HELLENIC DATA
PROTECTION AUTHORITY

Summary of Annual Report

Athens, 2021

HELLENIC DATA PROTECTION AUTHORITY

HELLENIC DATA PROTECTION AUTHORITY

FOREWORD BY THE PRESIDENT

The entry into force of the General Data Protection Regulation (GDPR) on 25 May 2018 paved the way for further positive developments in the protection of personal data during 2019, among which was the significant work by the national data protection authorities and the European Data Protection Board. Additionally, the awareness of personal data protection increased and many organisations and businesses considered this new regulation as an opportunity for re-engineering and adoption of good practices in data processing activities.

The GDPR is not only a new legislative framework but it also introduces a new culture of accountability and compliance. Undoubtedly, more time is needed in order to draw comprehensive and secure conclusions as far as the adaptation to the requirements of the new legislation is concerned. However, it became clear, in 2019, that the application of the new rules is a dynamic process which requires constant and systematic effort.

The delayed adoption of national Law 4624/2019 did not prevent the enforcement of the Regulation, which is the main legislation and has higher legal effect. From that perspective, Law 4624/2019 is complementary and applies in so far as it does not conflict with the GDPR. Law 2472/1997 establishing the Authority continued to apply, during most of 2019, but only in the part that did not conflict with the GDPR or pertained to issues that are not fully regulated by this new European legislation.

In 2019 the Authority examined important cases - either in response to complaints or investigations carried out on its own initiative or in the context of its consultative work - and released important decisions imposing fines but also issuing recommendations, warnings or reprimands.

Indicatively, I would like to point out that, among its many activities, the Authority drew the initial conclusions from the first large-scale series of audits

aimed at investigating compliance with the GDPR and the legislation on electronic communications of 65 data controllers, which operate online in the areas of financial services, insurance services, e-commerce, ticket services and public sector services.

In addition, the Authority initiated an ex officio investigation of companies in the auditing sector as far as their compliance with the obligations of protection of employees' rights is concerned. In 2019 the Authority also issued guidelines for the lawful processing of personal data for the purpose of political communication in view of the European and national elections in May and July 2019, respectively.

This annual report reflects the intensive and systematic effort made by the Authority to meet its new tasks and responsibilities although significantly understaffed. The Authority managed, however, to increase its effectiveness thanks to the high sense of responsibility and the intensity of the efforts of its staff. Against this backdrop, the Hellenic DPA carried out, as fully as possible, the work and tasks assigned to it by the GDPR. At the same time, it took initiatives to increase the awareness on the provisions of the GDPR, such as the organisation/co-organisation or support of informational events, the implementation of training seminars to data protection officers in the context of the implementation of EU-funded projects, the organisation of an educational workshop for students, the participation of its representatives in conferences, the publication of articles in the media and the creation of information content for its website[1].

The Authority, as all the independent data protection supervisory authorities comprising the European Data Protection Board, is called to find the balance point between privacy, the right to informational self-determination and the public interest. The right to the protection of personal data is not autonomous from the entire legal order. The application of the relevant legal rules is weighed against the need to safeguard other fundamental rights but also serve the public interest. This is difficult but indeed necessary in order to balance often conflicting individual and social rights, under real circumstances. In some particular cases, in which exceptional circumstances occur, this conflict appears to be intense and the need to address serious risks may lead to a shift in the balance point, but without exceeding the limits laid down by the principle of proportionality. The commitment to safeguarding human rights is a constant effort upon which the quality of our democracy and civilization will ultimately be based in the days to come.

Konstantinos Menoudakos

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

1 It is noted that the Hellenic DPA launched its new website in January 2021.

1.
OVERVIEW

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 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. It is noted that National 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" (Government Gazette 137/A/29-8-2019) was adopted on August 29th, 2019. Law 4624/2019 repealed Law 2472/1997, except for certain provisions, which remained in force.

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 a Directorate level and consists of four (4) departments: a) the Auditors' Department, b) the Communications Department, c) the Department of Administrative Affairs and d) the Department of Finance. In 2019, the Authority's

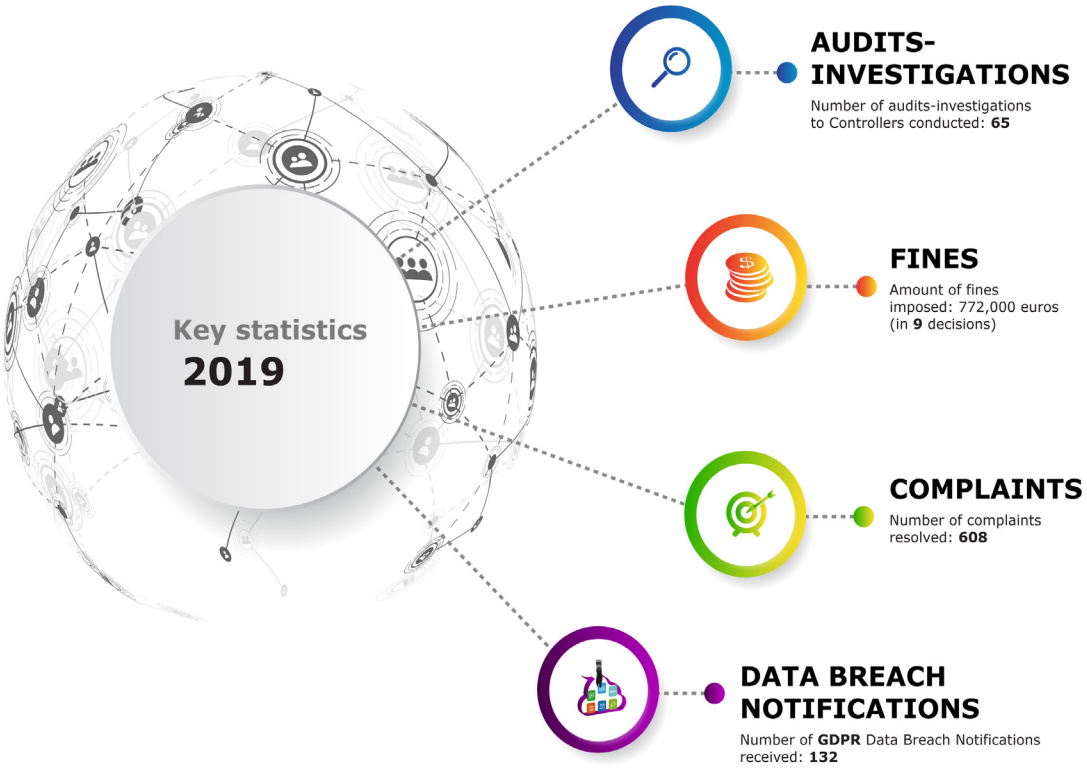
budget amounted to EUR 2,849,000.00, while the budget approved for 2020 amounts to EUR 3,101,000.00.

In all the annual reports of previous years understaffing has been identified as the most serious problem of the Authority. In the years of the financial crisis it has become even more acute because of the new powers and tasks of the Authority. In the light of its wide range of competences, which derive from European and national legislation, and the increasing number of cases, understaffing is an essential deterrent to the Authority's efforts to fully perform its assigned mission. The negative impact is greater on the development of its preventive work, such as systematic carrying out of investigations/audits or awareness-raising of data subjects, controllers and processors.

As far as appropriations available for 2019 are concerned, they were increased by around 12% compared with the previous year, but the increase was mainly for the major budget category "remuneration", which cannot be allocated to other needs of the Authority. The increase of around 9% in the appropriations for operational expenditure was not sufficient, despite constant requests for a significant increase. For this reason, efforts are being made to exploit as much as possible other sources of funding, such as European Union programmes, notably to expand digital infrastructure, strengthen its awareness-raising action and "support" controllers and processors so that they comply with the GDPR, through tool development. For 2020, the appropriations approved rose by about 9% compared with those in 2019, but again they came from a significant increase in the appropriations for "remuneration", while the appropriations for operational expenditure fell by around 8%. These appropriations fall short of what is necessary in order for the Authority to respond to the full range of its responsibilities, particularly to its new obligations arising from the GDPR, and at the same time they make the upgrade of IT infrastructures and networks, the development of awareness-raising action, as well as its active participation in the EDPB and other Joint Supervisory Committees and Working Groups a top priority.

In conclusion, the Authority, in all these efforts, has strived to achieve the highest possible effectiveness of its work, which generally aims to create a data protection-friendly environment in Greece. In order to achieve its mission, the Authority must necessarily have adequate human resources and the necessary financial and technical means and facilities, and expects the State to respond, in compliance with the relevant provisions of the GDPR.

2. KEY STATISTICS



In 2019, the number of incoming cases of complaints amounted to 983, up by about 16% compared to 2018 (847), while 608 cases of complaints were resolved. The number of data breach incidents notified to the Authority, according to the GDPR amounted to 132, increased by about 65% compared to the previous year (80 from 25 May to 31 December 2018), while 22 data breach notifications were submitted by electronic communications service providers. The examination of 48 cases was completed with the adoption of a decision by the Plenary or the Chamber. In 2019 the Authority also adopted an opinion.

It is noted that there is a change in the statistics presented in this Annual Report compared to past years, which is due to its differentiated responsibilities and tasks deriving from the GDPR. The main differences are that the Authority no longer examines questions of controllers, or grants permits, nor is there the obligation of controllers to submit notifications of processing operations. On the other hand, there is now provision for cooperation with counterpart supervisory authorities of Member States in cross-border cases and within the framework of the European Data Protection Board, 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, the Authority provides information to data subjects, upon request, for the exercise of their rights.

The total incoming documents in 2019 amounted to 7,563, reduced by around 28% compared to the previous year. With regard to the way incoming documents are submitted to the Authority, it is noteworthy that around 80% of the submission is by electronic means, in particular by e-mail, at around 75% and via its web portal at a rate of 5%. Fax was also used, at around 3%, but the use of this medium is rapidly declining. Overall, the use of electronic media in 2019, including fax, amounted to about 83% from around 74% the previous year. The use of e-mail increased particularly in 2019 compared to 2018 (to 75% from 58%), while the use of the web portal for the submission of documents, on the contrary, is significantly reduced (to 5% from 11%).

In 2019, the Authority completed its investigation-audit - that had begun the year before - on 65 data controllers operating online in the fields of financial services, insurance, e-commerce, ticket services and public sector services. Furthermore, in 2019, the Authority carried out an audit-investigation of the application of the electronic ticket at the Athens Public Transport Organization (OASA). Also, with regard to the aforementioned data breach incident notifications provided for in the GDPR, 122, out of 132, were submitted by companies with a main (120) or local (2) establishment in Greece and the other 10 by a controller with a main establishment in another Member State (6) or without an establishment within the European Union (4).

Twenty (20) of the Authority's decisions impose penalties on controllers. In 11 cases the sanction of warning – recommendation for compliance following a complaint and hearing was imposed and in 9 cases a fine was imposed ranging from EUR 2,000 to EUR 200,000. It is noted that with 1 of these 9 decisions the sanction of the

warning – recommendation was imposed too. In total, fines of EUR 772,000 were imposed. The Authority imposed penalties for infringement of the provisions relating to non-compliance with the principle of data protection by design, the conditions for the processing of personal data in the field of electronic communications, information and the right of access and objection to subjects, confidentiality and data security, as well as provisions on the use of geolocation and video surveillance systems for the protection of persons and goods. The above decisions of the Authority have been categorised in respect of the main thematic areas as follows: 1 in Public Administration, 1 in Social Security, 5 in Private Economy, 2 in Education and Research, 2 in Health, 5 in Electronic Communications, 2 in Labour Relations and 2 in Video-Surveillance.

3. ADVISORY – CONSULTATIVE FUNCTION

OPINIONS

Opinion 1/2019

The Authority examined ex officio a draft Law of the Ministry of Transport in relation to the upgrading of the driving licence examination procedure. It considered that, in principle, there is a reason of public interest that justifies the processing but it also highlighted certain issues in relation to the proposed measure. First, it doesn't appear that there is a need to record with audiovisual means the theoretical knowledge examination. Furthermore, the legislation should correctly define the controller and processors. At the same time, it must be ensured that the equipment used operates only during the examinations. The Authority also pointed out that the legislation neither refers to the principles of data protection by design, nor has it foreseen the obligation to conduct a data protection impact assessment, which should be addressed at an early stage. The Opinion also raises the question of satisfying the principle of time limitation by reducing data retention time. Finally, the Authority also indicated provisions which could be legally improved.

RELATED DECISIONS

Decision 18/2019

TIRESIAS S.A. submitted a request to the Authority so that it approves the extension of the recipients of DFO (Default Financial Obligations System/black list) and CCS (Credit Consolidation System/white list), and in particular the autonomous-direct access of claims management companies, as controllers (or joint controllers) when acting on behalf of Credit Companies (in addition to their indirect access as processors when acting on behalf of the banks) to the files of the TIRESIAS (DFO and

CCS files), substantially expanding such files.

The Authority considered that under the GDPR the controller, in this case TIRESIAS S.A., and the applicant for the autonomous -as controller- access to those files of the TIRESIAS Credit Company must carry out an impact assessment of the planned processing operations because (a) the intended processing operation is subject to the requirement for a data protection impact assessment and b) because the inclusion of claims management companies to the legitimate recipients action of those files, when acting on behalf of Credit Companies, is likely to result in a high risk for the rights and freedoms of natural persons.

Additionally, following a request of TIRESIAS S.A. to include the electronic money institutions in the recipients of the Terminated Merchants System (TMS) and lost/stolen Identity Card and Passport System, the Authority answered that (a) in accordance with the existing Regulation (EU) 2016/679 (Articles 57-58), it is no longer competent to authorise/approve processing operations of personal data and it is at the discretion of the controller to determine the purposes and recipients of the processing of personal data, to which each time, taking into account the principle of accountability (Article 5 of the GDPR); (b) the Authority with its Decisions 6/2006 and 135/2017 judged that the legitimate recipients of the Terminated Merchants System are credit card issuing or managing companies, if they bear liability themselves -and not the credit institution- from the unlawful use of the credit card; c) according to the Decision 25/2004 sources of these data are the natural persons that submitted a declaration of lost or stolen passport of ID, while companies issuing and managing means of payment are included in the recipients; and d) the Authority with its 11/2006 decision for the creation of a record of stolen or lost passports or identity cards by TIRESIAS SA and the sending of these data from the record of the ID section and archives of the Security Branch of the Hellenic Police, judged that the keeping or retention of this file of stolen or lost passports or id cards from TIRESIAS is lawful if certain conditions are met, among which, that access to this file can have only the banks that have a right of access to the files of Tiresias and also the access itself will be online.

Decision 21/2019

Furthermore, the Authority, in response to a citizen’s complaints, investigated ex officio the lawfulness of the installation of video surveillance systems in school units of a municipality. Taking into account that the management of school spaces when they are not closed and the responsibility for maintenance, cleaning and guarding of school buildings belong to the municipalities, as well as that the use of video surveillance system by public authorities for the protection of persons and goods is permitted only in the premises they manage, the Authority decided that a public school should not use a video surveillance system during working hours. During the non-working hours of the school unit, the municipality is responsible for the protection of the area and therefore only that entity can be the data controller; so only the municipality - through the relevant school committee - can judge the necessity and proportionality

of the use of a video surveillance system for the above purpose, taking into account the provisions set out in the Authority's Directive 1/2011.

In the same decision, the Authority notes that data subjects (parents, pupils and teachers) must exercise their relevant rights to the municipality, which must satisfy the rights of the subjects arising from the GDPR.

INVESTIGATIONS-AUDITS

On 28/11/2019, the Authority carried out an on-site administrative investigation-audit at the premises of the Athens Public Transport Organisation (OASA S.A.). The investigation-audit focused on the processing of personal data carried out within the framework of the Electronic Ticket system, in the light of the relevant opinions 1/2017 and 4/2017 of the Authority, which had been issued with a view to the initiation of such processing. The Authority's findings, as well as the adoption of a decision, are expected in 2020.

Furthermore, in 2019, the Authority completed its investigation-audit on 65 data controllers operating online in the fields of financial services, insurance, e-commerce, ticket services and public sector services. The goal of the audit was to investigate the level of compliance with the General Data Protection Regulation and the specific legislation on electronic communications. The main issue that remained to be resolved was the use of tracers (cookies and similar technologies). In this respect, the Authority clarified in many cases that, with regard to the installation of cookies, compliance is deemed incomplete when, through the mechanism for obtaining the consent, the user is urged to accept their installation. In particular, it must be ensured that the user can continue to navigate seamlessly without installing the unnecessary cookies at least as easily as s/he chooses to install them. For example, the user should be able to either accept the installation of cookies (those for which consent is required) or reject it with the same number of actions ("clicks"). By the end of 2019, most of the 65 controllers had met the conditions that were set by the Authority.

4. COMMUNICATION POLICY

A crucial aspect of the Authority's mission is to promote the data subjects' awareness of the risks, rules, safeguards and rights regarding the processing of their data and at the same time the controllers and processors' awareness of their obligations under the GDPR. In order to achieve this goal, specific communication activities were planned and carried out during 2019.

In brief, these include the following: a) organisation of an information day, on the occasion of the Data Protection Day[1], with the support of the Representation of the European Commission in Greece (January 28, National Hellenic Research Foundation, Athens), b) organisation of a GDPR workshop for junior secondary school pupils in collaboration with the Foundation for Research and Technology and Stavros Niarchos Foundation Cultural Center (November 5, Stavros Niarchos Foundation Cultural Center), c) organization of training courses and EU-funded research projects such as "Problem-based training on the data protection reform package in GR and CY – TRAIN GR-CY" (March 1-2 and 29-30, Hellenic DPA, Athens) and d) participation of the Authority's representatives -as speakers- in several scientific conferences, workshops and training seminars.

It is also noted that the 8th eDemocracy International Conference: Safeguarding Democracy and Human Rights in the Digital Age, that took place on 12-13 December 2019 in Athens, was organized by the Scientific Council for the Information Society, in co-operation with the Hellenic Data Protection Authority and a number of European and Greek Universities, Academia and Research (see http://edemocracy2019.eu/).

In view of the GDPR's first anniversary, on May 25, the Authority cooperated

1 Created by the Council of Europe in 2006, Data Protection Day is celebrated every year on 28 January, the date on which the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was opened for signature.

with the Representation of the European Commission in Greece in order to create an outdoor campaign with Greek airport ads for the rights of citizens under the GDPR. The campaign was launched in May at Athens International Airport and it ended in October, at Kos island Airport.

Additionally, during this year, the President, members and the scientific staff gave media interviews and published articles in the press, as well as in academic journals. The Authority also published 4 new issues of its e-Newsletter (in Greek), created new information content about the GDPR for its website, issued 21 press releases and responded to many media queries.

Following their invitation, the Hellenic DPA hosted on 14 June the Eurodiaconia workshop "Communications in a time of European General Data Protection Regulation", in the context of the "2019 Communications Network meeting in Athens". More particularly, sixteen Eurodiaconia members who attended the workshop had the opportunity to gain insights into the data subjects' rights and consent requirements under the GDPR, thanks to the presentation and the discussion that followed with the Hellenic DPA representatives.

Finally, in 2019 a special group of staff and trainees of the Secretariat of the Authority, which had been set up during the transition period to the new legal framework in 2018, continued to inform the general public.

5.
CASE LAW SELECTION

DECISION 18/2019

Title: On the expansion of the recipients of the DFO (Default Financial Obligations System/"black list") and CCS (Credit Consolidation System/"white list")

Summary:

TIRESIAS S.A. submitted a request to the Hellenic DPA so that it approves the autonomous-direct access of claims management companies, as controllers (or joint controllers) when acting on behalf of credit companies (apart from their indirect access as processors when acting on behalf of the banks), to the files of TIRESIAS (DFO and CCS files), thus expanding the recipients of these files.

Under the GDPR, the controller, in this case, TIRESIAS S.A. and the applicant for the autonomous, as controller, access to those files of TIRESIAS Credit Company, must carry out, as stated in the Authority's Decision, an impact assessment of the planned processing operations on the protection of personal data.

DECISION 25/2019

Title: Appeal against the refusal of Google search engine operator to satisfy the request for the removal of a link from the search results, based on the name of the applicant

Summary:

The Authority examined an appeal against Google in respect of its refusal to remove specific links appearing in the search results on the basis of the name of the applicant. The Hellenic DPA judged that three of the links leading to websites, with content that was found inaccurate by court decisions, should not appear in the search results, because that information creates an inaccurate/misleading impression for the applicant. However, the Authority, taking into account that the applicant is an

entrepreneur who has a role in public life and that the information is related solely to his professional activity, considered that it is not required that the other links - leading to websites with information the accuracy of which is not established by judicial decisions or which was found to be true by those decisions - are removed. As regards the applicant's allegations that the content of many of the websites in question constitutes either hate speech or slander and/or defamation, the Authority considered that it had no jurisdiction to deal with, and those claims could be judged by the competent courts. Finally, the Authority reprimanded Google for violating the provisions of Article 12 of the GDPR because the company's response, in one of the applicant's requests, was delayed.

DECISION 26/2019

Title: Infringement of principles for the processing of personal data of employees by the employer company

Summary:

The Authority, in response to a complaint, conducted an "ex officio" investigation of the lawfulness of the processing of personal data of the employees of the company 'PRICEWATERHOUSECOOPERS BUSINESS SOLUTIONS SA' (PWC BS). According to the above complaint the employees were required to provide consent to the processing of their personal data.

The DPA considered that PWC BS as the controller:

1. has unlawfully processed the personal data of its employees contrary to the provisions of Article 5(1)(a) indent (a) of the GDPR since it used an inappropriate legal basis.
2. has processed the personal data of its employees in an unfair and non-transparent manner contrary to the provisions of Article 5(1)(a) indent (b) and (c) of the GDPR giving them the false impression that it was processing their data under the legal basis of consent pursuant to Article 6(1)(a) of the GDPR, while in reality it was processing their data under a different legal basis about which the employees had never been informed.
3. although it was responsible in its capacity as the controller, it was not able to demonstrate compliance with Article 5(1) of the GDPR, and that it violated the principle of accountability set out in Article 5(2) of the GDPR by transferring the burden of proof of compliance to the data subjects.

The Authority, after ascertaining the infringements of the GDPR, decided that in this case it should exercise the corrective powers conferred on it under Article 58(2) of the GDPR by imposing corrective measures, and that it would order the company, in its capacity as the controller, within three (3) months:

- to bring the processing operations of its employees' personal data as described in Annex I submitted by the company into compliance with the provisions of the GDPR;

- to restore the correct application of the provisions of Article 5(1)(a) and (2) in conjunction with Article 6(1) of the GDPR in accordance with the grounds of the decision;
- to subsequently restore the correct application of the rest of the provisions of Article 5(1)(b)-(f) of the GDPR insofar as the infringement established affects the internal organisation and compliance with the provisions of the GDPR taking all necessary measures under the accountability principle.

Moreover, as the above corrective measure is not sufficient in itself to restore compliance with the GDPR provisions infringed, the Hellenic DPA considered that, based on the circumstances identified in this case and under Article 58(2)(i), an additional effective, proportionate and dissuasive administrative fine should be imposed in accordance with Article 83 of the GDPR, which amounts to EUR 150,000.

DECISION 28/2019

Title: Indication of religion and nationality in secondary education qualifications and in the information system "myschool" and exemption of students from the religious education classes

Summary:

The Authority, following complaints, considered that (a) the indication of religion and nationality on the data held at school, the qualifications and certificates of secondary education and the information system "myschool", as well as the existence of relevant fields in the relevant forms, even if it is optional to complete them, and (b) the statement that the student is not a Christian Orthodox and hence invokes grounds of religious conscience for exemption from religious education classes are not lawful because they contravene the fundamental principle of necessity of processing of personal data (article 4 par. 1b law 2472/1997 and 5 par. 1 of the GDPR). For this reason the Hellenic DPA has asked the Ministry of Education, as controller, a) to refrain from these unlawful acts of processing of pupils' personal data; b) to ensure that the relevant provisions are amended immediately and to take all necessary measures to ensure that religion and nationality are no longer indicated in the data held in the school and in the qualifications and certificates of secondary education as well as in the information system "myschool" and c) to issue every necessary guideline for the educational authorities and the directors of school units so that from now on the declaration that the pupil is not Christian Orthodox is not required and this right is exercised (by the same pupil if s/he is an adult or his/her parents if s/he is a minor) exclusively by invoking reasons of conscience.

DECISION 31/2019

Title: Violation of the principle of accuracy and data protection by design when

keeping personal data of subscribers

Summary:

The Hellenic DPA has received complaints from telephone subscribers of the Hellenic Telecommunications Organization S.A. ("OTE") who, although registered in the OTE's do-not-call register (according to Article 11 of Law 3471/2006), they received unsolicited calls from third companies for the promotion of products and services.

The investigation of the case showed that those subscribers had submitted a portability request for the transfer of their subscription to another provider. As a consequence, OTE deleted their entries from the do-not-call register. However, when those subscribers cancelled their portability request, there was no proper procedure to cancel their removal from the register. Subscribers were listed as registrants in the internal system of the provider's customer service, but their telephone numbers were not included in the register sent by OTE to the advertisers, as the two systems, due to the error in their interconnection, did not have the same content.

The Authority found that this incident affected a large number of individual subscribers, as there was an infringement of Article 25 (data protection by design) and Article 5(1)(c) (principle of accuracy) of the General Data Protection Regulation (GDPR). It therefore imposed an administrative fine of EUR 200,000 on the basis of the criteria laid down in Article 83(2) of the Regulation.

DECISION 34/20219

Title: Failure to satisfy the right to object and the principle of data protection by design when keeping personal data of subscribers

Summary:

The Hellenic DPA has received complaints from the recipients of advertising messages from OTE (Hellenic Telecommunications Organization S.A.) concerning their lack of ability to unsubscribe from the list of recipients of advertising messages. In the course of the examination of the complaints it emerged that from 2013 onwards, due to a technical error, the removal from the lists of recipients of advertising messages did not operate for those recipients who used the "unsubscribe" link. OTE did not have the appropriate organisational measure, i.e. a defined procedure by which it could detect that the data subject's right to object could not be satisfied.

Subsequently, OTE removed around 8,000 persons from the addressees of the messages, who had unsuccessfully attempted to withdraw from 2013 onwards. The Authority has found an infringement of the right to object to the processing for direct marketing purposes (Article 21 (3) of the GDPR) as well as Article 25 (data protection by design) of the GDPR and imposed an administrative fine of EUR 200,000 on the basis of the criteria of Article 83 (2) of the Regulation.

DECISION 43/2019

Title: Investigation regarding access to and inspection by the employer of an

employee's emails on a company server, illegal installation and operation of a closed-circuit video-surveillance system and infringement of the right of access

Summary:

The employer company had suspicions that a senior manager committed illegal acts against its interests; as a result, it carried out an investigation and recovered deleted e-mails from its server. The company had complied with the requirements of the GDPR and its internal policies and regulations provided for the prohibition of the use of the company's electronic communications and networks for private purposes as well as the possibility of carrying out internal inspections. On the other hand, the closed circuit video-surveillance system that had been installed operated illegally; furthermore, the recorded material submitted to the Authority was not taken into account pursuant to Article 19(3) of the Constitution. The company did not satisfy the employee's right of access to the personal data contained in the corporate personal computer that was used. The Authority imposed a fine of EUR 15,000 to the company for unlawful installation and operation of a video surveillance system and for the processing of the relevant material.

DECISION 44/2019

Title: Processing of personal data in computer infrastructure (material and server software) without abiding by the principles of Article 5(1) GDPR and 6(1) GDPR and in particular in breach of the security principle

Summary:

The audited company processed personal data in a computing infrastructure (material and server software) without abiding by all the principles set out in Article 5(1) GDPR and 6(1) GDPR, but also in the context of any subsequent or further processing of the same personal data, it didn't demonstrate compliance with the same personal data. In addition, it violated the provisions of Articles 5(1)(a) and (b) and (2) in conjunction with Articles 24(1) and (2) and 32(1) and (2) GDPR on the principle of safe processing (in particular of 'confidentiality') by failing to take appropriate technical and organisational measures, particularly those relating to the physical and logical separation of hardware, software and data in order to illegally copy the entire server content.

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