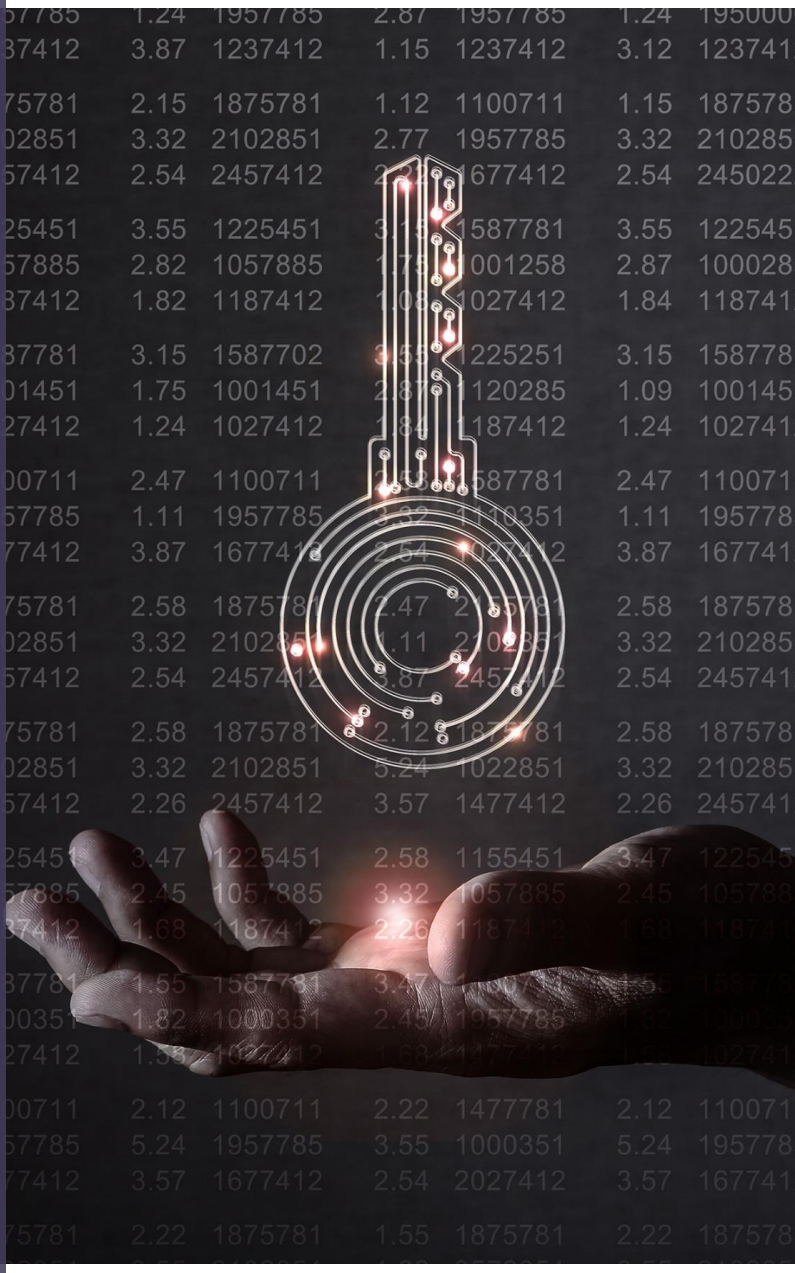
CottGroup®
Holistic Business Services

VeriSistem
a CottGroup® company



KVKK & GDPR NEWSLETTER

JANUARY 2020

DECISION SUMMARIES OF THE MONTH AND NEWS

A Penalty Fine of TL 100.000 Imposed by the Board on The Data Breach Realized In a Bank

Date of Decision: 26/11/2019 **Number of Decision:** 2019/352
Subject: Decision on the data breach in a bank

The Bank, which has made a data breach notification to the Personal Data Protection Board, detected that critical information of the customer, which are identity card, balance, identification, contact...etc. were sent by the bank employee to his/ her personal e-mail account and money was drawn from the customer's account with the obtained documents.

The Bank detected that the employee took out the data of at least 6 people out of the Bank and involved in fraudulent activities and provided benefits to himself/herself, and the number of people who were confronted data breach was 24. The Bank stated that due to his/her irregular actions, they terminated the employment contract with the staff and filed a criminal complaint with the Prosecution office and also compensated all the damages of the Bank's customers.

Within the scope of the decision, it was determined that the Data Leak Detection/Prevention System exists at the Bank, but there has been a personal data leak from the corporate e-mail that caused the break and this leakage could not be prevented.

As the technical measure taken by the Bank, if the e-mails with a number of cards above a certain number and the card number are sent out of the Bank, the method to put e-mails in quarantine has been overcome by malicious people.

For this reason, since the Bank was not able to prevent the leakage of information containing personal data, the Bank became an intermediary for high amount of fraud activity and could not prevent it.

For the above reasons, the Board imposed a fine of TL 70.000 to the Bank for not taking the necessary administrative and technical measures within the scope of data security in accordance with the provisions Article 12/1 and 18/1-b of KVKK; and for not complying with the notification obligation within the deadline of the period, imposed an administrative fine of TL 30.000.

Decision Regarding Publishing News on the Sensitive Personal Data of the Relevant Person by a Newspaper

Decision No: 2019/372 **Date of Decision:** 09.12.2019
Subject: Decision regarding publishing news on the sensitive personal data of the relevant person by a newspaper

As a result of the complaint made to the Authority;

- The relevant person shared that, in a newspaper containing a column about the father of the relevant person who has taken a break from her duty due to his/her father's cancer treatment, that the health data, which is sensitive personal data, is processed and shared with third parties without the consent of the relevant person,
- He has kept his illness from his son so that his psychology and morale are not disturbed due to his illness, after this news, the relevant person was called with get well wishes, having learned that he was ill, he was caught in fear of death and having learned his illness from the newspaper and third parties, turned into himself and rejected treatment, and requested legal proceedings to be carried out by the Authority.

Since it was concluded that the sharing of the sensitive personal data of the relevant person in a column without being based on one of the conditions listed in the Article 6 of the Law by the newspaper is contrary to the Paragraph 1/a of the Article 12, in the scope of the Paragraph 1/b of the Article 18, with the Board's decision dated 09/12/2019 and numbered 2019/372, it was decided to impose an administrative fine of TL 125.000 TL on the aforementioned newspaper.

Decision Regarding the Request for Opinion About Sharing the Candidate Points on the Website Without Obtaining Consent

Decision No: 2019/389 **Date of Decision:** 26/12/2019

Subject: Decision on the application of publishing information requested from the candidates on the internet which is personal data during the appointments to be made to the academic staff and research assistant staff

In the assignments to be made to the academic staff and research assistant staff, as a result of the examination of the request for the opinion made to the Authority about whether the sharing of the evaluation points with the public through the website of the data controller is in accordance with the Law;

Considering that the announcement which is published on the internet or physical media and contains personal data, is not beneficial for third parties to be known with all its elements;

It has been concluded that;

- Considering that the data published on the internet cannot be deleted completely, it should be announced in a way that the query can be made by authentication in such a way that it can only be viewed by data subjects applying to academic staff in accordance with the Article 4 of the Law;
- It is appropriate to remove the link between candidates and exam scores by masking method; accordingly, instead of removing the ability to make people identifiable and writing data clearly such as name, surname, Turkish identity number, certain parts should be announced by one of the masking methods, in a way that the candidates can understand,
- Disclosure should be made to data subjects by the universities regarding the related personal data processing activity in accordance with Article 10 of the Law.

Republic of Turkey Ministry of Health Published an Announcement about Verbis

As it is known, Data Controllers must register with the Data Controllers' Registry via VERBIS ("Data Controllers' Registry Information System") within the period determined and announced by the Board within the scope of the Law on Protection of Personal Data ("KVKK").

In this context, Republic of Turkey Ministry of Health, which is a legal person, has been admitted as the single data controller for public hospitals operating within the Ministry and the central and provincial offices, family practice centers, public and community health centers and such healthcare providers affiliated with the Ministry.

Therefore, the General Directorate will fulfill its obligation to register with VERBIS on behalf of the Ministry.

However, the obligation of all private health institutions to register with VERBIS will be done by their own private legal entities. Similarly, the registration obligations to VERBIS for the physicians operating a practice center, will be carried out by the related physicians.

Online Complaint Module Has Been Put into Service for Data Subjects

Pursuant to the following provision of the Article 15 of the Law *"The Board shall carry out the necessary examination on the matters falling within its task upon complaint or ex officio where it has learnt about the alleged infringement."*, complaints reported to the Authority are reviewed by the Board.

Complaints were used to be reported to the Authority via paper mail; as per the announcement of the Board dated 09.01.2020, the complaints can now be reported electronically via online module.

The data subject will be able to report complaint in person via complaint module by logging into the e-government system and the complaints to be reported through the attorney will continue as it is.

In addition, in accordance with the Articles 13 and 14 of the Law, as data subjects should apply to the data controller before submitting their complaint to the Authority; complaints that do not meet this requirement will not be considered by the Authority.

KVKK Complaint Module can be accessed at sikayet.kvkk.gov.tr.

In addition, the Authority published a guideline and presented the subject to the information of the data subjects. Further information on KVKK Complaint Module is available here.

Change of Application in Notification of Personal Data Breach to the Board

As it is known, in accordance with the Board Decision dated 24.01.2019 and numbered 2019/10, in case of a personal data breach, a notification should be made to the Authority by using Data Breach Notification Form as per the Board Decision.

According to the announcement made by the Authority on 06.01.2020, Personal Data Breach Notification that previously expected to be sent by paper mail can now be made on the internet at ihlalbildirim.kvkk.gov.tr.

System allows you to create a notification, query a previous notification and update the notification.

In addition, the Authority published a guideline and presented the subject to the information of data controllers. The Guideline on the Personal Data Breach Notification can be accessed here.

Penalty Fine Imposed to Archiving of Former Employee Personal Mails by the Hungarian DPA

A penalty fine was imposed to a company Hungarian DPA (NAIH) for illegal archiving of personal e-mails in the work e-mail of a former employee.

It is stated in the decision that personal e-mails of the former employee in the work e-mail should be deleted with active cooperation between the employer and the former employee and the employer has the right to make search in the archived mails about the job in the former employee account.

According to the decision, it is necessary to pay attention that the necessary notification should be made to the former employee, and necessary legal protections should be provided while using, archiving and searching business accounts. These transactions must have a legal basis. If there is no legal basis, any action taken will be illegal.

Due to the illegal archiving of the mails in the work e-mail of the former employee, NAIH (Hungarian DPA) imposed a fine of € 1500 to a company in Hungary as data controller.

A Fine of EUR 11.5 in Italy for Promotional Telemarketing Activities

The Italian Supervisory Authority imposed two fines on Eni Gas and Luce (Egl), a total of EUR 11,5 million, concerning respectively illicit processing of personal data in the context of promotional activities and the activation of unsolicited contracts. About 7200 consumers were affected by the said activities.

The first fine of EUR 8,5 million relates to unlawful processing in connection with telemarketing and teleselling activities as found during inspections and inquiries that were carried out by the Authority following several dozens of alerts and complaints received in the immediate aftermath of the full application of the GDPR, breaches include advertising calls made without the consent of the contacted person, the failure of EGL to take technical and organizational measures, longer than permitted data retention periods, and the acquisition of the data on prospective customers from entities (list providers) that had not obtained any consent for the disclosure of such data.

Misconduct by EGL made against the law was detected and announced by Italian SA. Italian SA has informed EGL that it is necessary to follow the procedures and systems required to verify the consent of those on the contact lists before starting telemarketing. In addition, the company's use of data provided by list providers was also banned as long as it does not have an additional approval.

It has been reported by Italian SA that, due to the conclusion of unsolicited contracts for the supply of electricity and gas under 'free market' conditions and contract and the invoices were made and issued with the previous supplier, and a new contract was not made. EGL forged the signatures of the data subjects and used incorrect data. For this reason, upon the complaints raised, the Authority imposed a second fine in the amount of EUR 3 million.

The Authority's findings showed that the conduct of Egl in acquiring new customers through certain external agencies operating on its behalf led, in organizational and managerial terms, to processing activities in breach of the EU Regulation as they violated the principles of data fairness, accuracy and up-to-dateness. In addition, Italian SA reported that the penalty should be paid within 30 days under the GDPR, due to taking the data of the data subjects more than necessary, continuity of misconduct, considering the duration of the breach and due to the economic situation of EGL.

Exeltis İlaç Sanayi ve Ticaret A.Ş. – Data Breach Notification

According to the data breach notification made by Exeltis İlaç Sanayi ve Ticaret A.Ş., the breach occurred as a cyber-attack caused by malicious software and ransomware, by obtaining the company's authorized user password, the affected persons by the violation are employees, users, customers and potential customers and the affected personal data are ID, contact details, location, personnel file, legal transaction, customer transaction, transaction security, risk management, finance and marketing information and there are also sensitive personal data affected by the breach which are information on health, criminal conviction and security precautions, the breach started on 11.01.2020 and detected on 12.01.2020, the estimated number of the persons affected by the breach is around 1000 and the exact number has not been detected yet, relevant persons can obtain information from IT Department help desk or KVKK Committee regarding the data breach via e-mail or telephone. The related data breach was published on the website of the Authority on 16.01.2020 and the investigation continues.

Penalty Fine Imposed to a Pharmacy in London Due to Careless Storage of Patient Data

A London-based pharmacy was imposed a fineof EUR 275.000 due to unsecure storage of sensitive personal data by The Information Commissioner's Office (ICO) in the scope of GDPR.

As it is known, the necessary care and attention should be taken in the storage of personal data and sensitive personal data. In this context, it has been detected that Doorstep Dispensaree Ltd, left approximately 500,000 documents in unlocked containers at the back of its premises in Edgware, where patient names, addresses, birth dates and health data were included.

In addition, documents dated between June 2016 and June 2018 were damaged in the container.

Since the unauthorized or illegal processing of the data, accidental loss, damage to the data, not being stored under proper conditions within the scope of GDPR constitutes a violation within the scope of the protection of personal data, the pharmacy was imposed a fine of EUR 275.000 by the related data protection authority.

Yahoo – Data Breach Notification

Yahoo, which is within the scope of GDPR, recently made a statement of violation. In the statement made, it was revealed that between 2012 and 2016, malicious people penetrated Yahoo's systems and stolen the data.

Within the scope of the breach that occurred from January 2012 to April, 2 different malicious people were logged into Yahoo 's system; however, in the light of the evidence obtained, it was not proved that they obtained users' information.

Then, in August 2013, a new data breach was encountered, and personal data (names, mailing addresses, birthdays, passwords; in addition, mails, calendars and contacts) of nearly 3 billion users stored by Yahoo were seized. By November 2014, another data breach was encountered, and it was detected that approximately 500 million users' personal data were seized worldwide.

From 2015 to September 2016, malicious people were able to reach 32 million Yahoo mail accounts thanks to cookies without the need for passwords.

If you have received a notice about Data Breach between January 2012 and September 2016, or if you have a Yahoo account and live in Israel or America, you can become a "settlement class member". Besides, Yahoo will continue to increase the Security of Personal Data stored in customers' databases and will pay the customers affected by the breach from the $ 117,500,000 settlement fund.

GET SUPPORT FROM EXPERTS
FOR YOUR DATA CONTROLLER SYSTEM REGISTRATION RECORDS

INFORMATION GUIDE

Interesting Topics

Administrative Measures: Disclosure Obligation and Explicit Consent

Disclosure is to inform data subjects by the data controller, or the person authorized, during the acquisition of the data as a rule, by using the data in a physical or electronic environment such as verbal, written, voice recording, call center. Explicit consent is a declaration of positive will about a particular subject, based on information and announced with free will.

One of the most important differences between disclosure and explicit consent is that explicit consent is a reason of compliance with the law; and disclosure is a liability. Namely;

Explicit consent is one of the legal terms listed in the law, and if the data processing activity is not based on any of the other legal requirements listed in Article 5 of the Law, the person must consent to the processing of his/her data. In cases where one of the other legal reasons exists, explicit consent will compare the data controller with the abuse of the right and an invalid explicit consent.

That means, explicit consent is one of the reasons for compliance with the law, which should be applied in cases where there is no legal reason, not in any case. For this reason, the data controller should determine whether the personal data processing activity is primarily based on a legal reason other than explicit consent, if this activity is not based on at least one of the legal reasons listed in the Article 5 of KVKK excluding explicit consent and if there is a legitimate aim, he/she should seek the explicit consent of the data subject.

In addition, the most important thing to remember about explicit consent is that the explicit consent of individuals must be obtained before starting data processing. Obtaining explicit consent after data processing begins will constitute a violation of the law. Besides, since giving explicit consent is an individual right, the explicit consent given can be withdrawn and the withdrawal declaration becomes effective as soon as it reaches the data controller.

Disclosure, on the other hand, is the necessity of informing the data subject, regardless of the legal reason for data processing. Data processing activity to be carried out with the explicit consent of the person or due to the performance of a contract, as stipulated by law, or if one of the other legal reasons listed exists, the person must be informed about the legal reason, for what purpose, by whom, in what way his/her data is processed, for which purpose the data is transferred to which parties and what his/her rights are. This information should be given before starting data processing activity or at the latest when data processing is started.

There is no need for the statement of positive will of the data subject for disclosure; it is sufficient for the disclosure to reach the data subject.

Explicit consent should be based on disclosure, while obtaining explicit consent of the person, explicit consent should be obtained by making disclosure to them on a particular subject.

Finally; explicit consent and disclosure should not be arranged in the same text and presented to the data subjects. The explicit consent text should be presented to the person in such a way that the data subject person can understand and his/her will is not injured for any reason. Otherwise, the declaration of consent issued within in the disclosure text will not be a valid explicit consent.

Differences Between Disclosure and Explicit Consent

Explicit Consent	Disclosure
Statement of the positive will of the data subject is required.	It is sufficient for the disclosure to reach the data subject.
It is the reason for compliance with the law.	It is one of the obligations stipulated by the law.
It is a reason to be consulted when there is no other reason for compliance.	It is necessary to make disclosure to the data subject for all legal reasons.
The explicit consent of the data subject must be obtained before starting the data processing.	Disclosure can be made at the latest when data processing begins.
All elements take place in the disclosure are also included in the explicit consent, because explicit consent is based on the disclosure.	Not all elements of explicit consent are applied for the disclosure.

Technical Measure: Keeping a log

According to the Article 12/1 of the Law on the Protection of Personal Data ("KVKK"), data controllers are obliged to take all necessary technical and administrative measures to prevent personal data from being processed unlawfully, to prevent personal data from being illegally accessed and to ensure that personal data are kept in accordance with the law. These measures are elaborated in the Personal Data Security Guide published by the Authority and specified during the notification to VERBIS.

First, it should be learned what the Log Records and Access Logs subjects in the Technical Measures table in the Personal Data Security Guideline mean and be aware of what technological solutions can be utilized in regard to these issues.

Log is the automatic generation of events related to a particular system and documentation with a time stamp. Logging (keeping a log) is the process of storing digital movements through records. For example; it is recorded on which date, at what time, with which IP address, which website is entered is recorded on the internet accessed through the firewall. Keeping a log, is not only made through the firewall, but many software, hardware and similar systems.

Although it is mentioned in the guideline published by the Board that the necessity of keeping the transaction logs of all users regularly, this requirement has already been made compulsory for the business organizations with the Law numbered 5651 (Law on the Regulation on Procedures and Principles Regarding the Regulation of Broadcasts on the Internet) which came into force in 2007. Organizations are responsible for keeping the transaction logs of users independently from KVKK in accordance with the law numbered 5651.

In accordance with this law enacted for the detection of crimes committed over the internet, in the event that organizations share a content that can constitute any crime by using the internet network, the identification of the person performing the transaction and reporting to the authorized institutions and organizations can be provided with log records. As per the relevant procedure, disclosure should be made to persons regarding the subject, whose records are kept in accordance with the KVKK.

Organizations may not notice their attacks for a long time or may be late for intervention, in order to prevent this situation, it is necessary to regularly check all the movements and events on the network and to act on the warnings from these systems and take relevant actions. SIEM (Security Notification and Event Management) solutions can be used to track these processes. SIEM monitors the behaviour of the systems and provides reports by analysing the logs.

Namely, when someone tries to log in to the firewall of the Organization with SIEM, the log produced by the firewall is transferred to the SIEM and action can be taken by the firewall with a rule to be written in SIEM. With the written rule, it can be provided to intervene the firewall by taking the action of "block that IP address if it tries to log-in more than 3 times over the same IP address". In this way, SIEM can interfere with the events and analyse the behaviours without interfering with any additional action. For example; If a user who is not authorized to write to the folder named Human Resources in your file server tries 3 times in 60 seconds, it can be provided to generate an alarm, and an e-mail can be sent to the unit manager by the system.

This issue should be given importance since the biggest deficiency of organizations in the face of cyber-attacks is not being able to have adequate command on the information systems infrastructures and keep the log records correctly.

LEGISLATION ANALYSIS

Article 5 of KVKK: Conditions for processing of personal data

(1) Personal data cannot be processed without the explicit consent of the data subject.

(2) Personal data may be processed without seeking the explicit consent of the data subject only in cases where one of the following conditions is met:

a) it is clearly provided for by the laws.

b) it is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid.

c) processing of personal data belonging to the parties of a contract, is necessary provided that it is directly related to the conclusion or fulfilment of that contract.

d) it is mandatory for the controller to be able to perform his legal obligations.

e) the data concerned is made available to the public by the data subject himself.

f) data processing is mandatory for the establishment, exercise or protection of any right.

g) it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

Explicit consent: According to the Law, personal data cannot be processed without the explicit consent of the data subject. However, in case of the presence of other legal reasons listed in paragraph 2, explicit consent of the person is not sought for data processing activity. In fact, the explicit consent to be obtained in the presence of one of these reasons will be invalid and conclude that the data controller has abused his right.

To be clearly prescribed by law: Personal data can be processed if clearly prescribed by law. For example; According to Law No. 5651, the processing of personal data for keeping logs related to the broadcasts made on the internet is based on a law provision and does not require explicit consent.

Situations of actual impossibility: In order to protect the body integrity of those who are unable to give consent due to actual impossibility or those who do not have the power to discriminate, data processing activities in these cases are not based on the explicit consent of the data subject. For example, taking action to protect body integrity by processing the contact and identification information of an unconscious person is within this scope.

Establishment or performance of a contract: It is the processing of personal data belonging to the parties of the contract directly related to the establishment or performance of a contract. For example, the cargo companies have to process the contact and identification information of the data subject to make the delivery.

Fulfillment of legal obligation: It covers the data processing activities that the data controller should perform within the scope of the legal obligation. For example, in some cases, the employer is obliged to report the identity of employees to law enforcement officers. This is due to the obligation to fulfil the legal obligation. Or the employer, who is obliged to employ a disabled person, has to make the notification to SSI to fulfill the legal obligation in regards.

Publicization: Publicization means public disclosure of a data. In order for the personal data to be processed based on the publicization condition, the data must be publicized by the data subject himself/herself. Also, the most important thing to note here is that the purpose of publicization and data processing should coincide. For example, sending an advertisement message to a lawyer whose identity information is publicly available on the bar sign will not match with the purpose of publicization, it will constitute a violation of the Law.

Establishment, exercise or protection of a right: Establishment, exercise and protection of a right can be considered as bilateral. Namely; data controller storing the information of an employee leaving the job throughout the trial timeout is a data processing activity aimed at protecting his/her right. The processing of his/her personal data in order to provide benefits to the employee is related to the establishment of the right.

The legitimate interest of the data controller: The data controller can carry out a data processing activity for his/her own benefit, provided that it does not harm the fundamental rights and freedoms of the data subject. Not damaging one's fundamental rights and freedoms is a decisive criterion here. For example, by making performance evaluations of the employer, to pay additional wages, premiums etc. to the employees or data processing activities that will be carried out to bring different practices that will increase employee loyalty will be in accordance with the law.

28 JANUARY

Data Protection Day

Follow Us on Social Media...