HELLENIC DATA
PROTECTION AUTHORITY

Summary of Annual Report 2020

www.dpa.gr

CONTENTS

HELLENIC DATA PROTECTION AUTHORITY

FOREWORD BY THE PRESIDENT

2020 was a year of unpredictable events. The COVID-19 pandemic gave rise to emergency circumstances that had a profound impact on our everyday life. During this global crisis of unprecedented scale, where the main challenge has justifiably been to protect public health, very often personal data and privacy-related issues have arosen. From the first phase restrictive measures against coronavirus were put in place, their lawfulness, in terms of personal data protection, was on the agenda of the European Parliament and the European Commission, the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS) and national data protection supervisory authorities. Many of these authorities, among which the Hellenic Data Protection Authority, issued announcements or guidelines. It should be noted that in 2020 the Hellenic DPA issued, among others, useful guidelines (1/2020) and a decision (5/2020) on the processing of personal data in the context of tackling COVID-19, guidelines on safety measures taken in the context of telework (2/2020) and an opinion on synchronous distance learning in primary and secondary education school units (4/2020).

The starting point for all announcements and guidelines was the fact that the GDPR and other relevant legislation enable the processing of health data in the context of combating the pandemic, in compliance with the safeguards and rights of data subjects. Independent supervisory authorities were tasked with the challenging work of trying to strike a balance between protecting privacy and the right to informational self-determination, and serving the general social interest. Striking the right balance is a particularly challenging task, as each time there are specific real-life circumstances in terms of conflicting individual and social rights.

The Hellenic DPA responded well to the challenges raised by the pandemic, adjusting almost immediately and switching to telework, securing its operational continuity and

ensuring full performance of its tasks. I would like to mention that, in the context of its responsibilities, the Authority issued significant opinions and decisions, the majority of which involved electronic communications, the public administration and work relationships. At the same time, the Authority submitted comments on the legislative initiatives of the Ministry of Digital Governance in connection with the provisions on the "Personal Number" included in the draft law entitled "Digital Governance Code", as well as in designing a COVID-19 tracing application. In addition, the Authority contributed to the procedures involving the drafting of the new Regulation on the protection of personal data in electronic communications (e-Privacy Regulation) and it forwarded its views to the Directorate of European Affairs and Bilateral Issues of the Hellenic Parliament in connection with the draft legislation on combating sexual exploitation of minors. Furthermore, the Authority identified a lack of compliance by information society service providers with the requirements set forth in the legislation on the processing of data in electronic communications and the GDPR in relation to the management of cookies and related technologies and issued specific recommendations (1/2020); it also issued recommendation 2/2020which included templates on fulfilling the right to be informed when processing data through video-surveillance systems.

At the same time, the Authority met its standard European and international obligations and was actively involved in working groups and committees operating under the European personal data protection legislation. Since November 2020, and aiming to raise awareness among controllers and processors about the personal data protection legislation, the Authority launched a project entitled "Facilitating compliance with the GDPR for Small and Medium-Sized Enterprises and promoting data protection by design on ICT products and services ("byDesign")". The project is being carried out for two years in collaboration with the University of Piraeus and the Greek IT company 'ABOVO', and is co-funded by the European Commission.The year 2020 also saw the beginning of the ambitious project of creating the Authority's new web portal. The main objective was to improve the information and awareness-raising content available to citizens regarding their rights, as well as to various bodies regarding their obligations, so that the work of the Authority can be as effective as possible in strengthening personal data protection in Greece.

The 2020 Annual Report of the Authority is a reflection of all the activities undertaken in the course of this unprecedented year during which human rights were put to the test. At the same time, it demonstrates the ability of the Authority's staff to adjust promptly, work diligently and commit to performing the critical mission it has been entrusted with by the State.

In an age of great uncertainty, where new challenges are constantly emerging, among other things, due to a digital transformation process that is accelerating, we must remain committed to safeguarding individual rights in practice, a task that - to a large extent - is intertwined with personal data protection.

Konstantinos Menoudakos

President of the Hellenic Data Protection Authority

HELLENIC DATA PROTECTION AUTHORITY

OVERVIEW

ROLE, MISSION AND RESPONSIBILITIES

The Hellenic Data Protection Authority is a constitutionally consolidated independent public Authority (Article 9A of the Constitution) established by Law 2472/1997 transposing European Directive 95/46/EC into Greek law on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Authority is assisted by a Secretariat that operates at a Directorate level and has its own budget.

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation - GDPR), which entered into force on 25 May 2018 in all EU countries, repealed Directive 95/45/EC. As of August 29th, 2019, Law 4624/2019 ("Hellenic Data Protection Authority, measures for implementing 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 transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions") has been in force. Articles 9 - 20 of the above law are dedicated to the Hellenic Data Protection Authority (supervisory authority). As for Law 2472/1997, it has been repealed, except for certain provisions explicitly mentioned in Article 84 of Law 4624/2019. Law 4624/2019 also transposed Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Furthermore, as regards the protection of personal data in electronic communications, the Authority applies Law 3471/2006 transposing European

Directive 2002/58/EC into national law. The Authority is responsible for monitoring the application of the provisions of the GDPR (Article 51(1), Recital 123), of Law 4624/2019 and other regulations relating to the protection of natural persons with regard to the processing of their personal data (Article 9 of Law 4624/2019). It also contributes to the consistent application of the GDPR throughout the Union and, to this end, it cooperates with the supervisory authorities of EU Member States and the European Commission (Article 51(2), Recital 123 of the GDPR; Article 10 of Law 4624/2019).

The Authority represents Greece to the European Data Protection Board (EDPB) and other committees or bodies tasked with data protection, and it cooperates with respective third-country authorities and international bodies (Article 50 GDPR, Article 10 of Law 4624/2019). The Authority is competent for the performance of its tasks (Article 57 of the GDPR and Article 13 of Law 4624/2019) and the exercise of the powers conferred on it (Article 58 of the GDPR and Article 15 of Law 4624/2019) on its territory (Article 55(1), Recitals 122, 129 of the GDPR; Article 9 of Law 4624/2019) acting with complete independence (Article 52, Recitals 117-118, 121 of the GDPR; Article 11 of Law 4624/2019).

HUMAN RESOURCES AND OPERATIONAL ISSUES

The Authority, in accordance with Article 20(1) of its founding Law 2472/1997 and presidential decree 207/1998 on the "organisation of the Secretariat of the Data Protection Authority and the establishment of permanent posts" still in force under Article 18(3) of Law 4624/2019, is assisted by a Secretariat that operates at a Directorate level and consists of four (4) departments: 1) the Auditors' Department, 2) the Communications Department, 3) the Department of Administrative Affairs, and 4) the Department of Finance.

For the financial year 2020, the Authority's budget amounted to EUR 3,101,000. As for 2021, the budget that has already been approved amounts to EUR 2,811,000.

In 2020, the Authority completed the upgrading of its Integrated Information System and web portal, incorporating electronic services related to the submission and monitoring of the progress of complaints under examination, requests made by citizens and bodies, data breach incident notifications submitted and requests for inclusion in the registry of Article 13 and its conditional provision to the persons concerned. The effort made by the Authority to adapt to the new framework of responsibilities, tasks and powers deriving from the GDPR on an organisational and operational level is ongoing. The additional accreditation requirements for certification bodies, as well as the accreditation requirements for codes of conduct monitoring bodies were finalised, following relevant opinions issued by the EDPB on the Authority's respective draft decisions.

In 2020, the Authority's effort to find funds with a view to upgrading its digital infrastructure was successful, thanks to the inclusion of the project in the NSRF Operational Programme "Public Sector Reform" of the National Strategic Framework

(NSRF) and the utilisation of European Union financial instruments. Furthermore, preparatory work was carried out, such as identifying operational needs and drafting the datasheet and tender dossier. This upgrade seeks to introduce new, and to a larger extent, automated electronic services, such as data breach incident management, safety and data protection (self-)assessment, and audit management, and to create information content in order to raise awareness among children on issues of data protection. Additionally, in 2020 the Authority submitted a project proposal for funding by the European Commission, which was approved, and the implementation of the project was launched in that year. With this project called "byDesign", the Authority seeks, on the one hand, to support small and medium-sized enterprises in their effort to comply with the GDPR by drafting templates and providing guidance on their fundamental obligations, such as providing information, managing consent, drafting records of processing activities, drawing up terms of use for online services, etc., and, on the other, to create training material and hold relevant seminars on "data protection by design and by default" for ICT specialists, such as analysts, IT application designers and programmers, sales managers and students who are experienced in developing relevant applications.

The measures taken to tackle the pandemic undoubtedly gave rise to some difficulties in connection with the Authority's daily operations, but the Authority managed to adapt swiftly to telework and remote meetings, given that significant steps had already been taken to prepare its technical infrastructure. The Authority issued guidelines on the processing of data in the context of the management of COVID-19, and on safety measures taken in the context of telework, an opinion on synchronous distance learning in primary and secondary education school units, as well as guidance for its staff on secure remote access to its information system, on communication and collaborations. It also suspended public hearings and modified its Rules of Procedure, in order to hold remote hearings.

As it has been pointed out in the past, understaffing combined with a broad range of responsibilities resulting from the European and national legislation, together with a high number of incoming cases, remains an essential hampering factor in the Authority's efforts to fully carry out its mission. The negative impact has been more profound in implementing its proactive actions, such as regular audits, and in carrying out information and awareness-raising activities for data subjects, controllers and processors.

Another significant aspect is the amount of work the Authority is called on to handle. As it has already been mentioned in previous reports, the entry into force of the GDPR has brought about changes in the mixture of tasks the Authority should perform in the context of its mission. Examining complaints remains the most demanding, effort-intensive task for the Authority, while queries are only limited to requests for information regarding the exercise of data subjects' rights, requests for

opinions or comments on preliminary questions, or for filling in questionnaires usually submitted by European authorities. On the other hand, although submitting processing notifications and granting permits are not applicable any more, data breach incident notifications provided for by law require more demanding labour-intensive processes.

In terms of the appropriations available for 2020, there was indeed an increase by about 9% compared to the previous year, but this rise involved the major category "Employee benefits", nevertheless, without an increase in the number of staff. As a result, these appropriations could not be used, since they could not be re-allocated to meet other Authority needs. That said, the appropriations available for operating costs showed no positive change; on the contrary, there was a drop by about 8%, despite constant requests for a significant rise.

As mentioned in every annual report, the Authority strives to perform its work in the most effective way and contribute to shaping an environment conducive to data protection in our country. To fulfil its mission, adequate staffing and availability of all necessary financial and technical means and facilities are of the utmost importance for the Authority. It is also looking forward to the State's response, in compliance with the relevant provisions of the GDPR (paragraph 4 of the Article 52).

KEY STATISTICS

In 2020, the number of incoming cases of complaints amounted to 973, down by about 1% compared to 2019 (983), while 700 cases of complaints were resolved, showing an increase of about 15% from the previous year (608). The number of data breach incidents notified to the Authority under the GDPR amounted to 130, down by about 2% compared to the previous year (132 in 2019), while 59 data breach notifications were submitted by electronic communications service providers under Law 3471/2006, showing a significant increase – more than double (22 in 2019). The examination of 51 cases was completed with the adoption of a decision by the Plenary or the Chamber. Furthermore, in 2020 the Authority issued five (5) opinions.

As was the case with the 2019 Report, the statistics differ to some extent from the ones included in previous annual reports, reflecting the differentiated responsibilities of the Authority (deriving mainly from the GDPR). Moreover, there is now provision for cooperation with counterpart supervisory authorities of Member States on cross-border cases ('one-stop-shop mechanism'), and, within the framework of the European Data Protection Board (consistency mechanism), prior consultation with the Authority for cases of processing of high residual risk following an impact assessment on data protection, the examination and approval by the Authority of codes of conduct and certification requirements of relevant models, etc. In addition to the above, there is also provision for giving information to data subjects upon request concerning the exercise of their rights, either orally or in writing.

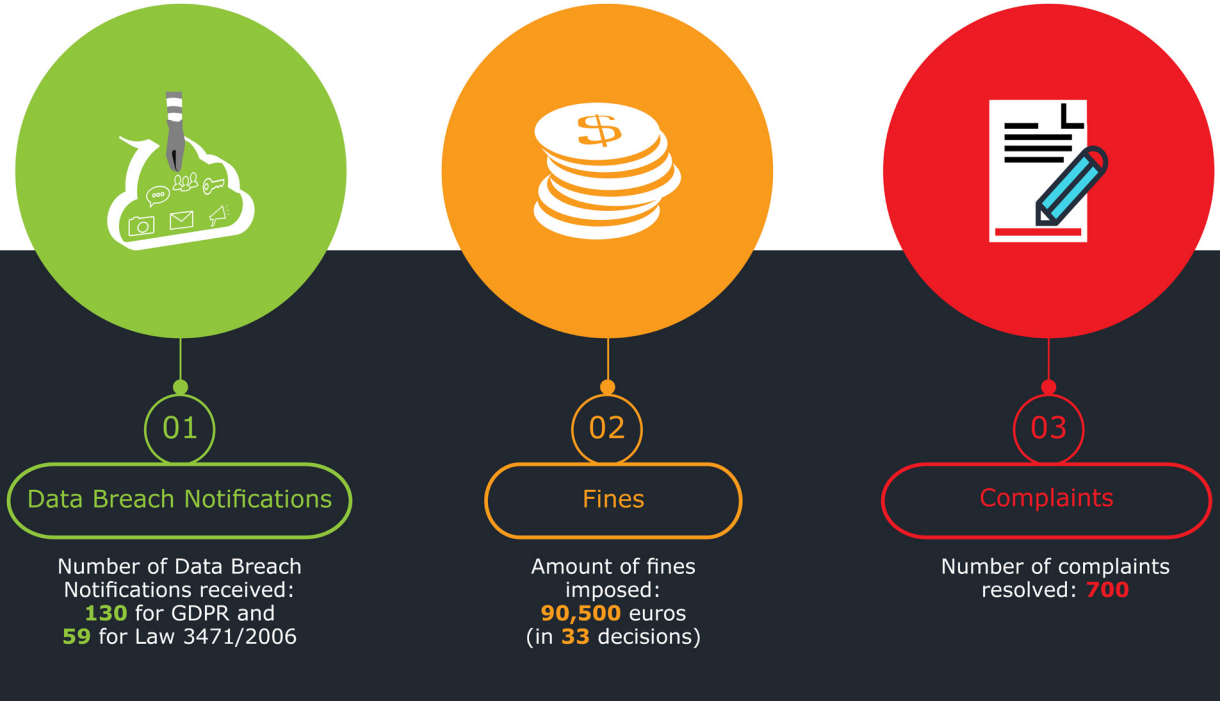
In early 2020, the Authority issued final recommendations and confirmed compliance with them in the context of its ex officio audit action - that had begun in 2018 - on 65 data controllers operating online in the fields of financial services, insurance, e-commerce, ticket services and public sector services. Moreover, in 2020, the Authority requested information and clarifications from competent Ministries and

services with regard to commissioning an epidemiological data analysis and predicting the course of the pandemic to Palantir Technologies, and from the Ministry of Citizen Protection with regard to the installation and operation of a portable surveillance system by the Hellenic Police. Additionally, the Authority examined a data breach incident at COSMOTE S.A. and requested information and clarifications from the banks involved in replacing the credit and debit cards of their customers due to leakage of relevant data, as well as with regard to the investigation of a breach incident by the operator of an electronic transaction platform that was allegedly the source of data leakage.

With regard to the above mentioned data breach incident notifications provided for in the GDPR, 119 out of 130 were submitted by companies with a main or local establishment in Greece, and the other 11 by a controller with a main establishment in another Member State (2) or without an establishment within the European Union (9).

Thirty three (33) of the Authority's decisions impose penalties on controllers. In two (2) cases the sanction of reprimand – warning was imposed following the lodging of a complaint and a hearing procedure, and in 31 cases a fine was imposed ranging from EUR 1,000 to EUR 8,000. It is noted that in 3 of those 31 decisions, an order of compliance was also imposed in addition to the financial penalty, in accordance with the provisions of the GDPR. In total, fines of EUR 90,500 were imposed.

Key statistics 2020



HELLENIC DATA PROTECTION AUTHORITY

ENFORCEMENT

SELECTION OF DECISIONS ON COMPLAINTS

Decision 2/2020

Fine imposed to DEI S.A. (Public Power Corporation) for failure to fulfil a data subject's right of access

Following a complaint filed to the Authority according to which DEI S.A. had failed to fulfil a data subject's right to access information about her, the Authority imposed an administrative fine of EUR 5,000 to DEI S.A..

DEI S.A., in its capacity as the controller, after a period of one month of receiving the request, didn't respond to the complainant with regard to its failure to satisfy her request promptly. Hence, taking into account that the same breach had occurred before, as becomes evident in its Decision 15/2019, the Authority was unanimous in the view that, in this case, based on the circumstances identified, an effective, proportionate and dissuasive administrative fine should be imposed as a punishment for this unlawful conduct.

Decision 5/2020

Processing of personal data in the context of tackling COVID-19

The Authority issued Guidelines on the processing of personal data in the context of tackling COVID-19, which set out the Authority's responsibilities under the GDPR 2016/679 and Law 4624/2019, and outline the legal bases applicable for processing by the competent public authorities and private bodies in their capacity as controllers. In particular, the Authority, in relation to the processing of personal data by employers for the purpose of containing the spread of COVID-19, points out specific issues of lawful processing of employees' personal data. The Authority has also drawn attention to the rules for the processing of personal data of family members or close friends who

have died of COVID-19, as well as the rules for the processing of personal data by the data subjects coronavirus sufferers themselves. Finally, the Authority is addressing the issue of the processing of personal data for journalistic purposes.

In view of the above, the Authority points out the following: 1) 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, such as the right to life and health. 2) The controller, both in the public and private sector, in taking the necessary measures to prevent the spread of COVID-19, may process personal data in accordance with Articles 5 and 6 of the GDPR, without it being possible to exclude from the outset that any processing operation is prohibited, especially during these critical and unprecedented times. 3) The legislation on the protection of personal data, in the context of measures to protect public health in general and the health of data subjects at work places, provides, on the one hand, the appropriate legal bases for the processing of personal data, and enables, on the other, national legislators to specify processing operations that are necessary for reasons of public interest, including the area of public health, and in accordance with the provisions of the GDPR.

Decision 18/2020

Imposition of a fine to New York College S.A. for unlawful processing and failure to comply with the obligation of accountability as a follow-up to a complaint filed for targeted phone communication

The Authority, in its Decision 18/2020, examined a complaint filed for a targeted phone call during which New York College proposed to the complainant to participate in a seminar for unemployed people subsidised by the Manpower Employment Organisation (OAED). The controller failed to provide evidence explaining how they had processed the complainant's personal data, that is, they failed to establish the lawfulness of processing, in breach of the principle of accountability. In addition, they failed to provide evidence on the general policy it had followed in this processing. The Authority imposed a fine of EUR 5,000 for unlawful processing and failure to comply with the principle of accountability. It also ordered that the processing operations involving the personal data of the persons concerned regarding their participation in subsidised training programmes be made consistent with the provisions of the GDPR, and that all necessary internal compliance and accountability measures be taken pursuant to the principles of Article 5(1)-(2) in conjunction with Article 6(1) of the GDPR.

Decision 20/2020

Complaint filed by a data subject against the 401 General Military Hospital of Athens (401 GSNA) for unlawful processing of personal data when entering the Hospital

The claim raised by the 401 GSNA according to which the Authority lacks

jurisdiction to handle a complaint filed against the Hospital on grounds of national security pursuant to Article 10 of Law 4624/2019 was rejected by the Authority as unfounded. The complaint filed by the data subject against the 401 GSNA was rejected by the Authority as unfounded. The Authority considered that the processing of personal data when entering the hospital is lawful. The Authority judged that the appointment of a DPO at the Hellenic National Defence General Staff cannot guarantee the effective performance of the DPO's duties for the unit subject to it, in this case the 401 GSNA, and calls on the 401 GSNA to arrange for the appointment of a DPO in a way that meets the requirements set forth in the data protection legislation.

Decision 30/2020

Imposition of a fine for unlawful processing of data through a video-surveillance system installed in a private residence, and order issued to make the processing activities consistent with the provisions of the GDPR and Guideline 1/2011

The Authority, in its Decision 30/2020, ordered the person complained against to restore the proper application of the provisions set forth in Article 5 of the GDPR and make the processing operations taking place through the installed video-surveillance system consistent with the provisions of the GDPR and Guideline 1/2011; it also imposed a fine.

The reason is that the person complained against failed to establish the lawfulness of installing and operating the video-surveillance system in accordance with the principle of accountability, and to provide the Authority with relevant documentation regarding its lawful operation. According to the information included in the case file and the fact that the person complained against admitted to their act, it became evident that the person in question installed and operated the system in an unlawful manner, as he switched on the camera installed on the roof of his residence and turned it in a way that allowed it to take images of the complainants, and every individual in their property, and record their activities.

Decision 52/2020

Sending political communication by postal mail in braille

The Authority considered that sending a brochure to the complainant by postal mail in braille for the purpose of political communication by a political party was in violation of Article 9 of the GDPR, and imposed on the latter, in its capacity as the controller, an administrative fine. The Authority found also that the data subject's right to be informed was fulfilled by the political party after the deadline had expired, in violation of Article 14(3) of the GDPR, and imposed on the latter, in its capacity as the controller, an administrative fine.

Fines imposed for sending unsolicited communication

The Authority, in its Decisions 10, 11, 12, 13, 17, 19, 28, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, and 58, examined complaints filed for unsolicited political communication sent by electronic means, that is, by short SMS text messages and electronic mails (e-mails), and imposed administrative fines ranging from EUR 1,000 to EUR 4,000. The following cases were taken into account, among other things, as the main aggravating factors for the incidents in question: whether the recipient's required prior consent had been ensured or if no such prior contact/communication had occurred, the number of messages sent, whether the controller enabled recipients via the messages in question to exercise the right to object in an accessible and clear way, and whether the controller cooperated with the Authority by providing the clarifications requested.

Moreover, the Authority examined complaints filed for unsolicited electronic communication with political content by phone, and imposed, respectively, in its Decision 24, an administrative fine of EUR 3,000, and in its Decision 56 and administrative fine of EUR 1,000. The Authority also examined a complaint filed in connection with ballot papers sent by postal mail and failure to fulfil the right of access, and, in its Decision 29, imposed an administrative fine of EUR 3,000 to the controller for failing to respond to the right of access that was exercised.

Additionally, the Authority, in its Decision 14, imposed the sanction of warning for sending unsolicited political communication by e-mail, and, in its Decision 57, it found –after examining a complaint filed for unsolicited political communication sent via short SMS text messages– that there is no reason to impose any administrative sanction.

Finally, the Authority issued Decision 52 in connection with a complaint filed for sending unsolicited political communication by postal mail in Braille.

INVESTIGATIONS - AUDITS

At the beginning of 2020, the Authority completed its ex officio investigation-audit action that had begun in 2018 in relation to the examination of websites operated by 65 data controllers, aiming, in particular, to investigate the degree of compliance with the General Data Protection Regulation and specific legislation on electronic communications. The Authority made recommendations to all 65 audited bodies and confirmed that its recommendations had been implemented. Against the backdrop of the conclusions drawn from its audit action, the Authority issued recommendations on the compliance of data controllers with specific legislation on electronic communications, and called on controllers to comply with them within two months. The recommendations made by the Authority revolved around three basic areas: a) the obligation to obtain consent, and potential exemptions to that obligation; b) how information is provided and what it includes; and c) how consent is obtained.

In its reply to a query posed by an online media outlet shortly before the expiry

of the two-month deadline, the Authority pointed out that it does take into account the challenges arisen due to the unusual circumstances in relation to the pandemic. These challenges are taken into consideration together with the facts relating to each specific case, in particular the evidence showing whether the controller in question has taken reasonable steps to comply or, on the contrary, if they have unjustifiably failed to take action. In this context, the mere expiration of the deadline that was set does not warrant the imposition of sanctions. It should be noted that in our country Article 5(3) of Law 3471/2006 had already defined the meaning of consent in a way similar to the one set forth in Article 7 of the GDPR. As a result, the provisions in question relating to the use of cookies and similar techniques have remained virtually unaffected since 2012.

In fact, it has been stressed that at this time in particular, when citizens have as their only viable option to use electronic services even for their most basic activities generating considerably more digital traces than ever before, complying with the relevant legislation applies to all. To this end, the guidance provided by the Authority becomes ever more important. The Authority has found that the situation in Greek webpages regarding the use of cookies and related technologies has changed considerably, and this is a positive aspect, since several controllers have already either adapted fully or have achieved a satisfactory degree of compliance by taking relevant steps.

Based on communications from Palantir Technologies and media coverage, the Authority, in the context of its responsibilities under Article 58 of the GDPR, and Articles 13 and 15 of Law 4624/2019, issued document under ref. no. Gen/Outc/8717/18-12-2020 calling on the Ministry of Digital Governance and the Ministry of Health to provide clarifications and immediate information as to whether Palantir Technologies has indeed been commissioned to provide services involving the processing of personal data, and, if so, what the exact purpose of this processing is and what types of data are being processed. The Authority also requested that the relevant contract commissioning the processing be submitted, including any annexes, together with the data protection impact assessment, if any. The investigation of the case was pursued in 2021 with the involvement of other bodies (EODY [National Public Health Organisation], General Secretariat for Civil Protection).

The Authority became aware, both from media coverage and the official website of the Hellenic Police, that on 6/12/2020, as part of the Attica General Police Directorate operational planning, a portable surveillance system was installed and operated in areas of the Athens city centre following a decision made by the Hellenic Police Headquarters, in accordance with the provisions of presidential decree 75/2020. The Authority contacted ex officio the Ministry of Citizen Protection/Hellenic Police Headquarters on issues related to compliance with the current legal framework.

In particular, the Authority requested information on whether a data protection impact assessment had been carried out in this specific case of a portable surveillance system and, if so, it requested that the DPIA be submitted. Furthermore, it also requested a copy of the decision made by the Hellenic Police Headquarters, and to receive more detailed information about how data subjects are informed, especially as far as their rights are concerned under the applicable provisions of Regulation (EU) 2016/679 and Law 4624/2019 (as specified further, in this case, in Article 10 of p.d. 75/2020). Finally, the Authority also requested information about the advisory role of the Hellenic Police Data Protection Officer. The Authority is pursuing the investigation of this case.

On 9/9/2020, COSMOTE notified the Authority of a personal data breach incident involving leakage of external communication data and other data affecting all company subscribers, in accordance with Law 3471/2006. Immediately after the original notification, staff members of the Authority contacted the provider's competent staff members in order to investigate the incident and assess its impact on subscribers. On 8/10/2020, COSMOTE submitted additional evidence to the Authority resulting from the process of examining the incident. The Authority, in the context of its responsibilities, pursued the investigation of the incident both in the course of 2020 and in 2021.

Based on media coverage, the Authority became aware that some banks had gradually been replacing thousands of their customers' credit and debit cards in an effort to eliminate the effects from a leakage of the above information that occurred at a travel agency. Therefore, the Authority contacted the banks (document under ref. no. Gen/Outc/322/15-01-2020) to request information, among other things, about the travel agency involved in this incident. Based on the replies given by the banks, an electronic transaction platform operated by a Greek company was identified as the common location where all cards had been used. The Authority posed a number of specific questions to the company in connection with the incident, and the company provided clarifications. The investigation of the incident was already under way through an outsourced contractor. On the basis of the evidence available to this day, it has not been possible to identify the source of the incident.

ADVISORY – CONSULTATIVE WORK

Action related to the COVID-19 pandemic

Guidelines 1 on the processing of personal data in the context of tackling COVID-19

The Authority specified the legal possibilities for processing by the competent public authorities and private bodies, as controllers, under the General Data Protection Regulation 2016/679, Law 4624/2019 and other relevant legislation, under the circumstances of the need to tackle the spread of the virus. Among others, with regard to the processing of personal data by employers for the purpose of restricting the spread of COVID-19, the Authority refers to specific issues of lawful processing of employees' personal data. In particular, according to the guidelines, the processing of personal health data in the context of anti-coronavirus measures taken by the competent public authorities as necessary for reasons of public interest in the field of public health, including protection against serious cross-border threats to health, is in accordance with the provisions of the GDPR.

As far as the private sector is concerned, employers are entitled to process data for the protection of the health of workers and themselves, in compliance with the principles of Article 5 GDPR, in accordance with the legal bases of the provisions of Articles 6(1), in particular, subparagraphs (c), (d) and (e), 9(2), in particular, subparagraphs (b), (e) and (i) GDPR and always under the instructions of the competent authorities for the implementation of the measures taken with the acts of legislative content in so far as they constitute the processing of personal data. Furthermore, the Authority noted the rules on the processing of personal data of relatives or relatives of COVID-19 deceased persons, as well as the rules for the processing of personal data by the coronavirus subjects themselves. Finally, the Authority dealt with the issue of the processing of personal data for journalistic purposes, in which it should primarily be

assessed the need to disclose identification data of the subject (e.g. name, photograph and other determinants), especially since the competent authorities (National Public Health Organisation and General Secretariat of Civil Protection process personal data of citizens of epidemiological association, without identifying personal data or following pseudonymisation and taking the necessary technical and organisational security measures.

Guidelines 2 on safety measures taken in the context of telework

Due to the fact that many organisations and businesses urge and/or force their staff to work remotely (telework) as part of restriction measures taken to prevent the spread of COVID-19, the Authority, aiming to raise awareness among controllers, processors, employees and the general public about the risks relating to the protection of personal data and, at the same time, the relevant obligations deriving from the General Data Protection Regulation 2016/679 and Law 4624/2019, issued guidelines on safety measures taken in the context of telework. These measures mainly involve accessing the network, using e-mail/message exchange applications, using terminal devices/storage media and holding video-conferences.

Opinions

The Authority issued opinion 1/2020 that includes introductory remarks and general comments on the provisions of Law 4624/2019 laying down measures for implementing the General Data Protection Regulation (EU) 2016/679 and transposing Directive (EU) 2016/680 into national law. The Authority decided to examine, on the one hand, the implementation of the GDPR through national legislative measures, restricting itself for the time being to more general comments on some provisions for which there are doubts in terms of their compatibility with the GDPR or need interpretation, and, on the other, the transposition of Directive 2016/680, focusing on the Directive's flagship provisions and reserving the right to examine any more specific issues that may arise in the context of its responsibilities under the GDPR and Law 4624/2019. It is noted that no provision of Law 4624/2019 will be implemented by the Authority in exercising its responsibilities if deemed to be in conflict with the GDPR or lacking any basis on "opening - specialisation clauses".

The Authority also issued opinion 2/2020 upon a request from the ASEP (Supreme Council for Civil Personnel Selection) with regard to a residual risk when posting rating tables on its website (www.asep.gr) listing the persons to be appointed, which tables might contain special categories of data. The Authority considered that such posting fulfils the constitutional right to transparency. However, for the posting to comply with data protection rules, it must be carried out on the following conditions: Fellow candidates have access to all information (both their own and that of other candidates) contained in the above mentioned tables by using a unique individual access account. The general public is informed of the results included in the mixed tables after redaction of special categories of data included in the fields of the respective columns and replacement of their headings without including an explanation regarding

the nature of the category in question. The public is also informed of the results included in the special category tables without including identifiers but by providing the remaining information. The measures proposed above apply mutatis mutandis to the posting of the tables at issue by all recruitment public bodies either in their physical establishment or on their website.

Upon a request from the Ministry of Citizen Protection for an opinion to be issued by the Authority on the draft Presidential Decree on the "use of surveillance systems able to obtain or record sound or image in public areas", the Authority, in its opinion no. 3/2020, after analysing the Greek and European legal frameworks on the protection of personal data, in particular taking into account the case law of the European Court of Human Rights and the European Court of Justice, makes a number of remarks and, among other things, points out the need to amend certain provisions to make them compatible with the national and European law in order to ensure and protect the fundamental rights of data subjects.

The Authority, following reports from OIELE (Hellenic Federation of Private School Teachers) and DOE (Hellenic Primary School Teachers' Federation) and a complaint filed by a parent, examined the lawfulness of the processing of personal data in the course of synchronous distance learning in primary and secondary education school units, which was implemented under Ministerial Decision no. 57233/Y1. Prior to the Ministerial Decision in question, the Ministry of Education and Religious Affairs carried out a data protection impact assessment (DPIA), as provided for in Article 63 of Law 4686/2020 and Article 35 of the GDPR. The Authority, with opinion no. 4/2020, held that the process of synchronous distance learning was lawful; it found, though, that the DPIA that had been carried out failed to take full account of a number of factors and risks in relation to the rights and freedoms of data subjects. Recognising the necessity to provide synchronous distance learning, especially in a pandemic setting, the Authority issued an opinion for the Ministry to ensure that the shortcomings identified above can be addressed, and it called on it to take, within a binding period of three months, the necessary steps to modify and complement the DPIA, and the measures taken thereunder.

Finally, the Authority, upon a request from the Ministry of Defence, issued opinion no. 5/2020 on a draft law concerning the processing of personal data by Armed Forces missions abroad with the main purpose of collecting and further processing personal data to recognise – disclose and identify persons posing a threat for national and coalition forces, and in general for the country's defence and security. The Authority, in this opinion, found that, although the more specific subject-matter of the draft law, insofar as it relates to national security, clearly falls outside the scope of both the GDPR and Directive 2016/680, it is nevertheless indicative of the will of the national legislators to purposefully include the intended processing into the legal status of the

GDPR and the supervisory powers of the Hellenic DPA. The Authority, therefore, has a favourable opinion regarding this choice made by the legislator. Besides, in no way does the processing of personal data carried out within the context of national defence fall outside the scope of the personal data protection legislation. In light of the above, the Authority identified specific parts of the draft law that need to be improved and/or clarified.

Recommendations

In 2020, the Authority issued two recommendations on the compliance of data controllers with specific legislation on electronic communications and on fulfilling the right to be informed when processing data through video-surveillance systems.

-**Recommendation 1** - **Recommendations on the compliance of data controllers with specific legislation on electronic communications**

The Authority has identified a lack of compliance by information society service providers with the requirements set forth in the legislation on the processing of data in electronic communications and the GDPR in relation to the management of cookies and related technologies. With a view to providing practical guidance to data processors and information to users of Greek websites, the Authority issued a document with specific compliance recommendations applicable to this sector. This document includes guidance regarding the lawful use of such technologies, and practices to be avoided. The Authority points out that consolidating those requirements does not consist a change in the applicable institutional framework and its case law with the provisions of which controllers must comply. Recognising, however, that some time may be required to adjust the management mechanisms used in websites, the Authority called on all controllers to complete that adjustment step within two months at most.

-**Recommendation 2** - **Recommendations-templates on fulfilling the right to be informed when processing data through video-surveillance systems**

Controllers using video-surveillance systems must provide thorough information on the operation of cameras before users enter the premises under surveillance. To this end, it is usually more appropriate to follow a multi-level approach, that is, to install notice boards that provide direct information to persons entering the premises and contain easily accessible detailed information. The Authority highlights, in particular, the obligation for enhanced transparency deriving from the GDPR, and provides new information templates, in addition to the template provided in the document of guidelines 3/2019 of the EDPB on processing of personal data through video devices.

The use of those templates is suggested for data controllers established in Greece who use video-surveillance systems to protect persons and goods. The new templates will replace the notice board template attached to guideline 1/2011 issued by the Authority, and must be adapted accordingly. Recognising that a certain amount of time is required to adjust notice boards and wordings, and handling processes for requests concerning the exercise of rights deriving from the GDPR, the Authority calls on all data controllers to complete that adjustment within two months the latest.

-**Recommendation on publishing images of minors**

The Authority, in the context of its ex officio responsibility, found that the photos of two under-age girls gone missing that had been lawfully published via AMBER ALERT, were reproduced in several online websites, mostly news sites, even after the purpose of their publication had been accomplished (the two girls were luckily found). Against this background, the Authority issued recommendation pointing out that upon expiry of the AMBER ALERT issued for the missing 10-year old girls found in Thessaloniki and Athens, respectively, once the purpose has been achieved, there is no need for further exposure of the children's personal data. For this reason, the Authority issued a warning according to which the photos of the girls featuring in the notice of disappearance and in every relevant report must be removed immediately. Moreover, any image of the girls may only be published following the required blurring (press release Gen/Outc/4118/15-06-2020).

COMMUNICATION POLICY

One of the crucial aspects of the Authority's mission over time is to raise awareness both among data subjects about the risks, rules, safeguards and rights regarding the processing of their data, and among controllers and processors about their obligations under the GDPR.

In brief, the communication activities that were carried out in 2020 were the following: organisation of an information day, contribution to the organisation of training seminars, research and other EU-funded projects, participation of the Authority's representatives in scientific conferences, workshops, events and training seminars, publication of new issues of the Authority's e-Newsletter, publication of press releases, responses to media queries, interviews and publication of articles in the Press. It is also noted that during 2020 the Authority started creating its new web portal.

Data Protection Day, 28 January 2020

On the occasion of the celebration of the 14th anniversary of the Data Protection Day, the Authority held an information day entitled "The right to personal data protection in the wake of the application of Regulation (EU) 2016/679 and the transposition of Directive (EU) 2016/680" at the Amphitheatre of the National Hellenic Research Foundation on January 28th, 2020. At the beginning of the event, the Minister of Justice Mr Konstantinos Tsiaras and the President of the Authority and Honorary President of the Council of State Mr Konstantinos Menoudakos delivered opening speeches. The Deputy President of the Authority, Honorary Judge of the Supreme Court of Civil and Penal Law, Mr Georgios Batzalexis, was moderator of the 2nd part and the Q&A session that followed.

Contribution to the implementation of training seminars, research and other EU-funded projects

The Authority, in the context of its responsibilities for raising awareness among controllers and processors about the personal data protection legislation, has been implementing a project entitled "Facilitating compliance with the GDPR for Small and Medium-Sized Enterprises and promoting data protection by design on ICT products and services (byDesign)" since 1/11/2020 and for a period of 24 months. The project is carried out in collaboration with the University of Piraeus and the Greek IT company ICT Abovo and is co-funded by the European Commission.

Furthermore, from 1/5/2018 to 30/4/2021 the Authority participated in the project entitled "Business Process Reengineering and functional toolkit for GDPR compliance (BPR4GDPR)" as part of "Horizon 2020-EU.3.7.6" — Ensure privacy and freedom, including in the Internet and enhance the societal, legal and ethical understanding of all areas of security, risk and management". The goal of BPR4GDPR was to provide a holistic framework able to support end-to-end GDPR-compliant ICT-enabled processes for controllers and processors.

During 2020, the President of the Authority, its members and scientific staff participated as speakers or moderators in scientific conferences and workshops. Additionally, scientific staff from the Auditors' Department participated as speakers in various training seminars/workshops with subjects, such as protection of personal data and access to public documents and court decisions, protection of personal data in work relationships, interpretation of the General Data Protection Regulation provisions and artificial intelligence.

E-Newsletter

During 2020, the Authority published four (4) new issues of its e-Newsletter aiming to provide a short but comprehensive account of its work, current developments in the field of personal data at national, European and international level, news on recent or upcoming events, useful links to websites related to the above issues, and news on relevant literature.

Media Interviews/articles and responses to media queries

The President of the Hellenic DPA, Mr Menoudakos, gave several media interviews (TA NEA, ANT1, Parapolitika FM, ERT, et.c.) and also his articles were published in national newspapers (Efimerida ton Sintakton, Ethnos, et.c.). It is also noted that the Authority responded to several media queries (Kathimerini, News247, Inside Story, ALPHA TV, Politico, Bloomberg, MLA et.c.).

Press releases

The Authority's press releases that attracted a lot of media coverage in 2020 were the following:

- Press release published on 14/1 entitled: "Examination of complaints filed for

accessing the company server and checking the employee's e-mails by the employer, for unlawfully installing and operating a closed circuit television (CCTV) system, and infringing the right of access";

• Press release published on 22/1 entitled: "Processing of personal data in a server without evidence of compliance with the principles set out in Articles 5(1) and 6 of the GDPR in breach of the principle of safe processing";

• Press release published on 25/2 entitled: "Recommendation on the compliance of data controllers with specific legislation on electronic communications";

• Press release published on 18/3 entitled: "Processing of personal data in the context of the management of COVID-19";

• Press release published on 15/4 entitled: "Guidelines of the Data Protection Authority on safety measures taken in the context of telework";

• Press release published on 12/5 entitled: "Video conferences held between the President of the Authority and the Hellenic Primary School Teachers' Federation (DOE), the Federation of Secondary School Teachers (OLME) and the OIELE (Hellenic Federation of Private School Teachers) and the Hellenic Association of Substitute Teachers, following their requests to this effect";

• Press release of 25/5 with statements made by the President of the Authority on the occasion of celebrating two years since the entry into force of the GDPR";

• Press release published on 9/6 entitled: "Fulfilling the right to be informed when processing data through video-surveillance systems – new notice board templates";

• Press release on 15/6 entitled: "Recommendation on publishing images of minors";

• Press release published on 30/6 regarding the publication of opinion 3/2020 by the Authority relating to the draft presidential decree on the use of surveillance systems able to obtain or record sound or image in public areas;

• Press release published on 22/10 on a data breach notification by COSMOTE S.A.

Publication of articles

The members and scientific staff of the Authority published articles in scientific journals with regard to new implementing Law 4624/2019 on personal data, the relationship between access to public documents and protection of personal data, and safety of blockchain solutions in relation to the Internet of Things (IoT).

Published by the Hellenic Data Protection Authority
Edited by the Secretariat of the Hellenic DPA

Hellenic Data Protection Authority
Kifisias 1-3, 11523, Athens – Greece
Website: www.dpa.gr
E-mail: contact@dpa.gr