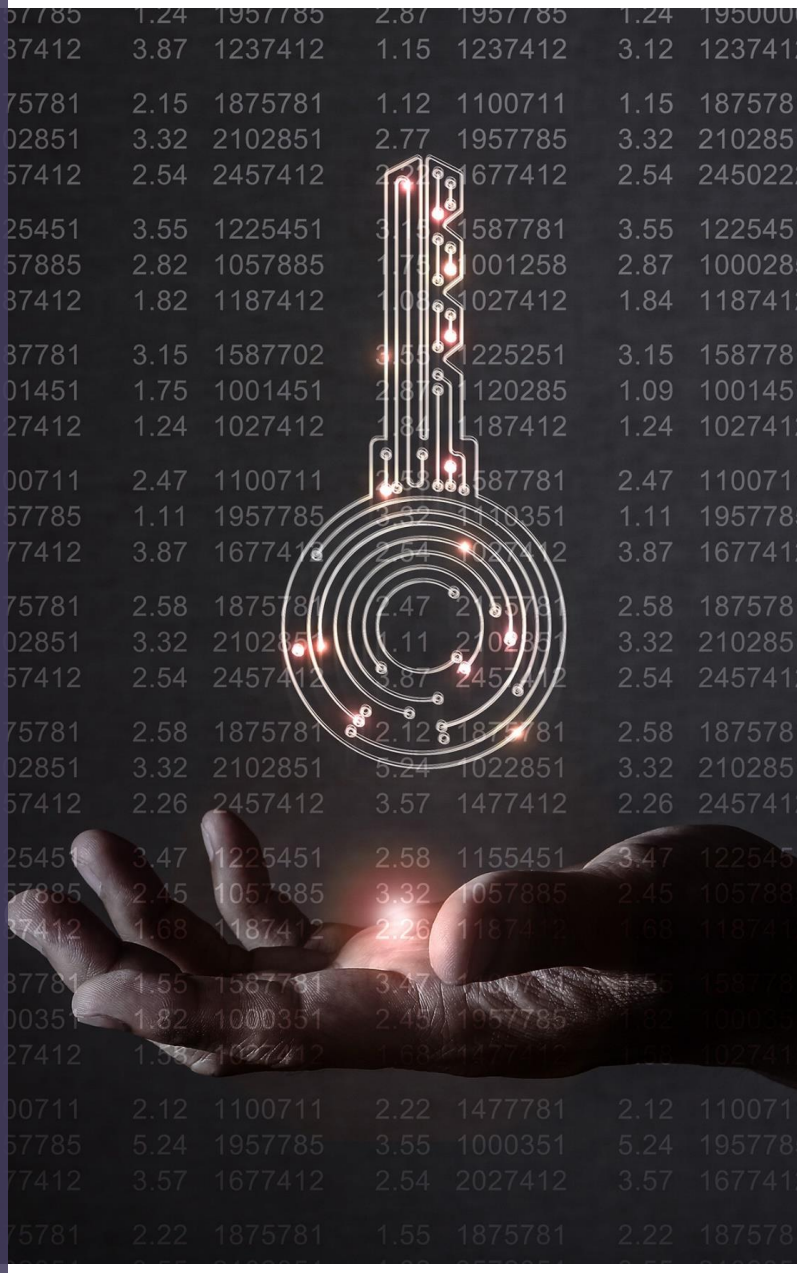
CottGroup®
Holistic Business Services

VeriSistem
a CottGroup® company



KVKK & GDPR NEWSLETTER

SEPTEMBER 2020

DECISION SUMMARIES OF THE MONTH AND NEWS

Appointment of the Same Natural Person as Contact Person for More Than One Data Controller Residing Abroad

Decision Number: 2020/542 **Date of Decision:** 16.07.2020
Summary of the Topic: Board Decision on the request of the same natural person to be appointed as contact person for more than one data controller residing abroad

As it is known, a contact person can be assigned only for one data controller during the fulfillment of the registration obligation to the Data Controllers' Registry Information System (VERBIS). In other words, a contact person cannot be assigned for more than one data controller at the same time. In addition, a data controller can only appoint one contact person.

However, it is possible that persons to carry out the work and transactions related to the registry listed in the Article 11 of the By-Law on the Data Controllers' Registry on behalf of data controllers residing abroad, who are specialized in the legislation on the protection of personal data and able to communicate with the data controllers located abroad, who will perform the duties of updating in VERBIS and providing communication with the Authority and data subjects on behalf of the data controller, to be appointed as the data controller representative by more than one data controller residing abroad.

In this regard; due to the fact that the main addressee who will provide communication with the Authority and data subjects on behalf of the data controller residing abroad is the data controller representative and the contact person will only carry out VERBIS transactions, the Board approved the appointment of a person as a contact person for more than one data controller residing abroad.

In addition, the Board has decided that the appointment of a person by more than one data controller residing in Turkey is not appropriate, which was a query raised. The justification of the Board regarding the subject has been explained as the necessity of closely monitoring the data controller activities, since the contact person appointed by the data controller residing in Turkey has duties such as communication with the Board and data subjects, having accurate information about the data inventory and the activities of the data controller, and fulfill the updates in VERBIS within 7 days when necessary.

The Personal Data Protection Authority Published the Decision Summary on Personal Data Transfer to Abroad Pursuant to the Convention no. 108

Decision Number: 2020/559 **Date of Decision:** 22.07.2020
Summary of the Topic: Board Decision on Personal Data Transfer to Abroad Pursuant to the Convention no. 108

The Authority launched an investigation upon the complaint made by the data subject about a SMS, sent by the data controller who is a player in the automotive industry.

The data controller explained in its defense statement that it uses a web-based software in its digital market communication; therefore customer data are transferred to the Outsourcer party, for the purpose of using a cloud database whose servers are located in a European Union member state, for sending SMS or e-mails to the customers; that transferred data include their customer data, marketing data and communication data; that their explicit consent has been obtained for the said transfer by means of an explicit consent form, which has been updated since 2018; that the Outsourcer has been processing the data in its capacity as the data processor on legitimate grounds as described in the KVKK.

The Company further argued in its defense statement that Paragraphs 5 and 6 of Article 9 of the KVKK are reserved; that the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the "Convention no. 108" or the "Convention") was a duly implemented one; that pursuant to Article 90 of the Constitution, the Convention was put into effect, and is a duly adopted convention dealing with fundamental rights and freedoms and therefore in case of a discrepancy between the Convention and the applicable laws, the Convention should prevail; that pursuant to Article 12 of the Convention, it is among the express rules of the Convention that data transfer as between Contractual parties should not be prohibited or subjected to special permission unless otherwise is expressly stated therein; that it was pursuant to the Convention that no restriction whatsoever or any attempt for special permission was made for data transfers from Turkey.

The Company further stated that pursuant to the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows", which supplements the Convention, it is prescribed that in case of cross border data transfer between states, adequate level of protection shall be assessed in case of a transfer to a country that is not a Party to the Convention; that considering the fact that this provision is applicable to any State or organization that is not a party to the Convention, an assessment for an adequate level of protection may not be applied for States that are parties to the Convention; that our country does not have any reservation whatsoever with regards to this provision of the Protocol in question; that consequently, the Company proceeds with data transfer by taking all administrative and technical measures on the basis of the relevant legal grounds set out in Article 12 of the Convention with reference to Paragraphs 5 and 6 of Article 9 of the KVKK and in Paragraph 2(f) of Article 5 of the KVKK with reference to Paragraph 2 of Article 9 of the KVKK ("if it is mandatory for the data controller to

process data for its legitimate interests ("legitimate interest") provided the fundamental rights and freedoms of a data subject are not prejudiced).

In this respect, the Authority noted that a two-stage test has to be applied to proceed with the "legitimate interest" basis; that the first stage concerns the determination of the legitimate interest while the second one concerns determination of whether this legitimate interest is prejudicial to the fundamental rights and freedoms of the data subject; however that the Company has not described the legitimate interest which underlies the data transfer abroad and has not indicated if the balance test in question regarding this legitimate interest has been performed; that therefore the Authority has come to the conclusion that there is no valid legitimate interest here.

The Authority stated that the Company gives the impression in its privacy and explicit consent statements, provided to the data subjects, that their personal data is processed merely based on their explicit and substantial consent; however, the underlying legal grounds on which the said data was processed are legitimate interest in addition to the explicit consent; that moreover, the said text states that there is "purpose for disclosure to outsourced third parties to ensure sending messages and e-mails" but there is no indication of a possible transfer to a company based abroad; that besides, it was not clear in the text in the first place as to which data are transferred abroad and on the basis of which legal grounds.

With respect to defense arguments relating to the Convention no. 108, the Authority noted that the said Article 12 of the Convention prescribes that a Party shall not, for the sole purpose of the protection of privacy, prohibit or restrict the special authorization transborder flows of personal data; that the purpose of that Article is to facilitate data flow based on the assumption that members to the Convention would already apply an adequate level of protection; that the Article does not impose a requirement that transborder data flow between member States shall be subject to a notice or a specific legal prohibitions. The Authority further contended that in light of the GDPR provisions and practices, being a party to the Convention no. 108 is only one of the criteria in the assessment of adequacy but does not necessarily mean that it provides for the adequate protection.

In addition to the foregoing, the Authority argued that for the purpose of evaluating permissions to data transfer, certain other factors should be taken into account as well in addition to the conventions to which States or organization are parties, including the purpose and duration of processing the personal data to be transferred, data protection legislation and practices in force in the jurisdiction for the intended data transfer, and the data controller who is the intended recipient or measures to be undertaken by the data processor or other measures intended to protect data as well as the status of reciprocity between the intended country and Turkey.

As for Article 90 of the Constitution, the Authority noted that the principle that an international convention shall prevail in case of a conflict between applicable laws and international conventions is valid only for conventions that are sufficiently clear, conclusive, unconditional and whose implementation does not require the state to adopt additional measures; that in case of a conflict between a rule of law and a more abstract and the provisions of a general international treaty that is not directly applicable, one cannot talk about the conflict as described in Article 90 of the Constitution, and therefore, that Article would not be applicable; that for this reason, the rule of law should prevail in case of a potential discrepancy in relation to the provisions of an international convention with a general purpose; that notwithstanding the foregoing, the Convention no. 108 is not directly binding on the states that are parties to it but rather lays down

basic principles, procedures and terms; that such principle in Article 90 of the Constitution which requires that provisions of a convention shall prevail in case of a conflict shall not be applicable here in face of the fact that the Convention provisions are not directly applicable.

The Authority emphasized that the Company has failed to provide the Authority with any piece of information that it has prepared or will prepare a letter of undertaking whatsoever despite its allegations that it transfers data based on the Convention no. 108 and one legal grounds of legitimate interest.

The Authority noted that the Company should either delete or destroy data, given the fact that it has failed to obtain a valid consent or perform the balance test which is requirement by the legal ground of legitimate interest or fails to draft a letter of undertaking in respect of cross border transfers and to obtain the consent of the Authority.

Lastly, the Authority stated that the Company's disclosure and explicit consent texts have failed to meet the requirements set out in the Communique On Principles And Procedures To Be Followed In Fulfillment Of The Obligation To Inform. They have not been elaborated as per the details of processing activities and were only stated to be transferred, without mentioning that the transfer is to be practiced cross borders and the data subject is not made fully aware of the granted consent along with the purpose and consequences of the provided consent. Overall, it has been made clear that the Company has failed to pay adequate attention and care in its efforts to ensure compliance with the Communique.

Consequently, the Authority decided that a fine in the amount of 900,000 TL should be imposed on the Company on such grounds that it has committed unlawful personal data processing operations regarding cross-border transfers; that the Company is also required to delete or destroy all data and that privacy notice obligation should be separate from the obligation to obtain explicit consent.

Board Decision Concerning Housing Estate Managements in Line with the KVKK No. 6698 and the Condominium Law no. 634

Decision Number: 2020/560 **Date of Decision:** 22.07.2020
Summary of the Topic: The summary of the Board Decision made in connection with the Housing Estate Managements in line with the Condominium Law no. 634 and the Personal Data Protection Law no. 6698

According to the decision made upon an examination by the Authority *ex officio* as well as upon a complaint filed with the Authority about the management of a Housing Estate:

• According to the Condominium Law, the unit which controls the entire real estate represents the condominium owners committee, as for the duties of the manager, decisions made by the condominium owner are decisive; the manager represents the condominium owners committee and the committee is also required to audit the works of the manager; it is the condominium owners committee which has control and command over the real estate; managers are not indispensable but a condominium owners committee should exist at all times and this is a committee that is formed due to ownership right;

• However, it is observed in the relevant Supreme Court decision that, because condominium owners committee lacks the capacity to sue or to be sued and does not have a legal personality, it fails to meet all criteria set out in the definition of a data controller according to the Law no. 6698;

• However, for matters concerning the entire main property, it has the authority to accept legal notices by means of the manager or professional service providers in this respect.

• Therefore, in light of the explanations above, the definition of a "data controller" should be interpreted broadly and even if a condominium owners committee lacks legal personality, it may qualify as a data controller for apartment buildings, housing estates and similar structures;

• It has been stipulated in the decision dated 22.07.2020 numbered 2020/560 that a condominium owners committee should hire and appoint such persons who shall assume and fulfil the tasks of a data controller after the committee determines the units which shall make decisions in respect of personal data processing in each case and which will set up, keep and manage a recording system.

The Decision in a Case Where the Father of an Data Subject Who Is A Minor Applies to the Data Controller for the Destruction of the Medical Report of that Data Subject

Decision Number: 2020/622 **Date of Decision:** 11.08.2020
Summary of the Topic: The Authority pronounced a decision in a case where the father of underage data subject applies to the data controller and because data controller fails to receive a response, the data subject himself files a complaint with the Authority

The father of underage data subject applied to the data controller for the destruction of the data subject's medical report but as the data controller did not give any response, the data subject himself filed a complaint with the Authority.

Thereupon, the Authority determined if the underage data subject would be eligible to file a complaint with the Authority and given that the applicant to the data controller is different from the applicant to the Authority, whether due to this the complaint fails to meet the formal conditions required under the applicable law. Accordingly, the Authority reported the following:

• Rights regarding the protection of personal data are firstly among constitutional rights and they are also governed in the Law numbered 6698;

• According to the Civil Code numbered 4721, underage people who have mental competence not obliged to obtain the consent of their parents or guardians in exercising their rights strictly attached to the person,

• According to Law numbered 4721, rights that regarding the protection of personality which constitute the subject of the litigation, may be exercised by the underage people or by his parent on behalf of him;

• On the other hand, according to the Regulation on Personal Health Data, parents may have access to the healthcare records of their children via e-Pulse system without any need for approval unless the underage person requires otherwise.

In light of the foregoing comments:

• On the condition that the underage person has mental competence, both the data subject and his guardian shall have competence to exercise the underage person's right in respect of both the application made to the data controller and the complaint filed with the Authority, given the fact that their wishes wills match. In the present case, the application by the father of the data subject to the data controller as well as the complaint filed by the data subject to the Authority were both accepted and an investigation has been launched.

Board Decision for the Use of Biometric Signature Data

Decision Number: 2020/649 **Date of Decision:** 27.08.2020
Summary of the Topic: The decision on the use of biometric signature data in line with the Personal Data Protection Law no. 6698

Upon request for an advice about whether or not secure electronic signature referred to in Articles 14 and 15 of the Code of Obligations no. 6098 falls within the scope of sensitive personal data as referred to in Article 6 of the KVKK no. 6698 and whether or not the provisions in the Code of Obligations constitute a basis for such legal grounds of "expressly prescribed in the laws":

• A biometric signature qualifies as a biometric data because an analysis of it reveals certain unique dynamic characteristics which are inherent in the signature, including the amount of pressure exerted when one affixes biometric signature, the speed and acceleration of the pen, the formation of letters, the angle of the signature and other similar personal unique characteristics;

• In order to process such data, an explicit consent should be obtained from data subjects or to fulfil the conditions set out in Article 6;

• Article 15 of the Code of Obligations no. 6098 does not contain the prescription required as sought in the Law no. 6698 and therefore the matter of secure signature should be governed in a special Law;

• In light of the foregoing, the Authority has decided that biometric data may be processed only subject to explicit consent and privacy notice requirements and by applying such appropriate published security measures concerning sensitive personal data.

Public Announcement on VERBIS Registration Obligation

As it is known, the periods during which natural and legal persons who process personal data should be registered in the Data Controllers' Registry (Registry) were announced by the Turkish Personal Data Protection Board (Board) in accordance with the Law on the Protection of Personal Data (KVKK) numbered 6698.

According to the data obtained from the Ministry of Treasury and Finance by the Turkish DPA for 2019, it has been found that there are data controllers who have not applied to the Data Controllers' Registry Information System (VERBIS) yet or have not completed their notification as of 01.10.2020, although they have more than 50 employees annually or a total financial balance of more than 25 million TL annually.

As a result of the examination and evaluation made by the Turkish DPA based on this determination; considering that some data controllers have not been able to fulfill their obligation to register with VERBIS due to actual, technical or legal impossibility within the scope of the fight against COVID-19, it has been deemed appropriate to inform the data controllers with a letter who have not fulfilled the obligation to register with VERBIS within the framework of the power given to the Board.

The relevant data controllers are required to fulfill their VERBIS registration obligation within the period notified to them by the Board with the said letter.

In addition, the Board announced that data controllers can continue their registration process without waiting for a letter from the Board.

To sum up, data controllers are expected to fulfill the registration obligation within the prescribed period of time in line with the letter sent by the Authority. VERBIS registration processes are also currently ongoing.

Yalova Municipality Data Breach Notification

According to the data breach notification made by Yalova Municipality, it is reported that the data breach took place between 01:00 - 09:00 on 30.08.2020 and was detected at 09:00 on the same day, due to the malfunction of certain servers,, files were encrypted with the use of ransomware as a result of work on servers by the Municipality and it is detected that there is a restriction in access to citizen information in the database, there is no data flow to the outside in servers and firewall reviews, the number of people affected by the data breach could not be identified at this stage. The investigation is still ongoing and the affected data from the breach are

the identity, location, customer transactions, financial, and operational data of employees, users and customers.

The said breach was published on the website of the Authority on 03.09.2020 and the investigation on the subject continues.

PSL Elektronik San. ve Tic. A.Ş. Data Breach Notification

According to the data breach notification made by PSL Elektronik San. ve Tic. A.Ş. to the Authority, it is reported that the data breach occurred at 01:00 on 20.09.2020 which has been identified at 08:00 on 21.09.2020 and due to the software running on the server and the files produced in the software are encrypted, the exact number of people affected by the breach is not clear, the affected data subject categories by the breach are customers, prospect customers and employees and affected personal data categories by the breach are identity, finance, personnel, customer transaction, communication, marketing, legal actions and professional experience, in addition race and ethnicity as a sensitive personal data.

The data breach in question has been published on the website of the Authority on 24.09.2020 and the investigation on the subject continues.

Polish Data Protection Authority imposed a fine of 100,000 PLN on Polish General Surveyor

The Polish Data Protection Authority deliberately fined the General Surveyor ("GGK") 100,000 PLN for violating the lawfulness principle and deliberately making public the land registry number data obtained from the land registries at GEOPORTAL2 (geoportal.gov.pl) without a legal basis.

In addition, it was noted that GGK needs to ensure GDPR compliance by restricting access to the personal data via the said Portal.

Furthermore, it has been stated that the Authority launched necessary audits in March 2020; however, GGK prevented such examination to determine if posting such land registry number data on the said Portal was lawful; that during the audit, GGK only applied administrative measures to ensure data security and the appointment of DPO.

Although GGM rejected the audit, it submitted an evidentiary affidavit in the trial in this respect. According to the statement presented, it was stated that the GGK published the information, including the land registry numbers obtained from the title deed ownership records, solely based on the agreements made with them.

It was stressed that pursuant to Article 5(1)(a) of the GDPR, data processing should satisfy the requirements under Article 6 of GDPR in order to ensure compliance with the law, rules of honesty and principles of transparency and lawfulness.

During the audit, GGK did not show any legal grounds; that moreover, there was no legal basis which was defined in the statutory regulations applicable to the Surveyor for making data available for public in respect of the said operation; that besides, according to the opinion of the President of the Authority, the Surveyor who was aware of this lack of legal grounds made an agreement with data subjects to legitimize its operations.

The Authority noted that the agreements with data subjects were intended to lay down and maintain common elements of a technical infrastructure in order to store and make available specific data filing systems; however it did not represent a legal basis or ground to make data available for use, including land registry numbers.

This way, the Agency decided that GGK violated Articles 6(1) and 5(1) of the GDPR as it made personal data available for use via its public registration system without any legal basis.

Notwithstanding the foregoing, it was finally noted by the Authority that data disclosed via the said Portal included names, surnames, parent names, ID numbers and property address; that these data allowed verification of the identity of an individual and that they could be acquired by anyone using the Internet; that this would expose many people to inadvertent consequences.

In its decision to impose a fine, the Authority took into account not only the seriousness of the violation but also its nature, duration and whether or not there was any commitment in relation to the purpose.

Polish Data Protection Authority imposed a sanction on a School for Processing of Students' Data Through Survey

Polish Data Protection Authority imposed a sanction on a school which processed the data of students for the intention of a survey; aiming to have an insight on the environmental conditions (for schools and houses) specific to the 2019/2020 academic year, without a legal ground.

It was reported that data collected by the school by means of the survey included names and surnames of the children, including those of minors, details of courses attended by them, whether their parents were living alone or in a family, they are alive or dead, their employment, income status and health conditions, their dependency, the number of household members, the condition of the house and social benefits. Besides, the data processing took place in the form of collection, storage and destruction.

Following an examination carried out by the Authority, it was revealed that the survey was made by classroom teachers among students in grades 7 and 8 and high school students in order to determine students who needed psychological support and that the survey was made following an instruction given by the school principal.

The notice of breach stated that survey documents were not recorded anywhere, including electronic mediums and that such data were not processed in anyway as of the date on which the survey was made by teachers; that survey organization was designed in a manner to prevent the disclosure of the resultant data.

It was stated that as a result of the survey, the school breached the principle of "lawfulness"; that the school was required to process data to perform its obligations and tasks defined in the Educational Law by considering that as a public agency, the school was entitled to process data whilst performing its tasks defined in the applicable law; however that the said laws do not call for or define any such task or obligation.

Accordingly, the Authority reported that the sanction was appropriate because the breach was without wilful misconduct and that the school immediately took corrective steps to address the breach, such as destroying the questionnaire forms, organizing awareness studies, analyzing the results of the violation and determining the risks. Finally, it was stated that there is no indication that any damage occurred as a result of the violation.

Hungarian Data Protection Authority penalized the publisher of the Hungarian edition of the Forbes in the amount of 4,5 Million Forint

Hungarian Data Protection Authority imposed administrative penalty fine of 4.5 million Forint to Mediarey Hungary Services Zrt., the publisher of Hungarian Forbes, for failing to abide the privacy notice responsibility towards data subjects and failing to make the required legitimate interest assessment.

The Authority noted in its decision that the Publisher failed to make the legitimate interest assessment (balancing test) in its "the richest 50 Hungarians" publication in February 2020 and in the "biggest family companies" publication covered by the magazine in September 2019 and omitted to inform the data subjects about the outcome of its legitimate interest assessment, violating Paragraph 1(f) of Article 6 of the GDPR in this respect.

Moreover, the Authority announced that Articles of 5(1)(a), 5(2), 12(1) and (4), 14, 15 and 21(4) of GDPR were violated as the Publisher failed to provide data subjects with adequate information in advance about the consequences of data processing and their right of objection, and it also failed to inform data subjects who have filed complaint about the exercise of their rights upon their applications.

Considering these violations, the Authority instructed the Publisher to provide data subjects with information about the interests of the Publisher in processing data, the consequences of the legitimate interest assessment and the right of objection as well as the fact that they can exercise their other rights and to proceed with a legitimate interest assessment in line with the applicable legislation and decisions and to update its practices to provide information in advance in line with the applicable regulations and decisions.

The Authority also noted in respect of September 2019 publication that despite the exercise by data subjects of their right of objection to the processing of data, the Publisher continued to process data and it failed to demonstrate in response to their objections that it has a legitimate interest that prevailed over the interests, rights and freedoms of the data subjects. According to the Authority, this was a factor that aggravated the fine imposed by it in relation to the said publication.

The Authority emphasized that Forbes can make lists of business life data in reliance of data that is accessible to the public but the publication of these lists is subject to GDPR requirements; that in its capacity as a data controller, the publisher is required to meet such requirements.

Finally, the Authority noted that it supports the publication of lists which are exhibited in the Hungarian market, which do not include the details of the relevant persons or include minimum amount of information about them but which do not contain information such as the relevant industry of data subjects, their names and surnames and their assets value.

Polish Data Protection Authority Fines Warsaw University of Life Sciences

In November 2019, portable computer for private usage, of a university employee who used it for business processes was stolen and President of Polish DPA had notification of data breach about personal data of candidates. After the examination, President of Polish DPA has started administrative proceedings.

Based on the evidence collected during the proceedings, President of Polish DPA imposed an administrative fine on the University. While DPA decided the amount of the fine, it considered a wide range of data which was breach, the number of persons who affected and data controller has not had knowledge of the processing of personal data on the employee's private computer. In addition, Authority reported that, these conditions show that confidentiality and accountability principles of GDPR's was breach.

There is worth to noting the university had specified retention period of personal data for candidates as three months upon recruitment process. However, reported that the personal data of candidates from five years were kept and processed, regardless.

The Authority has reported the measures which taken by the university were insufficient and the Data Protection Officer (DPO) did not consider the risks with data processing operations and fined 50 000 PLN.

Norwegian Data Protection Authority Imposed a Fine of 37.400 EUR on the Norwegian Public Roads Administration

Norwegian Data Protection Authority fined Norwegian Public Roads Authority a sum of 37,400 EUR for conducting a data processing activity that is not compliant with the original purpose and followed by the failure to delete the video records within 7 days.

To provide some further context on the incident, the fixed road cameras were used to watch employees, sub-contractors and the subcontractor's employees along with the other contractual parties where as per the this observation, data processing activities were carried out. It was noted that the use of such photographs to document contractual violations prior to the breach was not consistent with the original (main) purpose for using camera records which would be used to take emergency security measures in the first place. Therefore, it was stressed that these video records may not be used to monitor contractual relations.

In the evaluation of whether the purpose of the subsequent data processing activity is compatible with the original purpose, the Authority found that the new processing in question creates a disadvantage for the contracting parties and their employees, therefore it contradicts the expectations of the contracting parties, who are the relevant persons, regarding personal data processing.

Finnish Data Protection Authority imposed a Financial Sanction on a Company for Carrying Out Electronic Marketing Without Obtaining Prior Consent and by Violating Rights of Data Subjects

Finnish Data Protection Authority imposed a penalty fine to Acc Consulting Varsinais-Suomi for Sending electronic direct marketing messages without obtaining prior consent leading to the violation of the rights of data subjects.

According to the decision, in their complaints filed in 2019, data subjects stated that they have been receiving direct marketing messages without their consent; that pursuant to Article 4(11) of the GDPR, a consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes.

In addition, certain complainants were submitted by replying the SMS messages received to stop receiving messages; but the text messages still continued to be received which led the data controller fail to enforce data subject rights.

It was alleged by the Company that it carries out electronic direct marketing to entities therefore the legal requirement of prior consent has not been a subject for their organization; the phone numbers the text messages sent to our used by entities own staff and within this scope, the companies fall within its intended customer segment.

Notwithstanding the foregoing, the Authority stressed that the Company should have enquired about the position of data subjects prior to direct marketing operations, and in particular, it should have considered if the contents of marketing were substantially related to their tasks. It was underlined that for this reason, one may not assume that the Company's marketing efforts were intended for companies because it actually targets individuals and that it should have obtained prior consent.

Accordingly, the Company received a reprimand for its processing activities without a consent, and it was instructed to correct its direct marketing efforts targeting companies.

It was stated in the decision that the Company did not respond to the requests of data subjects and failed to prove the legal grounds underlying its personal data processing activities. The Authority imposed a sanction on the Company on such grounds that it failed to give a response within 1 month in respect of data subject rights; that it has failed to keep application records and that it thus fell short of implementing the appropriate organization measures to protect the data subject rights.

The institution also took into account the fact that this violation was committed without willful misconduct; it also noted the number of similar violations that took place in a very short period of time, the Company's indifference in cooperating with the Authority and the fact that it failed to demonstrate that it enforces data subject rights and has taken corrective measures about direct marketing. Therefore the Authority fined the Company a sum of 7,000 EUR on top of corrective measures. The decision made it clear that the fact that data subjects have not sustained any financial loss was a mitigating factor in determining the ultimate fine.

INFORMATION GUIDE

Administrative Measure: Information Obligation and Transparency Principle under the GDPR and the KVKK

Within the personal data processing activities, a data controller should be transparent in its relations with the data subject. Data subject should be given a clear, understandable and honest information about the aspects of the data processing operation. This principle applies to all rights and obligations under the applicable laws as it affects all processing operations by the data processor. This concept, referred as “transparency” in international literature, manifests itself in the privacy (information) notice obligation of the data controller in national literature.

Article 5 of the GDPR introduces 7 basic principles in data processing. These principles, including transparency, are the principles that encompass the processing of personal data within legal limits and shape up the data protection regime. These principles may only be restricted by those laws to be enacted by Member States of European Union provided that they are necessary and proportionate in the democratic social order without interfering with fundamental rights and freedoms.

Pursuant to Article 5 of the GDPR, personal data should be processed lawfully, fairly and transparently. Lawful and fair processing was already addressed in international regulations prior to GDPR and regulations concerning transparency completed the last leg of these three principles. In other words, these three principles are inseparable. According to the general acceptance in the European Union Law, if data controller processes data unlawfully or unfairly, it will be deemed to have violated all these principles.

Transparency means being clear and honest in all data processing operations from end to end. According to this principle, each and every information about data processing operations should be easily accessible, understandable and be expressed in a plain language. Individuals should be informed about which data are collected and processed while they should be entitled to have access to any information about the identity of data controller, the purpose of data processing as well as any data supporting the fact that processing is carried out fairly and transparently.

In its relations with data subjects, it is mandatory for a data controller to prove that it is transparent at all times. In a data protection regime, the reason why a data controller assumes such an obligation is the fact that this principal is vital for data subjects to exercise their rights. If individuals are aware of the purpose of processing of their data and the possible consequences of such processing in advance, they may evaluate whether or not they wish to be a part of this processing, and may make better informed decisions as they will be able to negotiate the terms of processing. Also, an informed consent enhances the accountability of a data controller.

Transparency is also critical in circumstances where data are not derived from data subjects because in such circumstances, data subjects will not be aware of the processing of their data and will not be in a position to exercise their such rights.

Each privacy notice to be provided in line with the transparency principle:

- should be plain, transparent, understandable and easily accessible.

- should be written in a plain and clear language.

Data subject should not be forced to search for his data.

It should be clear from where and how to access all information regarding data processing activities. As the information will be directly transmitted to the data owners; The relevant persons can be directed to an online platform where privacy principles are available or they can be informed digitally with an interactive chatbot interface.

When a data subject is informed, complex sentences should be avoided and a plain language should be used as much as possible. Information supplier should be specific and firm; an ambiguous, self-contradictory and open-ended language should not be allowed. For instance, the following sentence is not clear about what kind of services are entailed and the benefit the author is talking about: “We may use your date to improve our services”. Similarly, the following sentence is not clear about the type of research: “We may use your data for research purposes”. In the following sentence it is not clear what the personalization process entails. “We may use your data for the purpose of offering you personalized services.”

In our country, both regulations and practices follow international law. Principles defined in European legislation have found their ways into Article 4 of the Law; it states that the article is based on the Convention no. 108 and the Directive no. 95/46/EC, which is the draft form of GDPR.

It should be noted that principles of lawfulness and honesty are identical to the ones governed in the GDPR. Transparency may not have been clearly defined in the KVKK but it manifests itself in the privacy notice obligations of a data controller. Pursuant to the privacy notice in Article 10 of the Law, data controller or its appointee shall be obliged to provide a data subject with the following information: Identity of data controller, or if any, its representative, the purpose under which personal data is to be processed, method and legal grounds to collect personal data and other rights listed in Article 11

Communique on Principles and Procedures To Be Followed in Fulfillment of the Obligation to Inform lays down the general framework. The transparency principle is enshrined in Article 5 of the Communique. Accordingly, while the privacy notice obligation is fulfilled, general and obscure expressions should be avoided. There should be no expression which gives the impression that personal data may be used for some other potential purposes. The notice to the data subject under such obligation should be drafted in a plain, clear and understandable language. Data subject should be given this privacy notice whenever its own data is processed.

Rabia Dağcı | Legal Consultant | Attorney | CIPP/E

Technical Measure: Usage Updated Antivirus Systems

According to Article 12/1 of KVKK, data controllers have to take all necessary technical and administrative measures in order to prevent unlawful processing of personal data, to prevent unlawful access to personal data and to ensure that personal data are stored in accordance with the law.

These measures are set out in the Personal Data Security Guide published by the Authority and specified during the notification stage on VERBIS.

One of these measures is the usage of up-to-date anti-virus systems.

The Data Security Guideline published by the Authority prescribes that in order to protect one's systems against malware, certain anti-virus and anti-spam products should be used to regularly scan the information system network and identify risks; that it would not suffice to merely set up these products as they need to be constantly updated to make sure that necessary files are regularly scanned.

Anti-virus programs should be installed and to be ensured to have it kept up to date to identify malware within the organization to ensure cyber-security.

Anti-virus software supports your systems to defend themselves against malware and cyber-crimes.

Anti-virus programs: scan, clean, save and protect the systems. These methods determine the operational speed and principles of anti-virus programs.

First of all, systems are scanned and certain embedded viruses such as Trojan and Key Logger viruses, are isolated. Thereafter such isolated software is deleted. During this deletion operation, data that are indispensable may be deleted; following the deletion, such data are recovered and restored back following this operation. The final stage is the continuing protection against malware that poses a risk for systems.

An anti-virus program may properly function only if it is constantly kept up-to date.

Technological advances lead to the creation of thousands of viruses every passing day. Anti-virus programs are updated to ensure system security against these newly devised viruses so that they are blocked, and systems are now safe from them.

Companies should not overlook the importance of using anti-virus programs to ensure cyber-security and the need to constantly update them, and should be aware of the fact that in case anti-virus programs are not used or the program in use is not up-to date, then this may be very detrimental to the organization in case of a possible breach or attack.

Kübra Özkahraman | Quality Assurance & Training Responsible

LEGISLATION ANALYSIS

The Processing of Sensitive Personal Data for a Valid Legal Reason and Adoption of Protective Measures at Adequate Level

KVKK Art.6 – Conditions for processing of personal data of special nature

(1) Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be personal data of special nature.

(2) It is prohibited to process the personal data of special nature without explicit consent of the data subject.

*(3) **Personal data, excluding those relating to health and sexual life, listed in the first paragraph may be processed without seeking explicit consent of the data subject, in the cases provided for by laws**. Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, by any person or authorized public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.*

*(4) **It is stipulated that adequate measures determined by the Board are also taken while processing the personal data of special nature.***

***

As it is known, sensitive personal data are subject to special protective measures and data processing conditions as per the Law. According to the Third Paragraph of Article 6 of the Law, sensitive personal data other than personal data related to health and sexual life may be processed only if the data subject gives his explicit consent and it is expressly prescribed in the law, meaning that unlike other ordinary personal data, it is not possible to process such data for the purposes of entering into or performing a contract, actual impossibility, performance of legal obligations, legitimate interest of data controller, assertion, use or protection of a right.

Sensitive personal data may be processed without the explicit consent of the data subject only if the processing is expressly prescribed in the applicable laws and it is understood from the applicable regulation that the processing of such sensitive personal data is necessary. For instance, this requirement is evident in the regulation in Article 67 of the Social Security and General Health Insurance Law no. 5510 as it stipulates that biometric data should be obtained in order to benefit from health services.

Another condition set out in Paragraph 4 of Article 6 of the Law in order to process sensitive personal data is the adoption of an adequate level of measures. Methods of taking these measures are described in the decision taken by the Authority on 31.01.2018 under no. 2018/10 as follows:

According to the relevant resolution, it is necessary to;

• Determine a separate manageable and sustainable policy and procedure for the security of sensitive personal data, which is systematic, and which features clear rules,

• With regards to employees who are involved in the processing of sensitive personal data;

• Provide regular trainings relating to the Law and the relevant regulations as well as security of the sensitive personal data,

• Execute confidentiality agreements,

• Define the scope of powers and terms in a clear manner for the users who are authorized to access the data,

• Carry out periodical authority checks,

• Immediately revoke the authorizations of the employees who are reassigned or quit the job, İn this regard, take back the inventory allocated by the data controller to that person,

• If the sensitive personal data are processed, retain and/or accessed electronically;

• Storing the data by making use of cryptographic methods,

• Keep cryptographic keys in safe and separate places,

• Logging transaction records of all the activities concerning the data in a secure manner,

• Continuously monitor the security updates relating to the media where the data is retained, regularly conduct/have conducted the necessary security tests, record the test results,

• In the event that data access is enabled by means of a software, give user authorizations for this software, regularly conduct/have conducted security tests of the software, record the test results,

• Set up at least a two-stage identity verification system, if remote access to data is required,

• If the sensitive personal data are processed, retained and/or accessed in physical media;

• Ensure that adequate security measures (against electric leakage, fire, flood, theft, etc.) are taken by taking into consideration the characteristics of the media where the sensitive personal data is retained,

• Prevent unauthorized entries and exits by ensuring the physical security of these places,

• If the sensitive personal data is to be transferred;

• If the data are to be transferred by e-mail, transfer the data in an encrypted manner, by using a corporate e-mail address or a Registered E-Mail Services (hereinafter referred to as “KEP”),

• If transfer is required by means of memory stick, CD, DVD, encrypt by using cryptographic methods and the keep the cryptographic key in a separate place,

• If transfer is made between servers in different physical environments, carry out the data transfer by establishing VPN between the servers or by means of sFTP method,

• If the data need to be transferred through paper, take necessary the precautions against risks such as theft or loss of the documents or being viewed by unauthorized persons and send the documents as “classified documents”.

Prepared By

Kübra Özkahraman

Mustafa İvgin

Onur İzli

Rabia Dağcı

Sevcan Livanur Sefer

Şeyma Kaplan

Şule Özcan

Suzan Tepe

Follow Us on Social Media ...