Esin Attorney Partnership.

Data Protection Newsletter

December 2021

In November, the significant developments in the field of personal data protection were the Personal Data Protection Authority's ("**Authority**") announcement on certain municipalities' online query services, its decisions as to a data breach conducted by a retail store and unauthorized access to the Personal Health System (e-nabız) by hospital staff.

We set out summaries of developments in November in Turkey and from the world below:

Announcement — public announcement on online tax debt inquiry and debt payment systems of municipalities

The Authority published a public announcement on 5 November 2021 regarding the municipalities that only apply the single-factor verification method in their online tax debt payment and inquiry systems.

In its decision dated 25 February 2021, the Personal Data Protection Board ("**Board**") determined that individuals' access to debt information provided by some municipalities without a membership, password entry or double-factor authentication method violate the obligation to prevent unlawful access to personal data. Accordingly, the Board requested the termination of the unlawful data processing activities within three months in the letter sent to the metropolitan, provincial, district and town municipalities on 9 April 2021.

It was set out in the announcement that authentication through easily accessible data such as an identity number or date of birth constitutes single-factor authentication and instead of such authentication, double-factor authentication methods such as the use of personal password or SMS code should be preferred. The Authority's examination particularly focused on whether the information requested by the municipalities for identity verification purposes in the second stage is private and accessible by only the data subject. Following the examination, the Board decided to impose disciplinary provisions on the municipalities that continue to use a single-factor authentication system after the three-month period, and requested the relevant municipalities to inform the Board.

The announcement is available online here (in Turkish).

Decision — decision on the unauthorized access of the hospital staff to "e-nabız" system

In the complaint submitted to the Board, the data subject claimed that two different hospital employees accessed the data subject's e-nabız account without permission.

According to the Board's decision No. 2021/962 dated 21 September 2021: (i) only doctors operating at a data controller hospital are authorized to access the health data of data subjects, and thus access to the system by the doctor's assistant indicates that reasonable organizational and technical measures to prevent unlawful access to personal data have not been taken; and (ii) the provisions of the Turkish Criminal Code may be applicable against the employees who accessed health data unlawfully.

Accordingly, the Board decided to impose an administrative fine on the data controller hospital on the grounds that it failed to take reasonable technical and organizational measures and instructed the data controller hospital to respond to data subjects' applications with due care and diligence.

The decision is available online here (in Turkish).

Decision — decision against a retail store due to an attempt to sell customers' personal data

As claimed by the complainant in its submission before the Authority, personal data of a retail store's customers were offered for sale on the internet.

According to the Board's decision no. 2021/1021 and dated 7 October 2021;

- The fact that customer data of other data controllers, who received service from the same data processor were also offered for sale on the same date indicates that the data was obtained from the data processor.
- Although the violation is caused by the systems of the data processor, the data controller is jointly responsible with the data processor in taking the adequate measures.
- The fact that penetration test reports for the systems of the data processor were not provided prior to the breach indicates that the data controller failed to ensure appropriate level of security for the protection of personal data.
- The data controller failed to ensure that the data processor destroyed all data after termination of the commercial relationship.
- The fact that 4792 persons were affected by the breach and the breached data included name, surname, identity number, telephone number, gender, date of birth and order information, is likely to have negative consequences on the data subjects.

In light of the above, the Board decided to (i) impose an administrative fine of TRY 450,000 (approx. USD 35,000) against the data controller due to failure to take necessary technical and organizational measures, (ii) request the data controller to ensure that the affected data subjects are informed with notifications providing at least the elements required as per the decision No. 2019/271 dated 18 September 2019, and (iii) initiate an ex officio investigation subject to the decision on other data controllers whose personal data were offered for sale on the website.

The decision is available online here (in Turkish).

Significant developments from the world

- **European Data Protection Board released a draft guideline to clarify the scope of cross-border data transfers**

  On 19 November 2021, the European Data Protection Board (EDPB) published a draft guideline on the interplay between Article 3 of the General Data Protection Regulation (GDPR) and the provisions regarding cross-border data transfers. As per the guideline, the following three criteria must be met for data processing to qualify as a transfer to a third country: (i) the data processor or data controller is subject to the GDPR for the given processing, (ii) the data processor or controller (exporter) makes personal data available to another data controller, joint controller or processor (importer) through transmission or otherwise and (iii) the importer is in a third country or is an international organization[1] regardless of whether it is subject to the GDPR, according to Article 3.

  The guideline provides for processing examples for further guidance on the three criteria that are required cumulatively for cross-border data transfers. Accordingly, direct collection of personal data by a data controller located in a third country does not qualify as cross-border data transfer since the criterion number (ii) is not fulfilled.

  The guideline is available online here.

[1] According to the guideline "International organization" means an organization and its subordinate bodies governed by public international law, or any other body that is set up by, or on the basis of, an agreement between two or more countries.

Esin Avukatlık Ortaklığı.

Kişisel Verileri Koruma Bülteni

Aralık 2021

Kasım ayının kişisel verilerin korunması alanında göze çarpan gelişmeleri, Kişisel Verileri Koruma Kurumu'nun ("**Kurum**") bazı belediyelerin internet üzerinden sunduğu sorgulama hizmetine ilişkin kamuoyu duyurusu, bir mağazanın sebebiyet verdiği veri ihlali ve bir hastanenin personelinin e-nabız sistemine izinsiz erişimde bulunması hakkında verilen kararları oldu.

Kasım ayında ülkemizde ve dünyada yaşanan gelişmeleri aşağıda sizler için özetliyoruz:

Duyuru — Belediyelerin vergi borcu sorgulama ve borç ödeme sistemlerine ilişkin kamuoyu duyurusu

Kurum, 5 Kasım 2021 tarihinde, vergi borcu ödeme ve sorgulama sistemlerinde tek faktörlü doğrulama yöntemini uygulayan belediyeler ile ilgili bir kamuoyu duyurusu yayımladı.

Kişisel Verileri Koruma Kurulu ("**Kurul**"), 25 Şubat 2021 tarihli kararında, bazı belediyelerin; üyelik, şifre girme veya çift faktörlü doğrulama yöntemi kullanmaksızın, kişilerin borç bilgilerine erişim imkanı sağlamasının, kişisel verilere hukuka aykırı erişilmesini önlemek yükümlülüğüne aykırı olduğunu tespit etmişti. Bu doğrultuda, Kurum; tüm büyükşehir, il, ilçe ve belde belediyelerine 9 Nisan 2021 tarihinde gönderdiği yazı ile kanuna aykırı veri işleme faaliyetlerinin 3 ay içinde durdurulmasını talep etmişti.

Duyuruda, kolayca erişilebilen kimlik numarası veya doğum tarihi gibi veriler aracılığıyla yapılan kimlik doğrulamanın tek kademeli olduğu ve bunlar yerine, kişiye özel şifre veya SMS kodu gibi çift faktörlü doğrulama yöntemlerin tercih edilmesi gerektiği vurgulandı. Kurum, incelemesinde özellikle belediyelerin kimlik doğrulama amacıyla ikinci aşamada talep ettiği bilginin kişiye özel ve yalnızca ilgili kişinin erişebileceği nitelikte olup olmadığına odaklandı. Yapılan inceleme neticesinde, 3 aylık sürenin geçmesine rağmen tek faktörlü doğrulama sistemi kullanan belediyeler hakkında disiplin hükümlerinin uygulanmasına ve ilgili belediyelerin Kurul'u bilgilendirmesine karar verildi.

Duyuru metnine buradan ulaşabilirsiniz.

Karar — Hastane çalışanının e-nabız sistemine izinsiz erişimi hakkında karar

İlgili kişi, Kurum'a yaptığı şikayette, e-nabız hesabına iki farklı hastane çalışanının izinsiz olarak eriştiğini iddia etmiştir.

Kurul, 21 Eylül 2021 tarihli ve 2021/962 sayılı Kararı ile: (i) ilgili kişinin sağlık verilerine erişim yetkisinin veri sorumlusu hastanede çalışan hekime ait olduğunu, hekimin yanındaki sekreterin söz konusu verilere erişimininse kişisel verilere hukuka aykırı erişilmesini önlemeye yönelik makul idari ve teknik önlemlerin alınmadığını gösterdiğini ve (ii) sağlık verilerine hukuka aykırı olarak erişim sağlayan çalışanlar hakkında Türk Ceza Kanunu hükümlerinin uygulanabileceğini tespit etti.

Bu doğrultuda Kurul, veri sorumlusuna makul teknik ve idari tedbirleri almadığı gerekçesiyle idari para cezası uygulanmasına ve ilgili kişilerin başvurularına yanıt verilmesi hususunda gerekli dikkat ve özen göstermesi için talimatlandırılmasına karar verdi.

Karara buradan ulaşabilirsiniz.

Karar — Mağaza müşterilerinin kişisel verilerinin satışa çıkarılması hakkında karar

Kurum'a intikal eden şikayette, veri sorumlusunun müşterilerine ait kişisel verilerin internet üzerinden satışa çıkarıldığı iddia edilmiştir.

Kurul, 7 Ekim 2021 tarihli ve 2021/1021 sayılı Kararı ile:

- kişisel verilerin satışa çıkarıldığı internet sitesinde, aynı tarihte aynı veri işleyenden hizmet alan başka veri sorumlularının müşterilerine ait kişisel verilerin de olmasının, verilerin veri işleyenden elde edildiğini gösterdiğini;
- ihlal veri işleyenin kişisel verileri muhafaza ettiği sistemden kaynaklanmış olsa da gerekli tedbirlerin alınması hususunda veri sorumlusunun veri işleyen ile müştereken sorumlu olduğunu;
- ihlalden önce veri işleyenin sistemlerine yönelik herhangi bir sızma testi raporu bulunmamasının, veri sorumlusunun kişisel verilerin korunmasına için uygun güvenlik düzeyini temin etmediğini gösterdiğini;
- veri sorumlusunun, veri işleyenin muhafaza ettiği kişisel verileri aralarındaki ticari ilişkinin sonlanmasının ardından imha etmesini sağlamadığını;
- ihlalden etkilenen 4792 kişi olduğunu ve ad soyad, T.C. kimlik numarası, telefon numarası, cinsiyet, doğum tarihi ve sipariş bilgileri içeren ihlale konu kişisel verilerin ilgili kişiler üzerinde olumsuz sonuç doğurma riskinin bulunduğunu

tespit etti.

Bu doğrultuda Kurul, veri sorumlusu hakkında (i) gerekli teknik ve idari tedbirleri almaması sebebiyle 450.000 TL idari para cezası uygulanmasına, (ii) bundan sonraki bildirimleri etkilenen herkesin bilgi almasına elverişli ve Kurul'un 18 Eylül 2019 tarih ve 2019/271 sayılı kararında yer alan unsurlara uygun şekilde yapmasının hatırlatılmasına ve (iii) karara konu internet sitesinde kişisel verileri satışa çıkarılan diğer veri sorumluları hakkında resen inceleme başlatılmasına karar verdi.

Karara buradan ulaşabilirsiniz.

Dünyadan Göze Çarpan Gelişmeler

• Avrupa Veri Koruma Kurulu yurt dışına veri aktarımının kapsamını netleştiren taslak rehberi yayımladı

Avrupa Veri Koruma Kurulu ("**EDPB**"), 19 Kasım 2021 tarihinde Avrupa Genel Veri Koruma Tüzüğü'nün ("**GDPR**") 3. maddesi ile yurt dışına veri aktarımına ilişkin düzenlemeleri arasındaki ilişki üzerine rehber yayımladı. Rehberde, yurt dışına veri aktarımının (i) veri işleme faaliyetiyle ilgili olarak veri işleyen veya veri sorumlusunun GDPR'a tabi olması, (ii) söz konusu veri işleyen veya veri sorumlusunun kişisel verileri aktarım yoluyla veya başka bir suretle diğer veri sorumlusu/veri işleyenlerin erişimine sunması ve (iii) GDPR'ın 3. maddesinden bağımsız olarak, kendisine kişisel veri aktarılan kişinin üçüncü bir ülkede veya uluslararası bir kuruluş[2] olması kriterlerine göre belirleneceği belirtildi.

Yurt dışına veri aktarımında kümülatif olarak aranan kriterlerin uygulama örneklerine kapsamlıca yer verilen rehberde, yurt dışındaki veri sorumlusunun doğrudan kişisel veri toplamasının (ii) numaralı kriteri yerine getirmemesi sebebiyle yurt dışına veri aktarımı teşkil etmediği belirtildi.

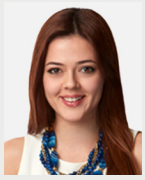
Rehbere buradan ulaşabilirsiniz.

Ekibimiz/Our Team

İlay Yılmaz
Partner
CIPP/E
+90 549 812 05 58
ilay.yilmaz@esin.av.tr

Can Sözer
Senior Associate
CIPP/E
+90 530 555 39 63
can.sozer@esin.av.tr

Ecem Elver
Senior Associate
+90 530 555 39 74
ecem.elver@esin.av.tr



Aybüke Gündel Solak
Senior Associate
+90 536 861 12 57
aybuke.gundel@esin.av.tr

Yiğit Acar
Associate
+90 549 825 77 69
yigit.acar@esin.av.tr

Berfu Öztoprak
Associate
+90 549 842 78 24
berfu.oztoprak@esin.av.tr

Ayça Doğu
Associate
+90 549 842 78 22
ayca.dogu@esin.av.tr

Ecenur Etiler
Trainee
+90 549 439 01 93
ecenur.etiler@esin.av.tr

[2] Rehbere göre "Uluslararası kuruluş", uluslararası hukuka tabi olan bir kuruluşu ve ona bağlı alt kuruluşları veya iki veya daha fazla ülke arasındaki anlaşma uyarınca kurulan herhangi bir kuruluş anlamına gelir.