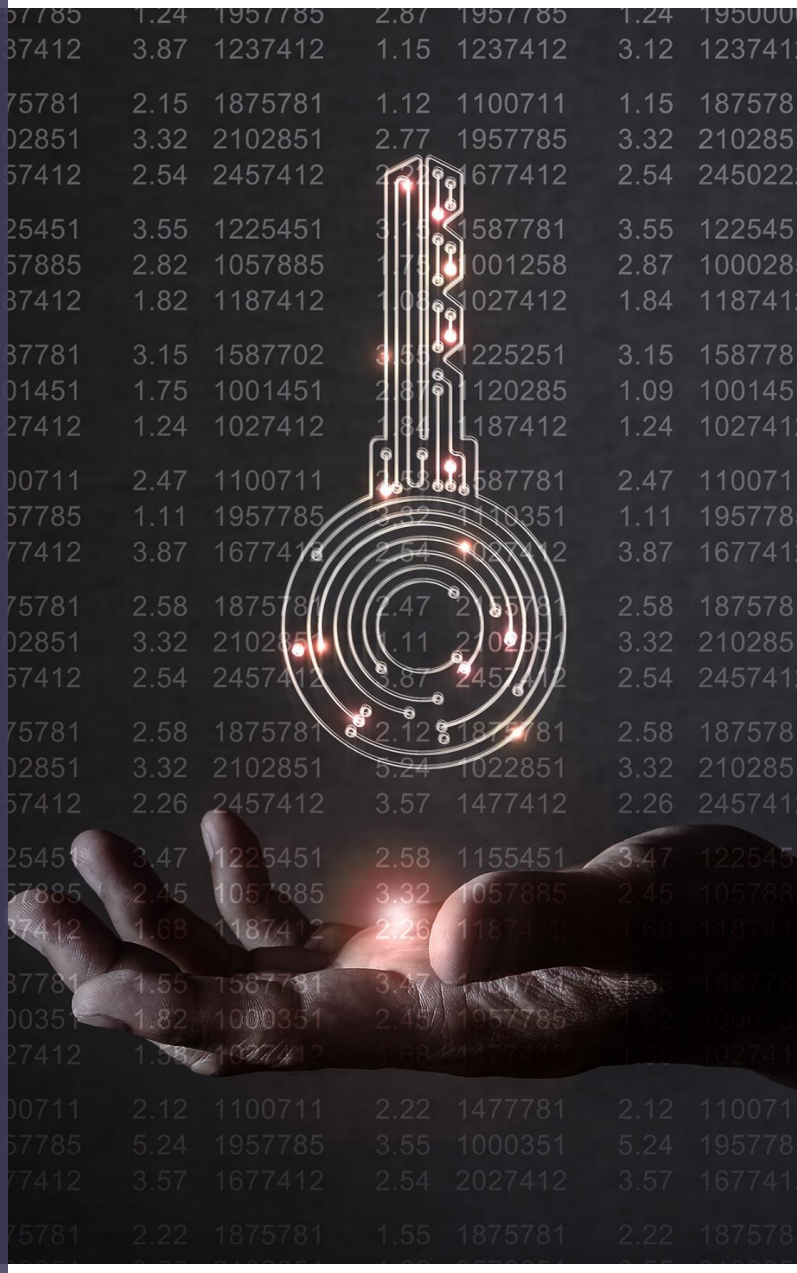
CottGroup®
Holistic Business Services

VeriSistem
a CottGroup® company



KVKK & GDPR NEWSLETTER

JULY 2020

DECISION SUMMARIES OF THE MONTH AND NEWS

Decision Regarding Applications with Incomplete Procedures Submitted by Proxy by a Person

Decision No: 2020/325 **Date of Decision:** 30.04.2020
Subject: Evaluation of high volume of incomplete applications submitted to the Authority by an individual by proxy

In a large number of applications submitted to the Authority with the same address information, format and content by proxy on behalf of some data subjects and in person on behalf of some data subjects, that within EU compliance laws, agreements under the name "Automatic Exchange of Information" ("AEOI") were made with 166 countries, among which Turkey also takes place and in accordance with the provision of the Article 9 of KVKK, that personal data cannot be transferred abroad without the explicit consent of the data subjects, since the persons on behalf of whom the applications are made, are concerned about exchange of their private information with the European countries, it has been requested that the information regarding retirements of the data subjects to be given only to themselves and those whom are appointed as their deputies.

As a result of the applications in question, it has been declared by the Authority that in order for the Authority to make investigations, data subjects should apply to data controller in accordance with the Article 13/1 of the Law titled *Application to the Data Controller*, as per the Article 13 it will not be possible to file a complaint before the application ways are exhausted, in accordance with the provisions of the Article 14 titled *Complaint to the Board*, as per the provisions that in cases that the application gets rejected or inadequately responded, as of the data controller's response is received within 30 days; in any case, within 60 days as of the date of application, complaint can be made to the Board, the data subjects should first apply to SSI (Social Security Institution) under the Turkish Republic Ministry of Family, Labour and Social Services which is primarily the data controller regarding their personal data on their retirement. However, applications continued to be submitted to the Authority by the person to whom the proxy has been given.

The Authority stated many times that the applications made by proxy cannot be investigated due to the lack of necessary procedural conditions, applications related to the subject should be made to the SSI first; and considering that the applications are still made on behalf of the data subjects and as a result of this, an unlawful profit can be gained from the data subjects under the name of

power of attorneys and this matter can be considered as a crime under the Turkish Criminal Code; it has been decided that as of the date of the decision, applications that have been submitted with the same address and similar applications to be submitted to the Authority in this content from now on will not be taken into consideration and evaluated, and the subject will be forwarded to the relevant institutions and authorities.

Decision Regarding the Use of Printouts of Medula Eczane by the Spouse of the Pharmacist Which Belong To Data Subject

Decision No: 2020/335 **Date of Decision:** 07.05.2020
Subject: A notification application submitted to the Authority for submitting a petition to the Provincial Health Directorate regarding the use of the Medula Eczane printouts of the data subject by the spouse of the pharmacist

As a result of the investigation of the complaint sent to the Ministry of Health that a pharmacist does not have the knowledge and skills to perform the profession due to health problems and includes the diagnosis and details of medicines, it has been determined that the spouse of the petitioner is also a pharmacist, and it has been stated that there is a strong possibility that the Medula Eczane[1] printouts might have been obtained through the pharmacy of the spouse of the data subject and notification has been made to the Authority by the Provincial Health Directorate.

As a result of the examination of the notification, it has been determined that Medula defined as an electronic information system implemented and operated by SGK in order to collect health service usage data and perform invoicing based on these data, and Medula Eczane is an information technology service that enables the receipt and invoicing of the prescription information of the medicines in electronic environment. In this system, where pharmacies are granted authorization, considering that personal data and sensitive personal data of the data subjects can be accessed by logging into system with the Turkish Republic ID numbers of them, pharmacists are considered as data processors within the Medula system.

Considering that the petitioner has obtained the Medula Pharmacy's printouts from the pharmacy of his spouse that are attached to the petition sent to the Provincial Health Directorate, it has been determined that the pharmacy has not taken the necessary security measures to prevent the access of third parties, it has been decided to impose an administrative fine of 60.000 TL within the scope of the paragraph 1 of the Article 12 and the paragraph 1/b of the Article 18 of the Law, and it has been concluded that since the spouse of the pharmacist obtained and used the personal data of the data subject, it has been considered that it constitutes a crime in accordance with the Article of the Turkish Criminal Code and it has been decided to notify the Prosecutor's Office about this person.

[1] An online system used by pharmacies powered by SSI

Summary of the Decision on the "Complaint regarding the illegal processing and disclosure of the personal data of the data subject by the lawyer who carries out enforcement proceedings"

Decision No: 2020/429 **Date of Decision:** 28.05.2020
Subject: Complaint regarding the unlawful processing and disclosure of the personal data of the data subject by the lawyer who carries out enforcement proceedings

In the petition of complaint sent to the Authority by the data subject, it has been stated that due to the data subject's debt to the bank, enforcement proceedings have been initiated by a lawyer, who is the deputy of the bank; on 27.11.2018, short messages containing the name of the data subject and enforcement order have been sent to the mobile phones registered on the colleagues of the data subject, whose numbers are not exactly known by the data subject and residing in the same social facility with him; and to the mobile phone registered on the elder brother of the data subject; that the data subject also applied to the Prosecutor's Office in regard to the subject, it has been requested to take the necessary action about the lawyer.

As a result of the investigation initiated on the subject, it has been stated in the defense requested from the lawyer that, the short messages in question have been sent to the data subject upon his given consent by calling the lawyer on the phone and the data subject has asked for information in person; that there are many lines registered on the data subject, and complaint has been made without exhausting the ways of application.

In the defense sent to the Authority, it has been understood that there are wrong determinations and evaluations regarding the Law No. 6698 and its applications, and it has been concluded to make an overall evaluation in this regard.

Considering the wrong determinations and evaluations regarding the Law No. 6698 and its applications in the defense of the data controller lawyer, it has been decided to instruct the data controller to show maximum attention and care in compliance with the Law.

As a result, it has been decided to reject the procedural objections in the defense of the data controller due to irrelevancy, considering that he does not fulfill its obligation to prevent unlawful processing of personal data and to prevent unlawful access to personal data and acts contrary to general principles; since the data processing activity carried out by the data controller constitutes a violation of the Law, it has been decided to impose an administrative fine of 125,000 TL to the data controller.

Summary of the Decision on the "Request for an opinion on whether a foreign bank having a representation office in our country will be regarded as data controller under the Law No. 6698 and whether obligated to be registered with the Data Controllers' Registry"

Decision No: 2020/471 **Date of Decision:** 23.06.2020
Subject: About a foreign bank having a representation office in our country whether it will have the title of data controller regarding the processing of personal data within the scope of the services it provides in accordance with the Law No. 6698 (KVKK) and its obligation to register with the Data Controllers' Registry

As a result of the evaluation made by the Board upon the request for an opinion sent to the Authority that whether a foreign bank processing personal data of the natural persons within the body of the legal entities they serve and having a representation office in our country will have the title of data controller in accordance with KVKK numbered 6698 (the "Law") and whether it has an obligation to register with the Data Controllers' Registry, it has been determined that the bank processes the personal data of the data subjects resident in Turkey within the scope of the financing services it provides.

As a result of the evaluation made by the Authority, due to the fact that the right to request the protection of personal data is a fundamental right and freedom regulated in the third paragraph of the Article 20 of the Constitution, and in determining the application area of data protection regulations in terms of location, it is necessary to adopt an approach that provides protection to individuals at the highest level and in the broadest scope, the Law KVKK numbered 6698 will find an application area in terms of personal data processing activities due to its constant presence in our country through the representation of a foreign bank requesting opinion and in this context it has been decided that the foreign bank in question has the title of data controller and has the obligation to register with the Data Controllers' Registry.

Delisting the Results of Search Engines in Searches Made Through Search Engines with Names and Surnames of the Data Subjects "Exercising the Right to be Forgotten"

Decision No: 2020/481 **Date of Decision:** 23.06.2020
Subject: Requests for Delisting Search Results from the Index Made Through Search Engines with Name and Surname of People

In the applications submitted to the Authority, it has been requested that the names and surnames of the data subjects mentioned in the news on the websites of the media organizations or news about data subjects to be erased in the scope of KVKK, necessary decisions to be made to subject the newspaper archives in question to a technical arrangement so that they cannot be indexed in search engines, as a result of the requests submitted, the Authority has stated that they have evaluated the applications as a whole within the scope of the "Right to be Forgotten".

The Authority has stated that the "Right to be Forgotten" is defined as "*the individual's ability to request that the information that has been spread in accordance with the law in the past and has the correct quality be delisted or not brought to the agenda depending on the passage of time*" in line with various judicial decisions and the opinions of international institutions, and also stated that the right to request the deletion of personal data is granted to individuals with the following statement added to the Article 20 of the Constitution within the amendment made in 2010: "*Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law.*"

The Authority has stated that in the Article 4 of the Law among the mandatory issues in the processing of data, being accurate and up-to-date, processing for legitimate purposes, and keeping personal data for as long as stipulated in the legislation or required for the purpose for which they are processed are counted, in accordance with the subparagraph 1/e of the Article 11 of the Law, the data subject is entitled to request the deletion or destruction of their personal data, and in the Article 7, even if the personal data has been processed in accordance with other relevant laws, if the situations requiring its processing have disappeared, it will be deleted by the data controller upon request of the data subjects, and stated that the provisions in other laws on this matter are reserved and the procedures and principles will be set forth under a regulation.

In a decision of the Court of Appeal regarding the "Right to be Forgotten", the Authority has stated that since the news on the website is out of date and will not meet the criteria of valid and accurate information at that time, keeping the news on the air will not contribute to the progress and development of the society, the information on the criminal background does not concern the society, since the subjects of the news are not elected or appointed politicians, artists or intellectuals, the right to be forgotten is superior to freedom of expression and press, considering that the press organs are data controllers, applications for deletion of personal data processed by giving place in the media and various websites and news, in line with the right to be forgotten, the need for evaluation has emerged about how the requests of the data subjects to be handled to remove their names and surnames from searches in search engines when the relevant provisions of the Law has been examined by the Board.

Stating that the Right to be forgotten is considered as a superior concept within the framework of the Article 20 of the Constitution and Articles 4, 7, 8 and 11 of KVKK;

The Authority stated that,

• In the searches made with the name and surname included in the applications, that the right of the data subject regards to the search results about himself/herself not to be accessed is considered as a request to be excluded from the index, considering the fact that the processors of search engines automatically and systematically find the information disseminated on the internet and then organize personal data with indexing programs as a list of search results, stored on servers, presented to users, the activities of search engines are considered as data processing activities and that the data subjects should make their applications to search engines first, taking into account the procedures, periods and principles specified in the Law,

• In case the process does not progress and is rejected, a complaint may be filed to the Board, and direct judicial proceedings can be executed, and the form of the applications will be determined by the search engines.

In order to implement the right of the data subjects to be forgotten on the websites, it has been decided that the necessary actions to be taken for the provision of communication channels to be used by the citizens of Turkey and to inform search engine operators about the procedures and principles specified in the decision.

You may access the full text of the Board Decision and The Criteria to Be Taken into Account When Assessing Requests to Delist the Results Displayed Following a Search Made Based on Person's Name and Surname from a Search Engine's Index by clicking this link.

Doctor Ataman Egemen Koyuncu – Data Breach Notification

With the data breach notification made by Doctor Ataman Egemen Koyuncu; it has been reported to the Authority that the system where patient information is stored has encountered a cyber-attack, the breach has been detected by realizing that the patient program has been deleted on 06.07.2020, the data affected by the breach are the identity of the patients, contact information and detailed information about health, examination findings, sexual problems and laboratory test results and the estimated number of the people affected by the breach is 10.000.

The data breach in question has been published on the website of the Authority on 09.07.2020 and the investigation on the subject continues.

Fluke Corporation and Fluke Electronics Corporation - Data Breach Notification

Fluke Corporation, and Fluke Electronics, which has the title of Data Controller, have been sanctioned by the Turkish Personal Data Protection Authority. The Data Controller reported the data breach by sending a letter to the Authority.

In the report, It was stated that the breach occurred by penetrating into the Fluke Connect environment as a result of the hijacking of the data controller's web service administrator account. The data controller explained that the date of the data breach was uncertain, but the penetration was detected on 29.06.2020. It has been determined that e-mail addresses, phone numbers, company names, personal and/or company addresses, contact information, measurement data from Fluke Connect handsets and Fluke Connect Sensors, subscription information, and encrypted passwords have been affected by the breach. Data Controller stated that 4,282 people were affected by the data breach in Turkey and the investigation on the subject continues.

Mert Grup Sigorta Aracılık Hizmetleri Ltd. Şti. Data Breach Notification

In the data breach notification conveyed to the Authority by Mert Grup Sigorta Aracılık Hizmetleri Ltd. Şti., it has been stated that the breach occured on 11.07.2020 and identified on 13.07.2020, the systems of Atlas Mutuel Sigorta and Corpus Sigorta have been hacked which are the agencies of Mert Grup and amounts such as 1, 5, 10, 15, 25, 30, 50 TL have been withdrawn from the cards of some persons; identity, contact and finance data and 707 people have been affected by the breach.

The data breach in question has been published on the website of the Authority on 16.07.2020 and the investigation on the subject continues.

Belgian Data Protection Authority Imposed a Fine on Google Belgium

The Belgian Data Protection Authority imposed a fine of 600.000 EUR to Google Belgium for not allowing a citizen to have his right to be forgotten and for not being sufficiently explicit in the delist form.

The Authority discovered that most of the links were needed for the public interest and should not be removed. The Belgian citizen was indeed a public figure, and the relevant contents were affiliated to a political party. Besides, there were also other contents which were outdated, unreliable, and could potentially damage the reputation of the data subject. The Belgian DPA considered that Google Belgium should have delisted those links. At the same time, DPA found that Google Belgium wasn't given a reliable response to the data subject and had no clarity in its delist form.

Under these circumstances, the Authority issued a record fine of 600.000 EUR to Google Belgium.

Spanish Data Protection Authority Fines 25.000 EUR to Spanish Company Glovo

The Spanish Data Protection Authority fined 25.000 EUR to Spanish company Glovo for not assigning a Data Protection Officer and not providing the necessary information on time.

The Spanish Company Glovo did not appoint a DPO and did not inform the Spanish DPA. An investigation was started with the complaints of two data subjects. During the investigation, Glovo informed the Spanish Data Protection Authority that an official DPO will be appointed. In the Spanish Law, which complies with the GDPR, a 10-day delay is envisaged to notify the Data Protection Authority of the appointment or dismissal of the DPO.

However, Glovo has violated the rule that bases on the 37 of the GDPR. The Authority decided that Glovo had to appoint a DPO considering the number of customers it has and fined Glovo 25.000 EUR for violating the Article 37 of the GDPR.

The Dutch Data Protection Authority fined the Netherlands Credit Bureau with 830.000 EUR

The Dutch Data Protection Authority (DPA) fined 830.000 EUR against the Netherlands Credit Bureau (BKR) for violating the rights of the data subject. The fine stems from the practice of BKR for charging a fee to individuals to deter them from wishing to request access to their personal data.

BKR is responsible for maintaining the Dutch central credit information system, which is knowledgeable about all credit registrations and repayment behaviour of individuals, including bankruptcy, sanction screening, and public records, as well. The system is usually checked by various companies, including financial institutions, municipalities, payment service providers, and car rental companies (for example, checking if a person is eligible for credit, mortgage, or credit card).

According to the GDPR, individuals have the right to access personal data collected about them and use it easily and at reasonable intervals.

The Dutch DPA received many complaints about the high standards BKR has set for personal data access.

According to the complaints, BKR asks individuals to send a copy of their passports via mail while providing access to personal data.

BKR has stated that it may charge a reasonable fee for repetitive requests based on the Article 12 (5) paragraph (a) of the GDPR and also requested a minimum subscription of 4.95 EUR per year from individuals for access requests made more than once a year to provide them instant digital access to personal data.

The Authority has decided that these practices violate the Articles 12/2 and 12/5 of the GDPR, since they do not make the rights easier to access and fail to provide access to personal data for free.

The Authority denied arguments made by BKR, stating that free access to personal data once a year and multiple annual access requests would not be considered "repetitive" without individual assessment.

The Authority states that requests may be rejected in cases where it is manifestly unfounded, irrelevant or excessive due to its repetitive characters. However, this should be assessed on a case-by-case basis as soon as the request is submitted prior to handling the request. It is the controller's responsibility to explicitly show the manifestly unfounded, irrelevant or excessive character of the application.

Considering the penalty structure of the Dutch DPA, a fine of 385.000 EUR is envisaged for the violation of the Article 12 (5) of the GDPR, and a fine of 650.000 EUR is envisaged for the violation of the Article 12 (2) of the GDPR.

Since both violations are linked to the principle of transparency, which aims to give people control over personal data, the total penalty has been reduced by 20% to 830.000 EUR.

A Fine of 16.700.000 EUR Imposed on the Italian Telecommunications Operator Wind Tre S.P.A (WINDTRE)

In a press release, the Italian Data Protection Authority (IDPA) announced a fine for "illegal data processing" related to the company's promotional activities. The Authority stated that WINDTRE previously had a precautionary decision regarding data collection activities, but violations kept occurring.

According to the GDPR Enforcement Tracker, it is the 6th biggest penalty imposed under the GDPR since the data privacy regulation came into force in May 2018. It is the second largest penalty given by IDPA till January of this year, following the 27.800.000 EUR (31.000.000 EUR) fine against other telecommunications operator TIM.

In addition to the fine imposed, Wind Tre was banned from processing data received without consent, and Wind was notified by the Authority to implement procedures to respect users' requests not to be disturbed.

Polish Data Protection Authority (UODO) Fines 15.000 PLN to Polish Company East Power

Polish DPA (UODO) fined East Power company from Jelenia Góra 15.000 PLN on the grounds that the company did not provide the supervisor have access to the personal data and other information required to perform its duties.

A German citizen filed a complaint against the company that provides employment services in Germany and Poland, claiming that his personal data was processed without permission and for marketing purposes. The complaint was submitted to the German DPA competent with the Rheinland-Palentine; but since the company was founded in Poland, this complaint was considered by the so-called leading authority, UODO.

As part of the complaint, three requests have been sent by UODO to the company. Ignoring the first two of the complaints, the company gave incomplete and contradictory response to the final request. UODO stated that the statements given would not be enough for the case. Due to such behaviour of the Company, UODO concluded that it has deliberately obstructed the course of the proceedings or at least ignored its obligations to cooperate with the supervisory authority.

When deciding to impose administrative fines and quantify it on East Power, UODO took the severity of the breach (GDPR), the intentional nature of the breach, and the degree of cooperation of the Data Controller to resolve the breach and alleviate its consequences.

Personal Data Protection Authority (UODO) fined the Polish General Inspector (Główny Geodeta) for a sum of 100.000 PLN.

The Personal Data Protection Authority found that the Polish General Surveyor violated the provisions of the GDPR. The violation consisted of not providing access to data processing equipment and tools to the supervisor during the investigation and not providing access to the personal data and information required by the Authority to perform his duties.

The data controller and the data processor are obliged to cooperate with the supervisory authority in the performance of their duties, as specified in the Article 31 of the GDPR.

Violation of the provisions of GDPR by blocking access to data and information by the data controller or the data processor has led to the violation of powers of the supervisory authority specified in the Article 58 of the GDPR. Therefore, it has been decided to impose an administrative fine of 100.000 PLN on the Polish General Surveyor by the Authority.

The Polish Data Protection Authority Imposed 5.000 PLN Penal Sanctions on Kindergarten And Preschool Education Institutions

The Polish DPA imposed a fine of 5,000 PLN on the non-public nursery and pre-school institution due to the lack of cooperation with the supervisory authority. The entrepreneur, who runs a kindergarten and pre-school educational institution, has failed to provide the UODO with access to the personal data and other information required to perform its duties.

As a result, the data controller reported a personal data breach to the UODO, which consisted of losing access to personal data stored in private kindergarten and pre-school education.

In order to compensate for the lack of information required to evaluate the report, the supervisory authority sent three requests to the entrepreneur to provide the relevant explanations. The authority, which has not received any response to the first two requests, has been able to get a response on the third request. However, the Entrepreneur has failed to respond to the requests of the UODO adequately. In deciding to determine the administrative fine and amount, UODO considered it as aggravating circumstances, the severity, and duration of the violation, the deliberate nature of the breach, and the lack of cooperation.

The fine imposed by UODO aims to discipline the entrepreneur both in terms of data breach reporting and, in other possible cases, to cooperate with the UODO properly.

Frequently Asked Questions on the judgement of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems

On July 16, 2020, the Court of Justice of the European Union legally nullified the US-EU Privacy Shield, which some companies use to justify personal data transfer from the EU to the United States. As stated in the decision of court, Standard Contractual Clauses ("SCCs[2]") which are used by many companies to justify such transfers and approved by the European Commission will remain valid. The court obliged the parties and European data protection authorities to assess the adequacy of protection in the country where data is transferred.

The court's judgement is based on the belief that there is a significant disconnection between the EU's emphasis on data privacy as a fundamental right and the U.S. intelligence agency's pressure on national security, which is essential for access to data transferred to the U.S.

[2]Standard Contractual Clauses are standard contract terms and conditions sets which aim to protect personal data separated from the European Economic Area (EEA), of which the personal data transferring party and the recipient is a member, through contractual obligations in accordance with the GDPR requirements in the regions.

Frequently Asked Questions

The Schrems II Decision has led to important changes regarding data transfers between the USA and the EEA. Regarding the changes that took place with this decision, EDPB published an announcement to clarify some points; the announcement included frequently asked questions on the subject:

Does the Court's judgement have implications on transfer tools other than the Privacy Shield?

The threshold set by the court applies to all appropriate safeguards under the Article 46 of the GDPR used to transfer data from the EEA to any third country. Besides, the U.S. legislation referred by the Court applies to any transfer to the United States by electronic means, which falls within the scope of this legislation, regardless of the transfer vehicle used for the transfer.

Is there any grace period during which I can keep transferring data to the U.S. without assessing my legal basis for the transfer?

No. The Court invalidated the Privacy Shield Decision without sustaining its effects, because the US law assessed by the Court does not provide an EU level of protection.

How can data continue to be transferred to a US data recipient bound by the Privacy Shield?

Transfers to this legal framework are illegal. If you wish to continue to transfer data to the USA, it must be checked whether it is possible to do this under the conditions listed below.

What should be done if SCC is used for data transfer to the USA?

Whether it is possible to transfer personal data through SCCs will depend on the assessments, taking into account the circumstances of the transfers, and extra measures implemented.

What to do if Binding Corporate Rules ("BCRs") are used with an entity in the U.S., what should I do?

Whether personal data will be transferred on a BCR basis will depend on the evaluation, taking into account the transfer conditions and any additional measures to be taken. These other measures need to ensure that, together with BCRs, it is to ensure that U.S. law guarantee

What about other transfer tools under the Article 46 of the GDPR?

EDPB, which is one of the independent data protection authorities within EU, will assess the consequences of the decision on transfer tools other than SCCs and BCRs. The decision clarifies that in the 46th Article of the GDPR, the standard of appropriate measures is "essential equivalence." According to the GDPR, that the level of protection of fundamental rights and freedoms in the laws and practices of a third country is equivalent to the EU, called "essential equivalence".

It is also important to remember that the Article 46 of the GDPR must be read under the light of the Article 44.

Are the derogations in the Article 49 of the GDPR valid for transferring data to the USA?

Data transfer from EEA to the USA is still possible based on the derogations provided in the Article 49 of the GDPR, provided that the conditions outlined in this Article apply.

Is it possible to continue to use SCCs or BCRs to transfer data to another third country other than the U.S.?

The Court indicated that SCCs could be used to transfer data to a third country. Besides, the Court also emphasized that data recipient and data transferring party shall be liable to evaluate whether the level of protection required by EU law in the third country has been respected or not.

What additional measures can be taken if SCC or BCR is used to transfer data to third countries?

The measures in question should be provided on a case-by-case basis, by taking into account all the conditions of the transfer and following the third country's laws to check whether it offers adequate protection.

The Court emphasized that it is the primary responsibility of the data transferring party and data recipient to carry out this assessment and provide the necessary additional measures.

What additional measures can be taken if SCC or BCR is used to transfer data to third countries?

The contract to be signed with the data processor under the Article 28.3 of the GDPR should indicate whether the transfers are consented by the parties. For example, it should be borne in mind that accessing data from a third country for management purposes is also a transfer.

Sub-processors must be authorized to share data with third countries.

If the contract signed under the Article 28.3 of the GDPR indicates that the data may be transferred to the US or another third country, what can be done to continue using the data processor's services?

It is not possible to take measures to ensure that U.S. laws do not substantially affect the level of equivalent protection in the EEA provided by transfer vehicles in the data transfers to the U.S.

Also, derogations under the Article 49 of the GDPR does not apply. The only solution is to make amendments in your contract or negotiate additional terms to prohibit transfers to the U.S.

If your data are to be transferred to another third country, you must also verify the third country's legislation to check whether it complies with the requirements of the Court and the level of protection of the personal data. If a suitable ground for transfers to a third country cannot be found, personal data should not be transferred outside the EEA region, and all processing activities should be carried out within the EEA.

Baden-Württemberg State Commissioner for Data Protection and Freedom of Information Imposes Fine on AOK Baden-Württemberg

The Baden-Württemberg State Commissioner fined € 1,240,000 against AOK Baden-Württemberg in accordance with the Article 32 of the GDPR due to violations of secure data processing obligations.

At the same time, the Department of Fines who was in a constructive cooperation with AOK, has provided the improvement of technical and organizational measures for the protection of personal data in AOK Baden-Württemberg.

From 2015 to 2019, AOK hosted raffles on different occasions and in this context, AOK collected the personal data of the participants, including their contact information and health insurance link. AOK wanted to use this data for advertising purposes, provided that the participants consented properly. The measures set by AOK during this activity did not comply with legal requirements and as a result of this, personal data of over 500 raffles participants were used for advertising without their consent.

With the spread of the claims, AOK stopped all sales activities in order to control all procedures in detail. In the light of what happened, AOK has created a task force for data protection in sales and has made adjustments especially regarding internal procedures and control structures in addition to the consent statements. In addition, AOK stated that they will stay in close coordination with LfDI and implement additional measures.

LfDI spoke in favor of AOK in the light of a comprehensive review and correction of its technical and organizational measures and after constructive collaboration. Protection of personal data during AOK's sales activities has improved in a short time. In the future, AOK will provide legal improvements and additional control mechanisms with the guidance it will receive from the Authority.

INFORMATION GUIDE

Administrative Measures – Obligation to Prepare Personal Data Processing Inventory and Register with VERBIS

As it is known, with the decision of the Board dated 23/06/2020 and numbered 2020/482, the deadlines of VERBIS registration have been extended and the deadline for natural and legal person data controllers with an annual number of employees more than 50 or with an annual financial balance exceeding 25 million TL, and the natural and legal person data controllers resident abroad to fulfill the obligation to register at the Registry has been determined as 30.09.2020. One of the obligations that depend on the registration obligation to VERBIS is to prepare a personal data processing inventory, and the fulfillment of this obligation requires a long-lasting determination study within the Organization. In other words, registration with VERBIS requires a detailed study and compliance with the Law No. 6698. In order to be ready for registration with VERBIS until 30.09.2020, it is recommended by the experts of the subject to start working within the Organization as soon as possible. You may access further information about preparing Personal Data Processing Inventory and registration with VERBIS via this link.

Personal Data Processing Inventory

Pursuant to the Article 4, paragraph 1 (h) of the Regulation on the Data Controllers' Registry published in the Official Gazette dated 30.12.2017 the personal data processing inventory is defined as "*the inventory in which the measures taken regarding data security are explained and elaborated in the course of the data processing activities carried out by the data controllers in connection with their business processes; the purpose of the processing of personal data and its legal basis, the category of the data, the maximum retention period of that data which is necessary and determined by means of associating the data with the recipient group of transmission and group of persons who constitute the subject of the data and the detailed explanation of the measures taken in respect of personal data which is intended to be transferred to foreign countries*".

Accordingly, personal data processing inventory is a document which will be created as a result of the detailed analysis of information obtained by virtue of an assessment of all the processes and the scrutinizing of all the activities within the scope of these processes by the data controllers who process personal data as part of their activities, such as the types of personal data and data categories processed in relation to each activity, the purpose for processing and the legal basis,

whether they are transferred or not and the parties to whom they are transferred, whether they are transferred abroad or not, the identity of the data subjects to whom the personal data which are processed belong, retention period specified by the data controller and the technical and administrative measures which are taken to ensure the security of the data.

The Authority has explained that the aim for imposing the obligation of preparing an inventory is "to detect whether there is any personal data processing activity which violate the provisions of KVKK". In this way, by preparing the personal data processing inventory, the data controller shall check whether it is complying with KVKK.

As also described in the beginning of the article, the obligation to prepare the inventory belongs to the persons who will submit a declaration to the Data Controllers' Registry pursuant to the provisions of the Article 5 of the Regulation on the Data Controllers' Registry, which stipulates "*The data controllers who are obliged to register with the Registry are obliged to prepare a Personal Data Processing Inventory.*" It means that the persons who are exempted from registering to VERBIS are not required to prepare the data inventory. Even though the obligation to prepare a data inventory has been listed among the administrative measures by the Authority, it is not among the mandatory administrative measures as far as the data controllers who will not register with VERBIS are concerned; however, it will be useful to prepare it.

As a result; the obligation to register with VERBIS is only one of the obligations listed in the Law No. 6698. Since preparing a Personal Data Processing Inventory and adapting to the Law will be the product of a work that requires analyzing the processes of the whole Organization and declaration of correct information to VERBIS is a legal requirement, Organizations should start process analysis studies as soon as possible.

You may contact us at ask@cottgroup.com to have further information about the subject.

Technical Measure - Encryption and Key Management

According to the 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 elaborated in the Personal Data Security Guide published by the Authority and specified at the notification stage to VERBIS.

One of these measures is encryption.

The use of access control authorization and/or encryption methods will help ensure personal data security against the loss or theft of devices containing personal data.

In terms of protecting data integrity, appropriate cryptographic methods should be applied in order to prevent an unauthorized alteration on the personal data.

The following points have to be considered about encryption;

• Sensitive personal data transferred in portable memory, CDs, DVDs must be encrypted when transferring.

• If sensitive personal data are to be sent via e-mail, they must be sent in encrypted form using KEP (registered e-mail) or corporate mail account.

• Secure encryption / cryptographic keys should be used for sensitive personal data and managed by different units.

• Key management should be implemented. The encryption key should be stored in an environment accessible only to authorized persons and unauthorized access should be prevented. All copies of encryption keys that could be used to make personal data usable should also be destructed.

• Encryption is a security providing tool that is used in different forms and provides different conditions according to these forms. In this context, with full disk encryption, the entire device can be encrypted or a file on the device can be encrypted in particular.

As a result, whatever encryption methods are used, it should be ensured that personal data are fully protected and for this purpose, the use of internationally accepted encryption programs should be preferred.

LEGISLATION ANALYSIS

GDPR - Article 17 – Right to be Forgotten

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

*****

The right to be forgotten can be defined as the right of individuals to request the deletion of their personal data from the data controller. According to the Article 17 of the GDPR, the data subject has the right to request the deletion of his/her personal data from the data controller without any delay, and if one of the conditions set forth in the relevant article is valid, the data controller has the obligation to delete the personal data immediately.

According to the Article 17;

• When the collection and processing purposes of the data are complete,

• If the data subject has withdrawn his/her explicit consent and there is no other purpose or legal reason for processing the data,

• If the data subject objects to the processing of his/her data and there is no legitimate interest in continuing this processing,

• If the personal data is processed for direct marketing purposes and the data processing activity has been rejected by the data subject,

• If the personal data processing activity is against the law,

• If the data processing activity needs to be stopped due to legal liability, when the data subject uses his/her right to be forgotten, the data processing activity must be stopped by the data controller immediately.

In addition, if the right to be forgotten is exercised by the data subject, personal data must be deleted from both actively used systems and backups; however, since the destruction of the backups will take time, the immediate destruction rule will apply to systems in active use; and the data subject will need to be informed about the backups. It should also be noted that; for both actively used systems and backed up data, the data should never be used during the destruction process with the exercise of the Right to be Forgotten.

Right To Be Forgotten In Turkey

About the implementation of the Right To Be Forgotten, the Law No. 6698 (KVKK), the decision of the Personal Data Protection Board dated 23.06.2020 and numbered 2020/481, the Article 20 of the Constitution, the Law No. 5651 and the Decision of the Constitutional Court (AYM) about N.B.B. should be considered and handled together. In general, the Law No. 6698 and the decision of the Board adopt a GDPR-based view; however, in accordance with the Constitution and the general legal norms, the decision of the Constitutional Court given in regards is important in the exercise and implementation of the Right to be Forgotten.

Although there is no regulation of right to be forgotten directly in the Law No. 6698, the right of the data subject to "*request the deletion or destruction of his personal data*" is regulated in the paragraph (e) of the Article of the Law. As can be seen in the opinions of the Authority and other regulations, this right is subject to the principles of the Right to be Forgotten regulated in the Article 17 of the GDPR.

In addition, in the decision numbered 2020/481, announced to the public in the announcement of the Authority dated 17.07.2020, the principles and *the Criteria to Be Taken into Account When Assessing Requests to Delist the Results Displayed Following a Search Made Based on Person's Name and Surname from a Search Engine's Index* have been specified. Although the decision has been concentrated on the search engines in particular and the criteria have been announced

within this framework, the subject is directly related to the Right to be Forgotten, as the Board also stated in its decision. Thus, all the issues explained in this decision should be evaluated within the framework of the Right to be Forgotten.

In the relevant decision, the Board has defined the Right to Be Forgotten as "*the individual's ability to request that the information that has been spread in accordance with the law in the past and has the correct quality be delisted or not brought to the agenda depending on the passage of time*" in line with various judicial decisions and the opinions of international institutions. In addition, with the following statement of the Article 20 of the Constitution, *"Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives...*", it has been stated in the decision that the Right to be Forgotten is recognized as a constitutional right in Turkish Law.

On the other hand; while evaluating the Right to be Forgotten, the decision of the constitutional court dated 03.03.2016 on the protection of human dignity guaranteed in the Article 17 of the Constitution should be taken into consideration. In the decision, the Constitutional Court accepted the application with the assessment that the article in the internet news archive subject to the request of the applicant was out of date, had no news value, there was no public interest in keeping it on the agenda, and that it was a hurtful and abusive information about the applicant's private life and decided to ensure that the data subject to be forgotten.

In addition, in the decision, the sensitive balance between the freedom of the press and the right to develop the spiritual existence of the people was taken into consideration and the legal benefit of the news being still on the air was investigated. That is, the cases in which the right to be forgotten cannot be applied as per the Article 17 of the GDPR under the paragraph 3 and the issues that are parallel to the concepts of legitimate purpose and legal reason included in the Regulation on Deletion, Destruction and Anonymization of Personal Data are mentioned. The points mentioned in this decision exactly corresponds to the Article 17 of the GDPR, Article 20 of the Constitution along with KVKK and the relevant other legislation. Finally, the decision made by the Board in 2020 has been written in a way to include the same principles, the framework of the general principles on the subject has been outlined and the criteria have been determined. In addition, the regulation of blocking access set forth in the Law No. 5651 also appears as one of the means of implementing the Right to be Forgotten, and it stipulates a procedure for the use of the Right to be Forgotten in this context.

Lastly, during the implementation of Right to be Forgotten, it is necessary to pay attention to the principles of the destruction of personal data included in the Article 7 of Law No. 6698 and other legislation; because deletion, destruction and anonymization is a method for establishing the Right to Be Forgotten, and the implementation of these methods must comply with the Law and the relevant Regulation. In this context, the data of the data subject should be destructed with the appropriate method and it should not be forgotten to inform the data subject. You may access further details on the subject in our VeriSistem® February KVKK & GDPR via this link.

As a result; the issues regulated by the Constitution such as the protection of the privacy of individuals, fundamental rights and freedoms, protection of the moral integrity of the person, superior public interest, freedom of expression and freedom of the press regarding the processing

of personal data should be handled together. At this point, when the Board's decision regarding the superior court decisions in Turkey and Europe has been examined, it is seen that the application is in form of preserving the balance between freedom of expression and press, and the fundamental rights and freedoms of the individual and examining what is the best advantage without harming freedom of expression/press.

It should be mentioned briefly about the method here that while the Right to Be Forgotten in Europe is used in accordance with the Article 17 of the GDPR, in Turkey, in order to determine the principles and procedures about the use of the Right to Be Forgotten, the Law No. 6698, Law No. 5651 and other legislation should be taken into consideration. In cases that fall under the scope of the relevant legislation, in addition to sending the requests of individuals directly to the data controller, it may be necessary to make a decision to be taken to block access, especially by applying to the court for information spread via the internet.

You may contact us at rights.consents@cottgroup.com to have further information on the subject.

Follow Us on Social Media...