internet connection for business and not the simple home connection, devices that are lawfully controlled and monitored from employers, installation of firewalls/ antivirus/ original softwares that are up to date, new clauses for confidentiality that would supplement the existing contracts of the employees and all these must be followed by data controllers and processors as well.

Scholars and researchers believe that this period a largest in history cyberattack can happen[62].

Apart from what is already mentioned, issues arises the employees surveillance by the employer. Years ago, in 2017, before the transformation of Working Party Article 29 (WP29) to EDPB, an Opinion 2/2017 was released, concerning the data process at work[63]. In that Opinion, it is mentioned the "Monitoring of home and remote working", it is underlined the risk of such decision for both the data of employers and also the data that employees process while working remotely. Also, it is estimated, that any exaggerating surveillance from the employer upon the employee, is not likely to have as legal basis any legitimate interest of the employer. For instance, there is no legitimate interest for the employer to monitor the employee's way of living while

---

[60] Recital: 83, 74, 75, 76, 77 and in case of breach administrative fine: Art. 83 (4) lit a

[61] Read ENISA's PRESS RELEASE "Tips for cybersecurity when working from home The EU Agency for Cybersecurity shares its top tips for teleworking in times of Covid-19", Published on March 24, 2020, https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home

[62] MacBride St., the FORBES https://www.forbes.com/sites/stephenmcbride1/2020/05/14/why-the-largest-cyberattack-in-history-will-happen-within-six-months/amp/?fbclid=IwAR3EvgBB2Qy-h33B49ck1c-KTg_-RiKrS9zdB4_7zykCl73WFm1VecvPdAE . "…The more devices connected to a network, the larger its attack surface grows, making it easier for hackers to infiltrate the network. In short, each new device is a gateway where hackers can find vulnerabilities in and use it to wreak havoc on your system…"

[63] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

working from home, whether he chats through personal emails or to phone calls or if there is someone else at home or the place where s/he lives etc.

Naturally, it is compatible and imposed that employer shall protect the employees, meaning in emergencies there shall be allowed the process of employees' any kind of data. In many European, as Italy, Germany, France, it is accepted by DPAs. But this process has a limit, and this is the prohibited violation of privacy and non-controlled process of data.

The Greek DPA, on the 15th of April 2020, published the Guidelines for security in remote work[64]. These guidelines deal with anything, that may cause risk for data breach, while working without having physical appearance in the place of the work. These Guidelines aim to raise awareness of data controllers and processors regarding data protection, to impose certain policies and procedures for remote working, to train both employers and employees but also data subjects. These recommendations include the necessary remote access to files and desktop, e.g. VPN network, cloud services that are not appropriate, e.g. Dropbox/Google Drive etc., communication through emails, that are professional and not home accounts, and teleconference that shall be encrypted as a measure provided against the risks. After all encryption is one of the two technological measures for security, proposed directly by GDPR, while there is no other choice provided.

In the notion of remote work, we face also the remote surveillance of the employees from their employers[65], that was totally banned and is already known since 1980[66] through CCTV or software downloaded to employees devices (PCs), but now is happening with further ways. Remarkable is, the obligation of security of remote worker privacy against any surveillance due to the Directive 90/270 that lead to article 5 GDPR and the principle of proportionality.

Formal notification of the employees from the employer, is needed, where the specific purposes for such surveillance shall be analyzed. That may happen through the supplement provisions in existing contracts and the context is what articles 13 and 14

---

64 https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/HOME/FILES/KATEFTHINTIRIES%20GRAMMES_TILERGASIA.PDF

65 Igglezakis I, "Surveilance and Monitoring of electronic communication in workplace" DIMEE 1/2005, p. 55.

66 Douka V., "The personal data protection in dependent work", 2011, pp.182-191.

GDPR imply. Notification leads to transparency in the above data process, but also policies and procedures are needed, proving the accountability of data controllers and processors.

Finally seeking for the legal basis, that remote control shall be relied on, it can probably be:

a.the law and the provision that allow or implement remote control e.g. up to 40%,

b.the contract and the special clauses that shall be added[67] or

c.the legitimate interest of the employer. In the last case, there shall be a data protection impact assessment, as article 35 GDPR implies. For instance, if a special software shall be downloaded to employee's device that collects any kind of data, while remote working, or if s/he accepted from employer a device that may collect geographical or health employ's data, this technique shall be examined, balanced and can be followed only if passes the proportionality test. Elsewhere it shall be considered as illegal process and rejected as such.

Naturally, employees' consent cannot be legitimate basis for any process conducted by employers, for the simple reason that an employee can never provide her/his consent "freely, specific, informed and unambiguous"[68].

b. CONTACT TRACING/MOBILE TRACKING[69]

The most crucial process, that is followed during COVID-19, and has already occupied many scholars and experts, is contact tracing[70] devices and applications. It is a "Orwellian nightmare", like a UN expert said. Contact tracing is crucial, because of the States penetration to the human rights. Naturally, the speed of the disease's spread has approached that level, and only with such method authorities could recognize the alert areas, where there is high level infected and imply stricter measures. Regardless of that

---

[67] Clauses both for employees information -due to articles 13 & 14 GDPR, about the data processes that may occurred and the technological methods that may be follows- and confidentiality clauses as well.

[68] Article 7 specified further in recital 32 of the GDPR.

[69] Also known as "Proximity Tracing" apps.

[70] People who have been in close contact (according to criteria to be defined by epidemiologists) with an individual infected with the virus run a significant risk of also being infected and of infecting others in turn. Contact tracing is a disease control methodology that lists all people who have been in close proximity to a carrier of the virus so as to check whether they are at risk of infection and take the appropriate sanitary measures towards them.

necessity, though, it is the most aggressive process and monitoring method of data, that, after that procedure, are not considered personal any more.

That process was urged by WHO, in order to track and monitor probable victims of COVID-19[71]. That method also implied by "Joint European Roadmap toward lifting COVID-19 containment measures"[72], by the European Council and the European Commission on 15th April 2020 and also by the European Center for Disease Prevention and Control (ECDC). EDPB has expressed the opinion that the legal framework that operates data protection is so flexible, in order to both help controlling the pandemic and to protect fundamental human rights as well[73]. In mt view the above declaration is only for camouflaging the truth that is, by this way -that is not considered as productive- data protection dismissed in favor of public health.

Still, how easy or granted is that EDPB's belief for data protection? Is this belief realistic through that kind of process? The dangers that are hidden behind contact tracing, are who may process subjects' data, even worse special category data, how they process them, for how long and where the selected data are transferred. There shall be appropriate safeguards and cybersecurity. The Supreme Court of U.S.A in Carpenter vs. U.S. case, had another opinion[74]: "Mapping a cell phone's location (for an extended period) provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious and sexual associations".

The way this technological method works, is by downloading an application to smart devices, like mobile phone or smart watch or any smart device, and when this device with the certain app is approximated to a victim, less than a meter distance, and if that victim has also downloaded into her/his device such app, the two devices export-

---

[71] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf

[72]https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

[73] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020, EDPB, p.3

[74] www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

import signs and notifications. By that way, infected people will be isolated for the period of time that may infect other[75].

The conditions for operating this method is that anyone -and furthermore the victim itself- has to download that app or possesses that kind of smart device, because without these conditions, contact tracing is not possible. One more condition for operating that process is the victim has been tested and found medically to be a victim, otherwise again that method does not work[76].

This kind of procedure collects and process two kinds of data:

a.Location data, that are mostly anonymized. Anonymized data stand outside the scope of GDPR, but it stands upon the scope of E-Privacy Directive[77], to the level that location data are collected by telecommunication providers. Sometimes though, location data cannot be fully anonymized, and in that case there is application of GDPR provisions.

Either way, the download of this application is relied on users' consent as a legal basis. That means there cannot be an obligation or implementation for downloading the app of this app or the possess of smart device. Also, nobody can impose the health examination, in regular basis, of persons who may be considered as asymptomatic. That process works only in a freely voluntary basis. Law or employment contracts or even worse the legitimate interest of data controller/processor, cannot be the legal basis for a data subject to download the application.

---

[75] Abeler J, Bäcker M, Buermeyer U, Zillessen H, "COVID-19 Contact Tracing and Data Protection Can Go Together". JMIR Mhealth Uhealth 2020; 8(4). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7173240/

"…As soon as an app user is diagnosed with COVID-19, the doctor making the diagnosis asks the user to share their locally stored data with the central server (Figure 2). If the user complies, the central server receives information on all the temporary IDs the "infected" phone has been in contact with. The server is not able to decrypt this information in a way that allows for the identification of individuals. However, it is able to notify all affected phones. This is because the server does not need any personal data to send a message to someone's phone. The server only needs a so-called PushToken, a kind of digital address of an app installation on a particular phone. This PushToken is generated when the app is installed on the user's phone. At the same time, the app will send a copy of the PushToken, as well as the temporary IDs it sends out over time, to a central server. The server could be hosted, for example, by the Robert Koch Institute for Germany or by the National Health Service for the United Kingdom. This way, it would be possible to contact phones solely based on temporary IDs and PushTokens whilst completely preserving the privacy of the person using the phone…"

[76] https://www.homodigitalis.gr/wp-content/uploads/2020/04/HomoDigitalis_Report_COVID19_and_Digital_Rights_in_Greece_22.04.2020_Final.pdf

[77] 58/2002/EE first e-privacy directive.

b.The app also collects health data[78], through algorithms and that needs precaution. Collecting health data, is based upon the legal basis given by article 9(2)(j) GDPR, regarding data necessary for scientific research purposes or statistical purposes.

c.Finally, information that stand in the owners device and is protected by ePrivacy Directive[79].

Contact tracing shall be designed by default. Again, there shall be a data protection impact assessment, as article 35 GDPR stipulates, because of the severity of the procedure and the risks that are assessed is high.

The principles that shall apply is limitation of collecting data storage, only for the COVID-19 duration, after which period shall be either anonymized or deleted with special care and protocols. According to the author's opinion is, that data selected by that kind of apps, consist atomic bomb in the hands of uncontrolled data controllers and processors.

The main question is, whether these apps are, finally, safe and effective for controlling COVID-19. It is declared, that there is no need to be known the details of specific users but only the geographical stigma and the area maters, where many victims are concentrated. In the view of the author this is only the half truth. It s the half truth because, the COVID-19 victim, especially the non-symptomatic, does not stay still in an area that is under surveillance. The "victim" may move to several directions and spread disease to dozens of her/his contacts. So, the most efficient way to monitor the disease would be the surveillance of the victims themselves. But this persons' monitoring, means totally penetration to privacy to the maximum level, to the level of abuse and of course means the end of data protection, even for such sacred cause. That is the reason, why there is, at least, a need for a certain impact assessment to be recorded.

What it has to be assessed[80] is:

a.the effectiveness towards the limitation of disease's spread

b.the voluntarily nature of the choice

---

[78] Health data as the disease that subjects are infected of, the medicines they take, whether they were in quarantine etc.

[79] Flett E., Gover R., "European Commission and the EDPB lay out framework for privacy-compliant contact tracing apps". www.westlaw.com/Document/165293880C70011EAB4BE954…084a97727&list=RESEARCH_COMBINED_WLUK&rank=14&comp=wluk

[80]https://www.homodigitalis.gr/wp-content/uploads/2020/04/HomoDigitalis_Report_COVID19_and_Digital_Rights_in_Greece_22.04.2020_Final.pdf, p.15

c.the interim character of the measure

d.the limitation of data storage

e. The absence of profiling

f. The limitation of purpose

g, the description of anonymized procedure.

Due to severity of the specific process, there is a highly need of uniform and globally treatment of contact tracing, and not only in the EU area. As data controller shall be designated per each State centrally, for example the national health authorities, because of the duty of accountability. But on the top of the local authorities, there has to be a global supervisor, with common guidelines. But that seems not to be possible, because of the difference of legal systems and perspectives of the States[81].

Two of the first States, that brought this method to the table of the battle against pandemic, was Singapore and South Korea, in March 2020[82]. On 10th of April 2020, the two giants, Google and Apple, made the announcement of the use of Bluetooth for tracing approximate devices' users diagnosed positive to COVID-19[83]. In Europe there was an initiative, through the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)[84], with the aim to safeguard privacy and prevent breaches.

Worth mentioning, is the position towards these apps, of the Italian DPA, that was presented at a parliamentary hearing[85]. The key points of the presentation was the need for extremely voluntary basis, for limited storage and for less identifying

---

[81] E.g. Sweden has other perspective towards pandemic than Greece.

[82] https://www.etui.org/sites/default/files/2020-06/Covid-19%2Bcontact-tracing%2Bapps%2BCorona%2BPonce%2BPolicy%2BBrief%2B2020.05.pdf

[83] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf & "https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing- technology/ The announcement included the publication of three draft technical documents on Bluetooth and cryptography specifications and framework documentation."

[84] www.pepp-pt.org/

[85] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf p.47

information, leading to the proposal of existence of specific statutory offenses in case of breach of the above conditions.[86]

To summarize, admission and selection of contact tracing technique towards the COVID-19 battle, is a topic that extremely bothered all States globally. The maximum legality and transparency is the requested. The free will of the citizens to give their consent for such an ambiguous process, depends on the confidence of the data subjects, that their privacy is safe. Confidence towards the States, that State confide certain expertise in order to build the policies and procedures for such a process, who have the certain experience to recognize the risks and mitigate them. Confidence towards the providers and constructors of such apps. Confidence towards the net either vpn that will connect the devices, in order not to be hackerized or breached.

---

[86] Also see https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf "Alongside legislation, procedures to examine contact-tracing apps before their release and the involvement of authorities in their development can ensure their conformity with data protection principles and GDPR requirements (see Section 4.1.2 above on involvement of DPAs). In Italy, for example, the competent Ministry set up a task force of experts - including from the WHO and the national DPA (as observer) - to assess proposals for the development and authorisation of a contact-tracing app.214 The Finnish parliamentary working group on information policy is involved in a process to underline data protection and privacy requirements in advance. In other Member States, other authorities are also consulted or involved in assessing the legality and/or efficiency of apps, such as the Attorney General in Ireland or the Ombuds institution in Croatia.215 However, media in Bulgaria, where the app is officially approved, noted that neither the authorities nor the developers of the app, submitted it for independent assessment of its data protection compliance.216

In the majority of Member States, contact-tracing apps are based solely on the processing of Bluetooth proximity data, as the European Commission and the EDPB recommend (Austria, Czechia, Germany, Denmark, Estonia, Croatia, France, Finland, Ireland, Italy, Latvia, Poland and Portugal). In Estonia, although the use of location data was discussed, the app will ultimately only process Bluetooth data.217 However, apps in Bulgaria, Cyprus and Lithuania are based on network and/or GPS location data; in Slovakia the available app uses both Bluetooth and location data.

Evidence confirms that contact-tracing apps mostly take a decentralised approach, with users' data (such as keys, identifiers, etc) produced and stored locally on their devices (Austria, Cyprus, Germany, Estonia, Finland, Ireland, Latvia, Poland and Portugal). In some Member States, authorities can have limited access to users' data: in Estonia, Poland and Finland, users can voluntarily share their Bluetooth proximity data with health authorities.218 In Portugal, a user diagnosed with COVID-19 would have to authorise a health professional to share this data anonymously to warn others.219 However, in Belgium, Bulgaria, Denmark, Czechia, France, Spain, Lithuania, Italy and Slovakia, contact-tracing apps use centralised, so-called 'backend', models where users' data are stored and processed on a central server. The European Commission and EDPB do not specifically advocate either approach. The European Parliament, however, proposes the use of decentralised models by Member States.220 The choice between systems prompted much discussion amongst academia, NGOs and public authorities. These exchanges highlighted issues around the risk of function creep, identification of data subjects or vulnerability to cyberattacks, with centralised systems attracting particular concern.221

Contact-tracing apps in Austria, Bulgaria, Denmark, Spain (Basque region), Latvia, Lithuania, Poland and Slovakia also include further health functionalities, such as symptom reporting, medical screening and communication with health authorities. For example in Denmark, the app informs users if their COVID-19 test is positive.222 The app available in Lithuania enables daily coronavirus symptom tracking, and the receiving of health advice and information. In Austria, a draft law would allow voluntary screening functionalities to be added to the existing contact-tracing app to enable users to transmit personal and health data to the health authority.223 Combining such functionalities in one app could lead to 'function creep'. The European Commission stresses that users should be able to provide their consent separately for each of an app's functionalities. In Bulgaria, Denmark, Germany, Italy, Spain and the Netherlands, different apps are available for processing and communicating health data."

Confidence that this sacrifice of privacy will be time limited only for the pandemic era and not forever[87].

Consent, without established confidence that data subjects are safe, will never be given. Because, data subjects can not tolerate more data process than needed.

c.DISTANT EDUCATION

"The UN Convention Committee on the Rights of the Child set out in 2001, that Children do not lose their human rights by virtue of passing through the school gates. Education must be provided in a way that respects the inherent dignity of the child and enables the child to express his or her views freely…"

Social distancing is the best way for ruining the disease's chain and eliminating present pandemic, with all the parameters this distance causes. We have already analyzed the remote work and we have concluded that the remote-mode shall be chosen for all human actions. Of course, there is no education, if it is distant. The aim of education, from nursery to high school and universities as well, is mainly the socializing of young persons, in order to find the way to communicate with others, to work with them, to create relationships. In this emergency, socialization is the one needed less, not saying is not needed at all, as long as this isolation is considered as an interim measure and not permanent way of living.

Most of the States, in a very short time limit, managed to qualify schools and universities to change their routine. While many States globally were set in quarantine as a whole, pupils and students were being educated on line and in most countries that method has been continued after quarantine. Distant Education means all pupils, students and teachers/professors have the ability, meaning the equipment for conducting courses on line[88].

---

[87] Abeler J, Bäcker M, Buermeyer U, Zillessen H, "COVID-19 Contact Tracing and Data Protection Can Go Together". JMIR Mhealth Uhealth 2020; 8(4). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7173240/

"…The reason most frequently brought up against an installation is the worry that the government could use the app as an excuse for greater surveillance after the end of the epidemic. If the government wants as many people as possible to install the app, it should take these concerns seriously and refrain from using location data. Contact tracing works without it…"

[88] We are dealing with the on line education at the same time, not asynchronous distant education.

The prerequisite, for the right use of distant education, is all of the participants shall know, how to use electronically devices and how to be connected, but also means that the platforms and the devices can be compliant enough for protecting data. Also means, that are being adopted technical and organizational measures for data protection by laws (national and GDPR).

The data risk is larger, when the process concerns data subjects in sensitive age, that is underaged pupils, teenagers and younger than the age of 13.

The key elements, that have to be checked in distant education are:

a.that educational system shall not financial burden children's family,

b.children are more prone to leave an improper "fingerprint" online and that risk has to be eliminated,

c.children are mostly not aware of their rights[89] and shall be informed,

d.there is a high risk for profiling and also high risk for transfer of data in third countries, through the platforms used and shall be secure locks.

Some of the risks, that are faced through distant education are hacking pupils' - students' profile and accounts stealing material, the recording of the course by students or teachers and the usage of that material with any way possible, taking pictures of underaged persons and uploading them to illegal sites, strangers penetrating the course and causing problems.

Recommendations, Policies and Guidelines to education authorities as data controllers, to vendors as data processors, to professors and to legal guardians of the children (if they are underaged) are given to a very useful "Draft for Children's Data protection education Systems" on 11th February 2020[90] by Consultative Committee of the Convention for the protection of individuals. For mitigating risks, caused by distant education, in each State was conducted an effort to be selected the safest platform. Among prerequisites and standards were that, through these platforms, would not be permitted the collection of sounds and images, there would be created locked classes with time limit, both students and teachers could mute and unmute (as well video in and out) when necessary.

---

[89] Convention of the Rights of the Child

[90] https://rm.coe.int/t-pd-2019-06bisrev2-en-education-guidelines/16809c3c46

The educational platforms are in fact the highest problem, with several faces. One more problematic is that, in countries like Greece, the structure that is followed leads to a division of public and private education. Data controller for public schools, in Greece e.g., is Ministry of Education while controller for private schools is the legal person, who has the admission to operate, meaning the higher administration of private school itself from the competent authority[91]. Because of this diversity/ differentiation, we deal with several platform choices, because each private school select different platform and not the central platform that was selected by Ministry of Education. For that reason, private schools are not covered by the impact assessment that Ministry of Education elaborated[92], but have to conduct their own, and mostly by design and default. Most of private schools, have chosen also platforms that may be more student-friendly, but are high perforated, referring to cybersecurity or face the problem that was caused by Schrems II decision[93], that has not been solved up to now[94].

Worth mentioned to that point, is the Greek's DPA Opinion 4/2020[95], for the DPIA conducted by Greek Ministry of Justice. That extremely long Opinion market the above DPIA's problematics and asked them to be corrected in a deadline of three months, that is expired. The DPIA was conducted in a short time because of the emergency, for that reason the gabs were many. The major fault of the above DPIA, though, is that is presented to be approved by Ministry's DPO, who had no such responsibilities and duties by GDPR.

The principles that dominating distant education, are again the implication of lawful data process, limitation of purpose and of data storage and of course transparency needed through certain policies, procedures and notifications from the chair of schools/ universities to teachers/ professors, students and legal guardians, when

---

91 Of course, the processor is the provider of the selected platform.

92 https://www.minedu.gov.gr/publications/docs2020/Μελέτη_Εκτίμησης_Αντικτύπου_rsz.pdf

93 see below Level 2.

94 It is expected that up to December 2020, EDPB will release guidances and there is a standard contractual clauses' draft for public consultation until 10th, December 2020. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

95 https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=227,67,104,7,118,167,124,247

students are underaged. The legal basis in these processes is either the law, article 6 (1) (c) GDPR, in connection with the exercise of official authority of the controller, article 6 (1) (e) GDPR or the consent, article 6 (1) (a) GDPR, provided by students or their legal guardians -where underaged pupils[96].

d.HEALTH DATA PROCESSING

During the period from the breaking point of pandemic's outbreak, the highlights were directed towards the health sector and the data that should be collected. Especially, the sensitive or the special category data. The European Union Agency for Cybersecurity, ENISA, has mentioned health sector has become "direct target or collateral victim of cybersecurity attacks" [97].

Health data[98] collection and process is the main target of many procedures followed this period, as the above mentioned contact tracing or even remote work. Some new entry procedures have been recently adopted by public organizations and private entities, as thermal cameras, drones for infected person's surveillance, national health catalogue.

Apart from drone surveillance that it is collected mainly pictures and sounds, and seems not to be supported by any legal basis, so it is considered as unlawful data processing, the other procedures can be selected by authorities, as long as no data or only anonymized data are kept, either automated processed or in filing system and only for the purpose needed[99]. E.g. the material that thermal cameras collect, meaning the temperature of the passengers, shall not be kept or shall be anonymized if it is filed and saved. As far as the national health catalogue, the elements shall be anonymized and kept only for scientific reasons and research or statistics.

---

[96] https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter?fbclid=IwAR0geAAqTdiI0d7oKYjpJp53BZkN0JI9RM_vz-0pnb5srEn4wDg5MawZpyM

[97] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic

[98] "According to Article 4 (15) GDPR, "data concerning health" means "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status". As indicated by Recital 53, data concerning health deserves higher protection, as the use of such sensitive data may have significant adverse impacts for data subjects. In the light of this and the relevant jurisprudence of the European Court of Justice ("ECJ"),4 the term "data concerning health" must be given a wide interpretation. "

[99] Article 9 (2) GDPR

It is a vertical change of the routine in our lives. Some examples that we experience every day are, the need to complete questionnaire for visiting gym or public services with questions -whether we feel certain symptoms, that WHO recognizes as COVID-19, or whether we have traveled to suspicious for COVID-19 spread counties etc. The need of undergoing temperature control before entrance for instance Courts or other entities. The need to express to children's school whether there are persons with vulnerabilities in order children not to be physically present in class but attend distantly. These examples and many other that we practice lately, expose everyday our health data to innumerable amount of people. We have no information about almost nothing, where are these sensitive data kept, for how long, where are they transferred. Are we going to have any problem in the future because of our disclosure of data, for instance are we going to enjoy health insurance or insurance companies have access to national health catalogue? These gabs have not been filled yet, even after months from pandemic outburst and even after all this legislative flood worldwide.

Health data shall be processed for scientific purpose and research ("primary use") but they may be collected for other reason ("secondary use")[100]. The legal basis for that process is the Articles 6 and 9 GDPR, depending in the process. Transparency and full disclosure of all information needed[101], as well certain policies and procedures to be conducted, that may add confidence to data subjects while facing such renovated methods.

In this point, shall be mentioned the publication of data, mostly health (as sensitive) data. Authorities shall publish the findings in order to prevent the disease spread. They shall do it anonymously, with numbers or proportions that exist to any area. The extent of publicity is a point that arises many issues because of the stigma that may causes. And that issue is not faced homogeneously by all DPAs, e.g. Irish DPC accept extended disclosure of data[102]. DPAs safeguard personal data, especially when are processed sensitive data that data subject wants to hide, having the anxiety of a stigma that might carry eternally. When, we talk about contradiction between data and privacy

---

[100] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

[101] Article 13-14 GDPR.

[102] Mitrou L. "Personal Data in times of COVID-19, Syntagma Watch www.syntagmawatch.gr/trending-issues/ta-prosopika-dedomena-stin-epoxi-tou-koronoiou/

protection and the freedom of press and expression, we are referring to not absolute rights that shall be ad hoc balanced[103]

3.2 How the new Schrems II decision affects the processes

Worth mentioning is the new C-311/18 Decision Facebook Ireland and Maximillian Schrems, known as Schrems II decision104. That Decision re-examined the Standard Contractual Clauses (SCCs) and the previous Decision 2010/87/EE. These Clauses used to cover the lawful transfer of data towards third countries, meaning the place where GDPR does not apply.

That decision enjoys unique importance, because many processes that are followed, during COVID-19 trying to resist pandemic's consequences, depend on methods that indeed transfer out of E.U.. We are referring to platforms for distant education, e.g. Google Meetings, teleconference for remote work, cloud computing for work as well for contact tracing etc. In particular, the contact tracing apps are relied on Apple/ Google system and the process conducting through smart devices.

Worth mentioned is the Article 49[105] GDPR, which offers derogations for data transfer to third countries as long as the transfer is:

"- Explicitly consented by data subject
- Necessary for the performance of a contract between the data subject and the controller
- Necessary for the conclusion or performance of a contract concluded in the interest of the data subject
- Necessary for important reasons of public interest
- Necessary for the establishment, exercise or defense of legal claims
- Necessary in order to protect the vital interests of the data subject or of other persons
- Made from a register which according to Union or Member State law"

The Schemes II Decision examined the Privacy-Shield Decision between EU and USA, and whether this Decision was adequate, for safe data transfer from EU to USA. The Privacy-Shield Decision Shield was finally, decided and judged as invalid hereafter. Due to Article 46 GDPR, this kind of judgement affects data transfer in any third country. This decision sets in questioning the process, through platforms, for educational or professional reasons or any cloud service dealing with data centers established outside EU, even if there are representatives established in EU, as branches of mother entities.

---

[103] Article 85 & recitals 4, 153, GDPR

104 http://curia.europa.eu/juris/liste.jsf?num=C-311/18

[105] https://www.privacy-regulation.eu/en/article-49-derogations-for-specific-situations-GDPR.htm

The solution for this problem is:
a.either data isolation that means that the entities will never collaborate with entities outside EU. They will be restricted within EU and that will harm the free movement of data, meaning the ratio of GDPR.
b.or supplementary measures, that are needed for such data transfer, which transfer is unavoidable, if we want to work or do all the good practices, that we have done for so many years.
These measures are going to be suggested with Guidelines that are expected by EDPB in December. There is conducted a public consultation (from 12 of November up to 10th of December 2020) for the new draft for Standard Contractual Clauses (SCCs) for safe data transfer to third countries, and also "Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems"[106] is published . A former judgement of that SCCs draft is that there is a rather non specific text, with many gabs and so much documentation implied that may not be a realistic choice for data transfers.
We have to wait to examine if that draft will be changed in future.

Chapter Four: Balancing test and the Principle of Proportionality

"Asking people to choose between privacy and health is, in fact, the very root of the problem. Because this is false choice. We can and should enjoy both privacy and health."

— Harari, Y.N. Financial Times, 22nd March 2020.

We have examined, up to now, how data protection right is approached, through the new methods that came into our routine, struggling against COVID-19. How the restriction of data protection right was predicted by laws, and how this limitation is nowadays a reality. Another question that has to be solved, but still is not easy to be corresponded, is how data protection right can be balanced with other rights, as the right to health and to life and to public interest, what should we balance and what are the results esteemed. That high technique of balancing rights, prerequisites a profound

[106] https://edpb.europa.eu/sites/edpb/filFrequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schremses/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

data protection impact assessment, especially for the special categories of data and, also well establishment of the principle of proportionality.

4.1 Article 35 GDPR Data Protection Impact Assessment

Privacy and dignity are goods/ rights that shall a free person enjoys in a free society. Public interest, public safety and health are goods, rights that shall all free persons enjoy in a free society. How can we balance these, somehow, contradicted rights that have the same weight?

The free-from-coronafear and normal days, seem to be so far away, either as past memories or future expectations. It is considered as a luxury to cast an eye to data protection, while there is fear for health humanity worldwide. Yet, personal data, privacy, self-determination shall be protected and have not lost their power, even at these strange moments.

Public interest is a vague as legal concept. It is not specific but shall be specified and justified by legal basis, in order to be protected, otherwise it may be examined by Courts, whether there was an abusive extension of that notion[107]. Public health is part of public interest because public health direct affects public interest.

Estimating where the scales close, public interest vs data protection, a test is needed. And will be needed for a long time so we have to consider it as a new custom. That test can balance the contradicted rights ad hoc, in each process and at each time period. What shall be examined is:

a.whether each process, that violates somehow subjects' privacy or data protection, is the proper method or shall be selected other process that intrudes less into our lives, through a risk and impact assessment. And also,

b.if the method is indeed the proper, whether the process is proportional or has exceed the limits, the proportionate test, as it is called widely.

That means practically, that before choosing the method that helps minimizing the curve of COVID-19, expertises shall take into consideration the risks that are undertaken and carried by this method, if there are other methods that threaten less risks, and if these risks are proportionate to the legitimate purposes. The reason for

---

[107] Panagopoulou - Koutnatzi, "Data Protection in pandemic times", https://www.constitutionalism.gr/wp-content/uploads/2020/03/2020.03.28_Panagopoulou_privacycoronavirus.pdf?fbclid=IwAR2BnMVMKA4bMToCNxQ2xoTMQal3yzpXY7gov-xYnolFclRsxLewjdjVx5o

that risk and impact assessment is because in many cases, when there is time pressure, the choices that are made are not correctly estimated.

Is there time for assessment? The answer is probably negative. Everyday missing is a bigger scale for COVID-19 victims or losses. Writer's personal view is that, there can be no adequate Data Protection Impact Assessment (DPIA), during pandemic, and the only question, that is considered in fact is do we want to eliminate victims, whatever this means or do we want to protect data and privacy for the CoronaSurvivors? That conclusion can be very disappointing, because, if this way of thinking prevails, then the answer will definitely be, that we decide to save lives, with any cost. And that will practically lead GDPR to be set aside. Governments and authorities have corona-fatigue and that is obvious and expected. COVID-19 doesn't wait and scans everything in his path. Though, the situation cannot be an excuse for setting aside the privacy or data protection. Some day, COVID-19 will pass but the stigma for all the subjects, who have their data published, will remain, both for themselves and for their families.

On the other hand, Robert Kirkpatrick, director of UN Global Pulse in 2018, declared that:

"ethical decision-making requires minimizing not only the risk of data misuse, but also that of missed use, that is, of leaving crucial data resources untapped in the global fight against famine, plague and war."

4. 2 DPIA examples

Naturally, data leads to a better risk management. The solution for this problematic is that given in article 35 GDPR[108]. A DPIA shall be conducted for overall measures taken during pandemic and not for each one, for not wasting precious time tackling pandemic.

For better understanding, there are some examples given[109], some processes that shall be conducted a DPIA:

---

[108] Article 35 (1) GDPR: "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."
In connection with Recital: 75, 84, 89, 90, 91, 92, 93
And administrative fine: Art. 83 (4) lit a

[109] Whitcroft O., "A guide to data processing during a pandemic", p.2

- For collecting health data, it must be assessed how many data are needed for what specific purpose. Competent authorities shall consider the principle of minimization of purpose and data. Or collecting health data for research it must be considered the anonymization or pseudonimization. There is essential an examination of methods that are recommended for collecting those data, that are processed and filed, and what is/are the legal basis for that process.
- When there is a need for disclosure information about COVID-19 patients, within an entity, it must be assessed whether there is need for disclosure names and other personal data. Entities have to consider technical measures GDPR recommends, as anonymity or pseudonymity and of course the legal basis.
- When working or educating from home, shall be considered the cybersecurity methods needed and shall be assessed the impact of the platform's function towards collection and process subject's data. The risks that are at stake, shall be able to be recognized in order to be overcome and recovered, when they might be happened. In particular, for online (distant) education, many scholars, associations (for example in Greece the Association of Private Schools) have the absolute opinion that no platform is safe enough for that kind of education and is not a proper way for online education, at least for pupils of primary and nursery school. It should be selected other methods that would lead to the same results without risks, for instance education that would not be provided in real time but asynchronous education. Though, writer's opinion is declined to that perception, Ministry's (of Education) DPIA was published, as it is above mentioned, and the conclusion was that kind of distant education has minimum risks and is safe for pupils/ students. Of course Greek Data Protection Authority was not totally convinced by that assessment and asked Ministry to supplement DPIA. And at this point is located, what causes ambiguity to parents, that are obliged to permit their children to participate in distant educational platforms. That is, the necessity to conduct processes very fast, and speed means gabs that are not filled.

Since competent authorities estimate, that methods taken in the present emergency are the proper and are used with the proper way, disclosure to data subjects as article 13 and 14 GDPR shall be available, due to principles of transparency and accountability for data controllers/ processors. It is granted, that such an intrusion to privacy and

personal life, demands the maximum respect of human's dignity and that is provided through explanation.
Humans shall know what is taking place in order to collaborate with authorities and State.

Chapter Five: Conclusions

Finally, is GDPR an obstacle for saving humanity from this pandemic and health crisis? Or, the necessity to control pandemic violates data protection, along with dignity and self-determination? Data process in COVID-19 era, especially health data, may be lawful, through some safeguards, that GDPR or other specific provisions provide. Though, is it moral?

5.1 COVID-19 vs personal data: The next day

Personal data protection, in ages of emergency, has not the meaning of banning the public good and interest, as the public health. On the contrary, Recital 4 GDPR imposes the balance data protection right with the contradicted rights, based on the principle of proportionality[110]. By this lawful way, the Chair of the Committee of Convention 108, Alessandra Pierucci, states, that restriction in data protection is justified "solely on a provisional basis and only for time explicitly limited to the state of emergency".
The above key elements are the prerequisites, for all processes, implied by the emergency, in order to be accepted, in the end of the day. The time limit that restrictions are going to have. What will be the next day though? Are we going to live eternally the way we have just learnt? How much time is this explicitly limited time?
Beyond the limited-time condition, added value has the condition/ prerequisite of security, mostly cybersecurity, because the majority of the new selected processes are relied on internet. What are the safeguards for data process? What are the technical

[110] Panagopoulou-Koutnatzi F., "Issues of constitutionality in distance school education",Journal Adm.Law 3/2020, pp. 292-303.

measures that authorities, employers, school chairs, researchers etc have taken for safeguarding all this mass data that are being processed by them?

Writer's personal view is that, the doubts have not been eliminated. There is no complete and transparent information about the above mentioned conditions for decreased protection of personal data. The pressure of time and the anxiety, due to the danger to face a crash of health system, has prevailed upon the personal data protection, which has lowered priority level. There is an ethical portion, that has been underestimated and new technologies often seem to invalidate or to violate principles for ethical process and use of these technologies, especially those who are relied on artificial intelligence (AI).

After all, it is stated in "Ethics guidelines for trustworthy AI of the High-level Expert Group on AI"[111], that:

"trustworthy AI should be:

(1) lawful - respecting all applicable laws and regulations

(2) ethical - respecting ethical principles and values

(3) robust - both from a technical perspective while taking into account its social environment"

Also, the above guidelines have seven requirements, among which, special attention is given to the respect of data protection and the implication of transparency. This transparency that is not granted nowadays.

Since there is necessity to process data the following shall be confirmed: process and purpose shall be clear, accurate and transparent, there shall be only on certain legal basis, subjects' rights are confirmed mostly the access to their data, there are measures for information security, there must be certain time limits, impact assessments shall be conducted by default and by design.

The mentioned conditions, writer claims that, are not totally followed by authorities and finally, the "by design and by default" of processes, that could guarantee data protection, has not been fully completed, nor there is complete conviction, that all the treatments analyzed above are required. For instance, contact tracing apps are not fully reliable and there is not efficient evidence for the proper collection and process of personal data.

---

[111] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

On the contrary, contact tracing seems not to be an efficient measure against COVID-19, because that measure cannot effectively help towards the battle against crisis. After all, any user can withdraw her/his consent and delete the app from the device, also there is no time limit for the application and there is no confidence that data are fully anonymized, since profiling is conducted.

Not all the new methods and technologies are needed during these tough times. The selections shall be tailored after efficient balancing and risk / impact assessment and these decisions shall be revised in every stage of the evolution of the crisis. Also which data are useful for the battle against pandemic, is a decision that can be changed, depending on the flow of the disease and always regarding the principles of data and purpose minimization, the principle of confidentiality and information security.

There has to be considered another point, that may causes adversities: as it is mentioned above, for contact tracing apps the owner of the device has to give her/his explicit consent. How, finally explicit and freely given is that consent? What will be happened if that owner withdraw that consent? What other legal basis will be selected or if that is impossible, what is plan B? Unfortunately, there is also no answer to that consideration. It is definitely a gab that will cause difficulties, when Authorities might use this kind of apps

After all, do we have to sacrifice and hand over our data, with the unique justification that it is necessary because of emergency? The answer is self evident and is negative. Humans shall acknowledge the legal requirements for the above processes, their rights and how they can claim them. In Democracy, States are obligated to save lives avoiding losing in fact Democracy.

The promise and challenge for Governments is to eliminate COVID-19 in the proximate future. The promise also, that humans are reassured by States, that personal data protection will not be eliminated after all this crisis. Or that humans will not be stigmatized because of the data process made during the health “war”.

Finally, will the next day find us free from all the derogation of data, or will we possess a familiarity to be data-abused? That will be revealed indeed the next day.

The present day, we can only know our rights, and try to resist against any monitoring that is beyond lawful limits and purposes, or that provides us no disclosure and notification about basic information we need to take into account. And that is the resistance we can only achieve: To be efficiently informed, as data subjects, about our

rights and to claim our rights' best application that shall depend on specific legal basis, with all the respect - on our behalf - to public interest, health and wellness.

Stay COVID-19 safe!

Bibliography

LEGISLATION-GUIDELINES

- Regulation (EU) 2016/679
- Constitution of Greece
- Relevant Guidelines by the EDPB, the national DPA's and the Hellenic DPA, ENISA
- ECHR (European Charter for Human Rights)
- FRA/EctHR/EDPS, Handbook on European Data Protection Law, 2018

BOOKS

- Abeler J, Bäcker M, Buermeyer U, Zillessen H, "COVID-19 Contact Tracing and Data Protection Can Go Together". JMIR Mhealth Uhealth 2020
- Flett E., Gover R., "European Commission and the EDPB lay out framework for privacy-compliant contact tracing apps". www.westlaw.com
- Rücker D./Kugler T., New European General Data Protection Regulation, 2018

In Greek

- Akrivopoulou X.,"In Between Autonomy & Intimacy - Self-defining the right to privacy", 2009
- Douka V., "The personal data protection in dependent work", 2011, Sakkoulas
- Koukiadis I., "Labour Law", version 8th, 2017
- Mitrou L, The Personal Data Protection Right, 2012
- Tintzoglidou N., "Practical GDPR Guide", 2020, Nomiki Vivliothiki

RESEARCH PAPERS/SCIENTIFIC JOURNALS

- Fazlioglu M., “Privacy in the Wake of COVID-19: Remote Work, Employee Health Monitoring and Data Sharing”
- Findlay M., Jia Yuan Loke, Remolina N, Tham B, Research Paper No. 2020/02, “ETHICS, AI, MASS DATA AND PANDEMIC CHALLENGES: RESPONSIBLE DATA USE AND INFRASTRUCTURE APPLICATION FOR SURVEILLANCE AND PRE-EMPTIVE TRACING POST- CRISIS” Singapore Management University, Centre for AI and Data Governance
- Granic M.-Antunovic K., Journal of Swiss Chinese Law Review Issue No.1
- MacBride St., the FORBES
- Whitcroft O., “A guide to data processing during a pandemic”

In Greek

- Akrivopoulou X.,”The Data Protection Right through the lens of Privacy’, Theory & Praxis of Public Law Journal Session 7, 2011
- Homo Digitalis
- Igglezakis I, “Surveilance and Monitoring of electronic communication in workplace” DIMEE 1/2005
- Koronaios Ai., Taxheaven, Article for Remote Working in pandemic era- Cybercrime and personal data
- Mitrou L. “Personal Data in times of COVID-19, Syntagma Watch www.syntagmawatch.gr/trending-issues/ta-prosopika-dedomena-stin-epoxi-tou-koronoiou/
- Panagopoulou - Koutnatzi, “Data Protection in pandemic times”, https://www.constitutionalism.gr/wp-content/uploads/2020/03/2020.03.28_Panagopoulou_privacycoronavirus.pdf?fbclid=IwAR2BnMVMKA4bMToCNxQ2xoTMQal3yzpXY7gov-xYnolFclRsxLewjdjVx5o
- Panagopoulou-Koutnatzi F., “Issues of constitutionality in distance school education”, Journal Adm.Law 3/2020