The COVID-19 Pandemic as a Stress Test on the Right to Protection of Personal Data

The Case of Greece

Niovi Vavoula

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

This article aims to critically examine the limitations to the fundamental right of personal data protection in Greece by exploring three instances in which the rules and practices have put the protection of personal data under significant pressure: (1) the processing of information on individuals who obtain movement permits via SMS; (2) the tracking of COVID-19 patients; and (3) the guidelines on the management of the COVID-19 crisis by the Hellenic Data Protection Authority (DPA). The article argues that the Greek response to COVID-19 has been fraught with over-restrictive measures that go beyond what is necessary and proportionate in a democratic society. In particular, the requirement of obtaining movement permits via SMS, which has been inserted through soft law, thus without parliamentary scrutiny, has relativized data protection and has lowered individuals' resistance to future surveillance practices marking everyday movement as a matter of interest to the state. In relation to contact tracing the article demonstrates that an excessive retention period of patients' data is foreseen. As for the DPA's guidelines on the processing of personal data within the framework of COVID-19 it is concluded that they have provided an unclear and overly permissible interpretation of the GDPR rules in favour of the state.

AUTHOR

Niovi Vavoula

Lecturer in Migration and Security
Queen Mary University of London

CITE THIS ARTICLE

Vavoula, N. (2021). The COVID-19 Pandemic as a Stress Test on the Right to Protection of Personal Data : The Case of Greece. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2021-018

Published in eucrim 2021, Vol. 16(2) pp 122 – 126

https://eucrim.eu

ISSN:

I. Introduction

The current COVID-19 pandemic is affecting our lives in an unprecedented manner and constitutes an intense crash test of a series of fundamental rights.[1] During the first few months of the pandemic, Greece emerged as the EU's poster child in tackling the spread of COVID-19. The Greek response entailed significant limitations on the exercise of fundamental rights, aiming in particular at the freedom of movement and assembly, economic freedom, and the exercise of freedom of religion. Concerns were voiced, particularly when the freedom of assembly and religion were in question. Although trust in political institutions may have been shaken, legal scholars have conceded that, in the context of the temporariness of the limitations and the public health interest at stake, the extreme limitations to these rights did not affect Greek democracy and the rule of law.[2]

This article aims to critically examine in depth the limitations to the fundamental right of personal data protection, especially as enshrined in Art. 8 of the Charter and in Art. 9A of the Greek Constitution.[3] Personal data protection has received relatively modest attention in comparison to other fundamental rights.[4] To this end, the article explores three instances in which the Greek rules and practice put the protection of personal data under significant pressure:

- The processing of information on individuals who obtain movement permits via SMS;
- The tracking of COVID-19 patients;
- The guidelines on the management of the COVID-19 crisis by the Hellenic Data Protection Authority (DPA).

II. Movement Permits via SMS: The Relativisation of the Right to Personal Data Protection

Throughout the pandemic, Greece has reacted swiftly by imposing restrictions on freedom of movement and other measures of social distancing. In particular, the Greek government first issued a ban on all unnecessary traffic from 23 March 2020, which lasted until 4 May 2020. Similar restrictions on movement of varying degrees and intensity were further imposed during the second and third waves of the pandemic on 1 November 2020 and continue to apply with less intensity to date. Restrictions on freedom of movement have gone hand-in-hand with efforts to monitor those on the move, as well as their personal associations if they have become infected. In a unique approach to handling the pandemic, during periods of lockdown and until 15 May 2021, anyone on the move falling within one of the six expressly listed exceptions has been required to carry an identification document and a movement permit. They could be obtained by filling out an online form, or – certainly the most popular option – by sending a mobile message to a dedicated number operated by the General Secretariat of Civil Protection (Γενική Γραμματεία Πολιτικής Προστασίας), a public law body that belongs to the Ministry of Citizen Protection. To obtain permission via SMS, the individual was required to provide his/her name and surname, residence address, and a code number corresponding to the purpose of movement. In the event of a random check by the police, individuals were required to show their movement permit; otherwise a fine could be imposed. Possible exceptions were the following: visits to pharmacy or doctor following an appointment (code number 1); supermarket/minimarket (code number 2); bank (code number 3); to help someone at home (code number 4); attending a funeral (code number 5); and physical exercise outdoors (code number 6).[5]

https://doi.org/10.30709/eucrim-2021-018

After sending the initial SMS, individuals immediately received an SMS with their movement permit. This did not apply to employees or self-employed persons who had to carry specific paperwork with them. During periods when Greece imposed restrictions on movement after a specific hour in the evening, all code numbers, except 1 and 6 (only in relation to taking out a pet), did not permit movement. Otherwise, there were no other restrictions as to how many movement permits a person may request per day, as long as the general lockdown rules were followed. This is a novelty of Greece; no other EU Member State has used this anti-COVID strategy, with the exception of Cyprus, where the rules were similar.[6] In January 2021, a cautious easing of the second lockdown was attempted and retail stores reopened, whereby consumers could only shop for two hours per day by making an appointment via SMS and showing a written confirmation of the electronic purchase, if applicable. In April 2021, stores reopened once again following the same rules, but by 15 May 2021 all requirements regarding movement permits were lifted.

Notably, although an abundant amount of ministerial decisions has been adopted in the context of the pandemic, the rules on the processing of personal data in the context of movement permits have not been laid down in law. Instead, the General Secretariat for Civil Protection merely released a "data protection policy" online, in the form of "soft law,"[7] without prior scrutiny, consultation, or transparency. The government opted for this approach, despite the possible implications it posed for the legality of data processing and the impact for individuals whose information is processed. The policy is written in Greek only, which does not enable foreigners living in the country to obtain information as to how their personal data are processed. The policy explicitly proscribes centralised storage and thus data must be deleted immediately. However, data can be anonymised for statistical use. Therefore, after an individual would receive an SMS message with a movement permit, his/her data are either deleted or anonymised.

One could argue that, because of the limited timeframe during which the measure applied and the deletion of data after issuance of the movement permit, there was no need for further formalisation of the rules. Perhaps this explains why the data protection policy in relation to the movement permits was suspended between the end of the first lockdown and the beginning of the second one and was located online only throughout the duration of the measures. This policy has raised significant concerns, however, due to the use of legal language that may not understandable and accessible to the layperson, the lack of reference that sensitive data are collected (as one of the exceptions permitting movement is a doctor's appointment), the confusion as to whether the information submitted by individuals could be submitted to third parties and, in general, as to who the recipients of the information contained in an SMS are.[8] Furthermore, Art. 13 of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) requires that persons whose personal data are processed must be informed about the purposes of the data processing and the details of the data protection officer, which are missing from the Greek policy.[9]

More worryingly, in November 2020, it was made known that an automatic decision refusing a movement permit is possible in cases of an increased number of messages coming from certain geographical areas. This automated individual decision-making significantly affects the legal position of individuals. According to Art. 22(2)(b) of the GDPR, such automated decision-making may take place *inter alia* if authorised by a Member State. However, safeguards must be laid down in such cases, at least "the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision." This has not been the case here.

Lastly, doubts as to whether SMS data are anonymised or remain personalised have also been voiced; whereas it may be useful for the administration to know how many people send an SMS invoking a particular exception as a reason for movement, it is worrying that, in the case of protest that took place in front of the American Embassy in November 2020, it became known to the authorities which reason of movement the demonstration participants had used to obtain their movement permit.[10] This is particularly worrying if one

considers the fact that, even if data are anonymised for statistical purposes, it is still unclear how it was possible to isolate that data by proximity to a specific location.

Overall, this lack of transparency and clarity in the elaboration of the data protection policy raises significant issues of unlawfulness and circumvention of the legislative process, even though criticism against the content of the data protection policy was raised during the first wave of the pandemic. By elaborating the data protection policy through soft law, the importance of the rights to the protection of personal data has been significantly downgraded, the right has essentially been relativized, and a negative precedent for normalised, unlawful processing of personal data *en masse* was thus created. Looking at the bigger picture, the use of movement permits may signify a detrimental mind shift that citizens' legitimate, everyday activities are also of interest to the state, thus increasing the social acceptance of other, more intrusive surveillance practices in the future.

III. Proportionality Concerns through the Tracking of COVID-19 Patients

The analysis above showcases how technological means have been a crucial component in efforts to contain the spread of the virus and protect public health, raising significant privacy and data protection concerns. Nowhere has the evolution of technology been more relevant in responding to COVID-19 than in so-called "exit strategies," particularly apps and other tools to trace and track the contacts of persons suspected of or diagnosed with COVID-19.[11] At the time of writing, the Greek government was still in the process of evaluating the different application models that have been proposed over the past several months, and a contact tracing app is still in the development phase.[12]

In the meantime, contact tracing takes place through traditional means of collection of patient data. Such collection has been mandated by acts of legislative content. In particular, Art. 5 of the Act of Legislative Content (Πράξη Νομοθετικού Περιεχομένου) of 14 March 2020[13] mandated the collection of personal data of potentially or actually infected persons by the Hellenic National Public Health Organisation (Εθνικός Οργανισμός Δημόσιας Υγείας, Ε.Ο.Δ.Υ), a private law entity, with the aim of sharing it with the General Secretariat for Civil Protection.[14] According to Art. 5(1) of the Act, the data shared include the person's name, gender, age, contact number, full address, information on whether he/she has been hospitalised and, if so, in which hospital, and, where relevant, the place of self-isolation. The data are pseudo-anonymised and its transmission encrypted; processing of the data is limited to the purposes of coordination between the Hellenic National Public Health Organisation and the General Secretariat for Civil Protection for the effective fight of COVID-19. In terms of the data retention period, Art. 5(2) of the Act foresees the storage of collected data for the duration of the urgent measures.

In addition, Art. 29 of the Act of Legislative Content of 30 March 2020 established a National Registry of COVID-19 patients, which regulates the processing of personal data and individual rights.[15] The Ministry of Health issued a Ministerial Decision on 14 April 2020 for the implementation of said registry. According to Decision No. 2650 of 10 April 2020 of the Ministers of Health and Digital Governance that was issued later, the data are to be kept almost indefinitely, as they can be retained for 20 years after the individual's death.[16] The lack of proportionality of this provision, which is in line with the overall restrictive nature of measures adopted by the Greek government in handling the pandemic, is striking.[17] It may be recalled that, in a series of judgments, both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) clarified that the temporal character of data retention is an important element for the proportionality test. In *S and Marper v. the United Kingdom,* the ECtHR emphasised that the indefinite retention of sensitive personal data, irrespective of their further use, may have a direct impact on the applicants'

private life interests, including their stigmatisation.[18] Furthermore, in *Digital Rights Ireland*, the CJEU opined that the retention period must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.[19]

In the present case, the long retention period is equated with indefinite retention, which, in keeping with the relevant case law, is disproportionate, particularly when the COVID-19 pandemic ends. Importantly, the retained data include information on the health of individuals, which qualifies as a special category of personal data according to Art. 9 of the GDPR. It is true that Art. 9 of the GDPR enables the processing of health data for various reasons, including reasons of public interest, but the end of the pandemic and thus the state of emergency will not justify the extensive retention period in any way. As for the contact tracing of individuals, this process is carried out by a designated centre situated in police headquarters. The process involves asking questions regarding the recent contacts of persons infected or suspected of being infected with the coronavirus. In order for public bodies (especially hospitals and clinics) to assess who constitutes a close contact and therefore must be subjected to a specific set of instructions due to the high risk of contracting COVID-19, the Hellenic National Public Health Organisation (EODY) circulated detailed guidelines specifying the relevant criteria about close familial and personal relations and associations.[20] These guidelines have also been made publicly available on the dedicated website of EODY, without elaboration in an administrative act.

IV. Hellenic Data Protection Authority to the Rescue?

A third example of how the right to the protection of personal data has taken a significant hit during the management of COVID-19 derives from the Hellenic Data Protection Authority (DPA). On 18 March 2020, the DPA issued guidelines on the processing of personal data within the framework of COVID-19, particularly as regards the applicability of the GDPR. [21] The DPA is an independent authority entrusted with various tasks in accordance with Arts. 51-59 of the GDPR, including the issuance of opinions on its own initiative or upon request on any issue related to the protection of personal data.[22] From time to time, the DPA issues soft law in the form of guidelines suggesting solutions to various problems arising from the advancement of new technologies. In this context, the DPA COVID-19 guidelines focus on the use of personal data including health data by both public and private bodies, especially in the employment field and in relation to media reporting and coverage. The DPA has provided a definition of health-related data, which includes naming or identifying a data subject as a patient, staying at home due to illness, and finding signs of illness based on clinical symptoms (cough, nasal discharge, body temperature higher than normal, etc.).[23] According to the DPA, such information falls within the realm of the GDPR only when processed wholly or partly by automated means and not when provided orally.[24] Therefore, the DPA guidelines are far from technical in nature and provide an interpretation of the GDPR in numerous respects.

In addition, the DPA states a series of applicable legal bases for the processing of personal data for COVID-19 related purposes,[25] provided that basic principles are met and that relevant substantive and procedural safeguards and conditions for lawful processing are ensured.[26] The DPA further emphasises the processing of personal data by the private sector within the framework of employment relationships. It opined that, insofar as the GDPR applies, employers are entitled to process personal data in order to protect the health of employees. As a result, the following practices are explicitly allowed: measuring the body temperature of incoming individuals; submitting questionnaires regarding the health status of employees or their relatives; requesting travel history; informing other employees of the fact that a fellow employee has been infected; exposing the employee's identity.

It is noteworthy that, in view of the "critical and unprecedented time," the DPA stressed that no policy choice could be excluded from scrutiny outright. However, the key data protection principles, as enshrined in Arts. 5

and 6 of the GDPR, are applicable. Thus, the DPA rightly noted that extensive collection of personal data resulting in profiling of employees does not comply with the principle of proportionality.[27] As has been pointed out, the guidelines are not particularly clear, and, in comparison to guidelines provided by national DPAs in other EU Member States, the Greek approach is somewhat overly permissive.[28] Another example of the ambivalent language used by the Greek DPA is a guideline according to which the transfer of information relating to the health status of individuals is prohibited "where it is creating a climate of prejudice and stigma, while it is also likely to have a preventative effect with regard to complying with the measures announced by the competent public authorities undermining eventually their effectiveness."[29] As a result, the DPA's view seems to have been influenced by the state of emergency and may have a considerable impact on the rights to respect for private life and the protection of personal data.

V. Concluding Remarks

The current COVID-19 pandemic is not only a health, economic, and social challenge but also a major challenge for national constitutions, international law, and the EU legal order. This article aimed to highlight how management of the pandemic has put the right to the protection of personal data to the test, even though Greece remains one of the few EU Member States in which a contact tracing app has not become operational yet. Although the debate about the constitutionality of harsh restrictions of rights due to the priority of public health interests and the exceptional character of the measures holds merit,[30] the present analysis has highlighted the sharp contrast between the constitutional protection of the right to data protection and the elaboration of rules that affect individuals on a daily basis outside the legislative procedure. Furthermore, despite the exceptional character of the limitations, certain (disproportionate) rules or the restrictive interpretation of rules may have wider, long-lasting implications on the protection of personal data. It remains to be seen whether the right to data protection has taken an irreversible hit.

---

1. For example, see EU Agency for Fundamental Rights, "Coronavirus pandemic in the EU – Fundamental Rights Implications: Focus on social rights" (November 2020).↩
2. G. Karavokyris, "Constitutionalism and COVID-19 in Greece: The Normality of Emergency", *Verfassungsblog* <https://verfassungsblog.de/constitutionalism-and-covid-19-in-greece-the-normality-of-emergency/> accessed 9 May 2021.↩
3. Art. 9A stipulates: "All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law."↩
4. This contribution is an updated and expanded version of E. Tsourdi and N. Vavoula, "Killing me Softly? Scrutinising the Role of Soft Law in Greece's Response to COVID-19", (2021) 21 *European Journal of Risk Regulation,* 59.↩
5. "SMS authorization for movement during lockdown back", *e-Kathimerini*, 5 November 2020 <https://www.ekathimerini.com/news/258853/sms-authorization-for-movement-during-lockdown-back/> accessed 9 May 2021.↩
6. In Cyprus, the regulatory framework of permits was different, as every individual had the possibility to receive only two permits per day.↩
7. General Secretariat for Civil Protection, "Personal Data Policy" (Section 4) <https://forma.gov.gr/docs/data-protection-policy.pdf> (in Greek), accessed 9 May 2021.↩
8. For concerns, see "Open Letter", *Homo Digitalis* <https://www.homodigitalis.gr/wp-content/uploads/2020/04/%CE%95%CF%80%CE%B9%CF%83%CF%84%CE%BF%CE%BB%CE%AE_%CE%A0%CE%BF%CE%BB%CE%A0%CE%94_13033_HD_30.03.2020.pdf> (in Greek), accessed 9 May 2021.↩
9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* L 119, 4.5.2016, 1.↩
10. "Τα προσωπικά μας δεδομένα απροστάτευτα στο 13033", *OSARENA* <https://osarena.net/ta-prosopika-mas-dedomena-aprostateyta-13033/> accessed 9 May 2021.↩
11. For an analysis on tracking apps in the EU, see H. van Kolfschooten and A. de Ruijter, "COVID-19 and Privacy in the European Union: A Legal Perspective on Contact Tracing" (2020) 41(3) *Contemporary Security Policy,* 478. For a comparative study, see EU Agency for Fundamental Rights, "Coronavirus Pandemic in the EU – Fundamental Rights Implications: With a Focus on Contact-Tracing Apps" (April 2020).↩
12. See European Commission, "Mobile contact tracing apps in EU Member States" <https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en> accessed 9 May 2021.↩
13. The Greek Constitution does not provide for a state of emergency. Instead, it establishes the notion of an "act of legislative content" (Ρράξη νομοθετικού περιεχομένου), on the basis of which the Greek government has adopted general measures in response to the COVID-19 pandemic.

For concerns on this approach, see E Fasia, "Effective but Constitutionally Dubious: The Constitutionality of Greece's Response to the Pandemic", *Verfassungsblog* <verfassungsblog.de/effective-but-constitutionally-dubious/> accessed 9 May 2021.↩

14. Act of Legislative Content, "Emergency measures in response to the need to limit the dispersion of the coronavirus COVID-19" OG A' 64/14-3-2020 <www.dsanet.gr/Epikairothta/Nomothesia/PNP_14-3-2020.htm> accessed 9 May 2021.↩
15. Act of Legislative Content, "Measures to tackle coronavirus COVID-19 pandemic and other urgent provisions" OG A '75/30-3-2020 <www.dsanet.gr/Epikairothta/Nomothesia/pnp30032020.htm> accessed 9 May 2021.↩
16. Joint Ministerial Decision 2650/10.04.2020 "Settlement of more specific technical issues for the operation of the National Patient Register for COVID-19, in accordance with the provisions of article twenty-nine of the Act of 30.3.2020 of the Legislative Content Act (PNP) 'Measures to deal with the pandemic of the corona COVID-19 and other urgent provisions' (A΄ 75) and 83 of Law 4600/2019 (A΄ 43)" OG B 1298/10.4.2020 <https://www.e-nomothesia.gr/kat-ygeia/astheneies/koine-upourgike-apophase-2650-2020.html> (in Greek), accessed 9 May 2021.↩
17. For criticism, see "COVID-19 και Ψηφιακά Δικαιώματα στην Ελλάδα" (COVID-19 and Digital Rights in Greece), *Homo Digitalis* <https://www.homodigitalis.gr/wp-content/uploads/2020/04/HomoDigitalis_Report_COVID19_and_Digital_Rights_in_Greece_22.04.2020_Final.pdf> accessed 9 May 2021.↩
18. ECtHR, 4 December 2008, *S and Marper v UK*, Application nos. 30562/04 and 30566/04, paras 107-121.↩
19. ECJ, 8 April 2014, joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (C-293/12) and *Kärntner Landesregierung and Others* (C-594/12) para 64.↩
20. "Handling COVID-19 patients' contacts" *EODY* <https://eody.gov.gr/wp-content/uploads/2020/03/covid-19-diaxeirisi-epafon.pdf> (in Greek), accessed 9 May 2021.↩
21. Greek Data Protection Authority, "Guidelines on Processing of Personal Data in the Context of the Management of COVID-19" (18 March 2020) <https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/NEWS/FILES/HELLENIC%20DPA_GUIDELINES_PROCESSING%20OF%20PERSONAL%20DATA_COVID-19.PDF> (in English), accessed 9 May 2021.↩
22. Art 57(3)(b) of the GDPR.↩
23. DPA, COVID-19 Guidelines, *op. cit.* (n. 21), para 1.↩
24. DPA, COVID-19 Guidelines, *op. cit.* (n. 21), para 2.↩
25. Specifically, Arts. 6(1)(c), 6(1)(d), 6(1)(e) as well as 9(2)(b), 9(2)(e), 9(2)(h) and 9(2)(i) of the GDPR.↩
26. DPA, COVID-19 Guidelines, *op. cit.* (n. 21), para 4.↩
27. DPA, COVID-19 Guidelines, *op. cit.* (n. 21), para 6.↩
28. Only the Greek and Belgian DPAs have adopted such an approach. For a comparative overview, see E. Pappa, "Κορωνοϊός, Θερμομέτρηση και Προστασία Προσωπικών Δεδομένων" (Coronavirus, Temperature Checks and Protection of Personal Data), *Lawspot* <https://www.lawspot.gr/nomika-blogs/evelina_pappa/koronoios-thermometrisi-kai-prostasia-prosopikon-dedomenon> (in Greek) accessed 9 May 2021.↩
29. DPA, COVID-19 Guidelines, *op. cit.* (n. 21), para 9.↩
30. E. Venizelos, "Pandemic, Fundamental Rights and Democracy – The Greek Example" <https://evenizelos.gr/other-languages/375-articles-eng/6235-ev-venizelos-pandemic-fundamental-rights-and-democracy-the-greek-example.html> accessed 9 May 2021.↩

Co-funded by
the European Union

https://doi.org/10.30709/eucrim-2021-018