HELLENIC DATA PROTECTION AUTHORITY

Summary of Annual Report

Athens, 2019

CONTENTS

FOREWORD BY THE PRESIDENT

The legal protection of personal data entered a new era on May 25th, the date on which the Regulation (General Data Protection Regulation) came into force. The GDPR is the starting point of a new "roadmap" in the long process of personal data protection without challenging, however, the achievements of the landmark Directive 95/46/EC.

The mission of the data protection supervisory authority is strengthened by the GDPR. The multidimensional role and objective of the Authority, namely in providing information, establishing the regulatory framework, conducting investigations - imposing penalties, is maintained. These tasks, however, are now carried out in different legal and factual circumstances. The Hellenic Data Protection Authority pursued its mission in this particularly crucial year full of challenges, being fully aware that it is at the dawn of a new era for the protection of personal data. It has, therefore, structured its action around two pillars: processing the backlog of cases and, at the same time, speeding up its preparation for the implementation of the GDPR, which tightened the protection status, mainly leading to radical changes in procedural matters. These changes resulted in the need to modify or adapt the Authority's internal organisation and operation to new circumstances.

At the same time, the Authority has successfully met its ongoing European obligations and has actively participated in the working groups and committees that operate under the European legislation on the protection of personal data. Furthermore, the Authority has, to the fullest extent possible, carried out the work and tasks conferred on it by the GDPR which has modified the Authority's competences that were provided for in the previous legislation. Concurrently, it took the initiative to provide general information on the provisions of the GDPR, such as organising, co-organising or providing support for information events, conducting training courses and research projects, participating in conferences, publishing articles in the press and creating information content for its website which has already been reformed and is constantly being updated and enriched. It should be noted that, despite the major issue of understaffing, and thanks to the increased efforts of its staff, the Authority has successfully met the high requirements of this demanding but necessary transition and adaptation to the new regulatory framework.

At the time this annual report was being printed, Law 4624/2019 implementing the Regulation and transposing Directive (EU) 2016/680 was being published. The Authority is now called upon to interpret and implement Law 4624/2019 by examining the compatibility of its provisions with the ones included in the GDPR. Its priorities include revising its statute and its rules of procedure based on the relevant authorisations provided for in this recent law.

On 25 May 2018, the application of the GDPR was initiated but not completed. Its effectiveness depends on its proper implementation and a sound approach by data controllers and processors who should consider it not as a mandatory "burden" but as an opportunity to change the culture aiming to increase the trust of citizens-data subjects regarding the protection of their personal data and privacy. We are still at the beginning of a new journey and compliance is an ongoing process which requires all stakeholders involved to step up their efforts, both in terms of providing information and training, and developing best practices.

Konstantinos Menoudakos
President of the Hellenic DPA, Honorary President of the Council of State

ROLE, MISSION AND RESPONSIBILITIES

The Hellenic Data Protection Authority is a constitutionally consolidated independent authority established by Law 2472/1997 transposing European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data into Greek law. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), which entered into force on 25 May 2018 in all EU countries, repealed Directive 95/45/EC. The Authority, as of May 25th, has the task of supervising the implementation of the General Data Protection Regulation and other provisions concerning the protection of individuals with regard to the processing of personal data, and of exercising the powers conferred on it from time to time. Furthermore, as regards the protection of personal data in electronic communications, the Authority applies Law 3471/2006 transposing European Directive 58/2002 into national law.

HUMAN RESOURCES AND OPERATIONAL ISSUES

Under Article 20(1) of its founding Law 2472/1997 the Authority is assisted by a Secretariat that operates at 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 Financial Services. In 2018, the Authority's budget amounted to EUR 2,541,000.00, while the budget approved for 2019 amounts to EUR 2,849,000.00.

As pointed out in the annual reports of previous years, understaffing is the most serious problem the Authority is facing, and it has been greatly exacerbated over the years of the financial crisis in Greece. This problem is becoming all the more critical due to the Authority's new tasks and duties. In connection with a wide range of powers conferred on the Authority under European and national legislation, as well as the volume of incoming cases, understaffing is a critical factor hindering the Authority from fully completing its mission. While grouping, auditing and prioritizing incoming cases enables the Authority to somewhat reduce the negative impact of understaffing, it continues to be a serious problem as it mainly prevents the Authority from taking ex officio action, such as audits, raising awareness among data subjects, controllers and processors, actively participating in committees and working groups, etc.

The total appropriations available for 2018 increased by around 7% compared to the previous year. However, this increase was, as in the previous year, due to the higher amounts available for the major budget category "remuneration", which by nature could not be utilized. This is because, on the one hand, the number of staff remained stable, and, on the other, the appropriations for operating expenditure remained insufficient, despite constant requests for them to be increased. The appropriations approved for 2019 have also increased by about 12 % once again in the major budget category "remuneration", while appropriations for operating expenditure remained approximately the same as in 2018. The appropriations in question are not sufficient for the Authority to meet the full range of its responsibilities, and in particular, its new obligations under the GDPR, making it a top priority not only to increase the number of staff but also to upgrade and adapt the IT and network infrastructure, and actively participate in the EDPB and other joint supervisory committees and working groups or committees.

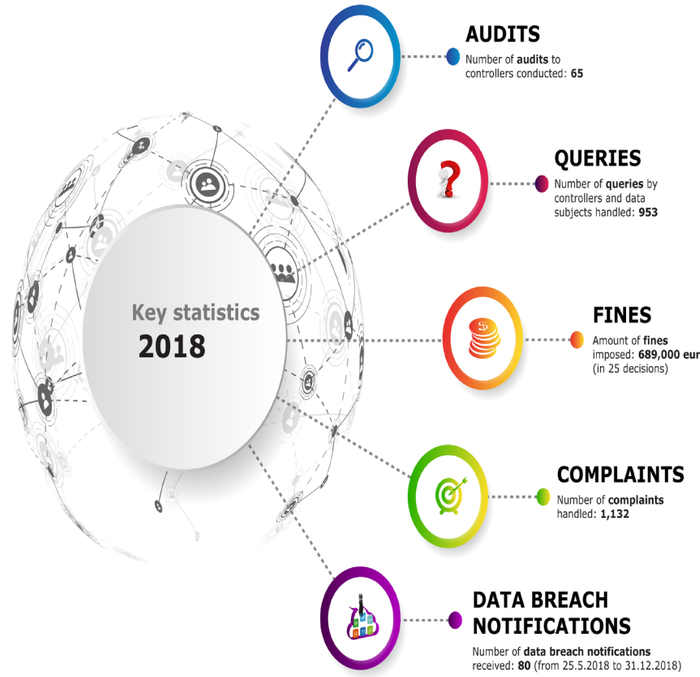
In 2018, all processed cases/complaints, queries and notifications of processing operations amounted to 3,064. The examination of 77 cases was completed by means of decisions issued by the Plenary or the Chamber. In 2018, the Authority also issued 3 opinions.

More specifically, the Authority handled 1,132 complaints and 953 queries submitted by controllers or citizens regarding the lawfulness of a particular processing or how to implement the relevant legislation. The Authority processed 979 notifications, of which 896 related to the installation and operation of closed circuit television systems. Furthermore, in 2018, the Authority granted or renewed 50 permits for keeping records of sensitive personal data and 19 licenses for data transfers to non-EU countries.

In addition, the Authority conducted audits in 65 data controllers who are active online in the fields of financial, insurance, e-commerce, ticket and public sector services. By means of these audits the Authority investigated how specific requirements of the data protection legal framework were met. In particular, the audits focused on the transparency of the processing, the use of cookies and technologies that require access to a user's terminal equipment, sending advertising e-mails, and the safety of websites through indicative points perceived by citizens when navigating the internet and using online services.

As for data breach notifications provided for in the GDPR, 80 notifications were submitted to the Authority from 25 May 2018 until the end of the year, of which 70

were submitted by companies which had their main establishment in Greece, while the remaining 10 were submitted by controllers which had their main establishment in another Member State or with no establishment in the EU. The Authority has already conducted further investigations in 13 of these breaches, and in 5 of these cases the investigation was completed before the end of 2018.



In 25 of the Authority's decisions for 2018, penalties were imposed on controllers. In 12 cases the sanction of warning-instruction to comply was imposed, while in 13 cases a fine ranging from EUR 1,000 to EUR 150,000 was imposed. It should be noted that in 4 out of these 13 decisions issued by the Authority, and in addition to the fine, a penalty of warning-instruction to comply was also imposed. Overall, the total amount of fines imposed was EUR 689,000. The Authority imposed sanctions for infringement of the provisions relating to failure to notify a personal data breach in a timely manner, the conditions for processing personal data in the electronic communications sector, the obligation to notify and obtain an authorisation to process sensitive personal data, to provide data subjects with the right to be informed as well as the right of access and to object, the lawfulness of the processing by a public authority, but also to provisions on the use of video surveillance systems for the protection of persons and goods. The above decisions of the Authority are classified into the following thematic areas: 2 in public administration, 4 in private economy, 7 in the financial sector, 1 in health, 6 in electronic communications and 5 in closed circuit television systems.

OPINIONS

In 2018, the Authority issued 3 opinions on the disclosure of personal information about political party donors (Opinion 1/2018), the draft law on "measures to promote the institutions of foster family and adoption" at the request of the Ministry of Labour, Social Security and Social Solidarity (Opinion 2/2018), and the retention of asset declarations for the years 2016-2017 in the Electronic Asset Declaration System "POTHEN" under Law 4571/2018 on urgent provisions for submitting asset declarations (Opinion 3/2018).

ADVICE — REMARKS

The Authority also provided advice and recommendations to controllers on a variety of personal data protection issues.

- **E-Privacy**

The Authority expressed its views on the draft regulation on the respect for privacy and the protection of personal data in electronic communications (e-Privacy) and the replacement of the existing Directive 2002/58/EC, which is under consultation with the European Council, following the European Parliament's approval in principle.

- **Remarks of the Authority on the Draft Law on the amendment/recasting of Law 3758/2009 on companies informing debtors on overdue claims and other provisions**

The General Secretariat for Trade and Consumer Protection of the Ministry of Economy and Development submitted to the Authority a preliminary draft amendment to Law 3758/2009 on companies informing debtors on overdue claims and other provisions in order for the Authority to comment in light of the new General Data Protection Regulation. The Authority submitted its initial remarks on the above draft, pointing out that its processing requires more time and a detailed study of the overlapping provisions. It also mentioned that it would be advisable and more appropriate to set up a law drafting committee -joined by a representative of the Authority- aiming to reform the institutional framework governing the activity of informing debtors on overdue claims.

- **PNR-Passenger records**

In addition, the Authority, following its participation in the special law drafting committee aiming to adapt the Greek law to the provisions of EU Directive 2016/681, gave its opinion on the remarks submitted during the consultation process of the draft law on how to use the concepts and terms correctly, and provide for a clear wording of provisions and meanings faithful to the Directive.

- **Europol**

Furthermore, the Authority, in response to a request from the Hellenic Parliament to provide information on the legislative framework for the protection of personal data in law enforcement activities, sent a relevant memorandum which initially referred to the previous legal framework, namely to Council framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which, however, has never been transposed into Greek law.

Finally, the Authority expressed its view on the legality of using closed circuit television systems operated by toll road operators with a view to establishing breaches of the Highway Code following a relevant question submitted by Police Directorates.

A fundamental aspect of the Authority's mission is to enhance the awareness of citizens (as data subjects) in relation to the risks, rules, safeguards and rights regarding the processing of their data, but also of controllers and processors in relation to their obligations regarding the protection of personal data, which is now explicitly provided for in the GDPR. In order to achieve this objective specific communication activities were planned and carried out during 2018.

In short, these include the following: organisation of "information days", conducting training courses and research projects, participation of the Authority's representatives in scientific conferences, workshops and training seminars, giving speeches-presentations, publishing new issues of the Authority's electronic newsletter, creating new information content about the GDPR for the Authority's website, issuing press releases and responding to questions raised by journalists, giving interviews and publishing articles in the press, as well as in academic journals. Finally, it should be noted that during the transition to the new legal framework, a group of staff and trainees of the Secretariat of the Authority was set up for a period of four months in order to inform the general public.

DECISION NO 34

Title: Inspection of an employee's computer by the employer

Summary:

Conditions required for the employer to inspect an employee's computer without the presence or knowledge of the employee. It was not established that the employee's computer contained personal data nor that the employer processed personal data when inspecting the computer. The employee's right of access was infringed by the employer's unsatisfactory response to the request for information. An administrative fine of EUR 3,000 was imposed. It is recommended that a regulation on the proper use and functioning of the equipment and the ICT network by the employees should be introduced and implemented, and that appropriate technical and organisational security measures should be taken for the computing system.

DECISION NO 41

Title: Imposition of a fine on a law firm for an unlawful operation of a video surveillance system

Summary:

An inspection on a law firm was conducted following a complaint submitted by the Labour Inspectorate of the Ministry of Labour and Social Security concerning the operation of a video surveillance system on its premises. It was found that the system operates in places not covered by the principles of necessity and proportionality, in breach of the provisions of Directive 1/2011 of the Authority and of Law 2472/97. In particular, the video surveillance system does not operate only in entrances and

exit locations or the cash desk, but also covers workplaces almost exclusively used by employees. A wide range of employees work in these workplaces, from call center employees to employees working in typical single space offices. The video surveillance system takes images from the public road, the sidewalks, the opposite buildings and the opposite perpendicular street outside the main entrance of the controller's establishment. The images taken are not limited to the space near the entrance. The controller has posted panels with relevant information material but only in the interior of the area. The controller failed to notify in time the Authority of the operation of the video surveillance system. A fine of fifty thousand EUR (EUR 50,000) was imposed on the controller for the above infringements.

DECISION NO 60

Title: Imposition of a fine on a controller for unlawful phone calls

Summary:

The Authority conducted a coordinated series of audits in companies for which it had received a large number of complaints concerning unsolicited phone calls for the promotion of goods and services. As part of this action, on-the-spot audits were carried out both at Wind's own premises and the premises of the cooperating company which makes phone calls. The Authority collected complete records of calls made during the first half of 2017, which were cross-checked with the registries provided for in Article 11 of Law 3471/2006 ("do not call"/"opt-out" registries) that are held by telephony service providers. From the aforementioned cross-check, a large number of unlawful calls was discovered (140,395). The evidence compiled during the investigation further revealed that more unlawful marketing phone calls had been made by companies cooperating with Wind, the details of which have not been submitted to the Authority. At the same time, the Authority examined the procedures applied by Wind and judged that, although the company has improved some of them, it does not apply, in practice, appropriate technical and organisational measures to ensure full legitimacy of its activity, despite the fact that it had sufficient time to do so since the adoption and notification of Decision 66/2016, which had addressed the same matter. The Authority imposed a fine of EUR 150,000 for all of the above infringements.

DECISION NO 63

Title: Imposition of a fine on a controller for unlawful phone calls

Summary:

The Authority conducted a coordinated series of audits in companies for which it had received a large number of complaints concerning unsolicited phone calls for the promotion of goods and services. As part of this action, on-the-spot audits were carried out both at Cosmote's own premises and the premises of the cooperating company which makes phone calls. The Authority collected complete records of calls made during the first half of 2017, which were cross-checked with the registries provided for in Article 11 of Law 3471/2006 ('do not call'/'opt-out' registries) that are held by telephony service providers. From the aforementioned cross-check, a large number of unlawful calls was discovered (at least 816,164). At the same time, the Authority

examined the procedures applied by Cosmote and judged that, although the company has improved some of them, it does not apply, in practice, appropriate technical and organisational measures to ensure full legitimacy of its activity, despite the fact that it had sufficient time to do so since the adoption and notification of Decision 64/2016, which had addressed the same issue. The Authority imposed a fine of EUR 150,000 for all of the above infringements.

DECISION NO 67

Title: Reprimand to DIMERA GROUP SPORTING GOODS TRADING SOLE OWNER L.L.C.

Summary:

DIMERA GROUP SPORTING GOODS TRADING SOLE OWNER L.L.C. (hereinafter, DIMERA) submitted to the Authority a personal data breach notification with ref. no. Γ/ΕΙΣ/7022/27-08-2018 under Article 33 of General Regulation (EU) 2016/679 (General Data Protection Regulation — hereinafter, GDPR). This incident concerned a security attack which was the result of "hacking". DIMERA submitted the above notification to the Authority within 72 hours after having become aware of the incident and immediately took action to investigate and address it. The company also informed the individuals (customers of its e-shop) whose data had been leaked.

The Authority, considering the notification in its entirety, as supplemented, in addition to the security measures that were in place before the incident, issued, by means of Decision 67/2018, a reprimand to DIMERA under Article 58(2)(b) of the GDPR for infringement of Article 32 of the GDPR concerning the security of processing — and, thereby, of Article 5(1)(f) of the GDPR — due to the fact that the company had not taken the necessary steps to update the software used, had not put in place adequate mechanisms to identify these attacks and did not have procedures in place to regularly assess the security measures. In order to issue this decision, the Authority took into account the fact that the company took all the necessary steps as soon as it became aware of the incident, including security measures, to ensure security in the future.

DECISION NO 77

Title: Question submitted by the Association of Judicial Officers of the Administrative Courts of Athens concerning the use of personal TAXISNET codes for official business purposes

Summary:

The Authority considered the legality of the mandatory and continuing use for official business purposes of authentication information attributed to natural persons for private purposes — and, in particular, of TAXISNET information (codes) provided to taxpayers making use of the electronic services of the Ministry of Finance and the Independent Authority for Public Revenue. This issue was brought to the attention of the Authority by the Association of Judicial Officers of the Administrative Courts of Athens, as the above mentioned information is required for the certification of the competent officials in order to enable them to commit electronic administrative fees (e-fees), as part of a pilot implementation of the measure by the Ministry of Justice, Transparency and Human Rights, and, more specifically, by the Administrative Court of Appeal of Athens.

The Authority, by means of its Decision No 77/2018, considered that the State's requirement that the codes/credentials in question, which have been provided to the citizens/persons entitled to enable them to log on to TAXISNET information system with a view to mainly carrying out their obligations to the public finance services, be used for another incompatible purpose (as part of their employment relationship), which is clearly separated from the individual's private life without this being the decision or choice of the citizen, constitutes a restriction of the constitutional right to informational self-determination (Article 9a of the Constitution), a fundamental component of which is also the processing of personal data for a predetermined and specific purpose. It is, therefore, in contradiction with the substantive conditions necessary for processing personal data, as laid down in Law 2472/1997 (principle of purpose — Article 4(1)(a)) which is applicable in this case. By virtue of the same Decision, the Authority acknowledged that such processing also gives rise to safety issues which can be limited by technical measures; however, taking security measures does not mean that the breach caused by the mandatory use of credentials for two incompatible categories of purposes has been waived.

Based on the above, the Authority, pursuant to Article 21(1)(a) of Law 2472/1997, issued a warning to the Independent Authority for Public Revenue (IAPR) and the Ministry of Justice, Transparency and Human Rights, according to which they should adjust the authentication mechanisms they have in place for judicial officers responsible for committing and handling electronic fees in general by the end of 2019, so that they are not required to enter their TAXISNET credentials to obtain authentication. The Authority also noted that the above applies to employees of all public bodies as regards the process of issuing electronic administrative fees.

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