



Bilgi güvenliği: Kişisel verilerin korunması



HAKAN GENEL



Neden?

- ❑ Toplum ihtiyacı
- ❑ 1981 tarihli "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"
- ❑ 2010 yılı Anayasa değişikliği
- ❑ Diğer yasal mevzuat değişiklikleri
- ❑ AB uyum süreci-**Vizesiz Avrupa!**
- ❑ Türk Ceza Kanunundaki Gerekçe ve ilgili maddeler: TCK 134-140
- ❑ Anayasa Mahkemesi Kararı
 - ❑ Herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı, kişisel verilerin, ancak kanun oluşturularak düzenlenebileceğini,...

Anayasa

2010 yılında 5982 sayılı Kanun'la yapılan Anayasa deęişiklięi ile Anayasa'nın 20. maddesine ilave bir fıkra eklenmiřtir. Söz konusu fıkrada;

“Herkes, kendisiyle ilgili kiřisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kiřinin kendisiyle ilgili kiřisel veriler hakkında bilgilendirilme, bu verilere eriřme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doęrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kiřisel veriler, ancak kanunda öngörülen hallerde veya kiřinin açık rızasıyla işlenebilir. Kiřisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

hükmüne yer verilmiřtir

Genel mevzuat

- ❑ Anayasa
- ❑ Türk Ceza Kanunu
- ❑ Kişisel Verilerin Korunması Hakkında Kanun
- ❑ Yönetmelikler
- ❑ Kararlar
- ❑ **AB Yasal Mevzuatı**
 - ❑ 1995 Tarihli "Data Protection Directive 95/46/EC"
 - ❑ 2016/679 sayılı AB Tüzüğü ve 2016/680 sayılı AB Direktifi

Önemli kanunlar

İş Kanunu, İşçi Sağlığı ve İş Güvenliği Kanunu, Borçlar Kanunu, Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Ticaret Kanunu, Kimlik Bildirme Kanunu, Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu, Medeni Kanunu, Elektronik İmza Kanunu, Ceza Kanunu, Adli Sicil Kanunu, Elektronik Haberleşme Kanunu, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, Vergi Usul Kanunu...

Kişisel verilerin korunması kanunu

6698 sayılı Kişisel Verilerin Korunması Kanunu 24.3.2016 kabul tarihinde kabul edilmiş ve 7.4.2016 tarihli ve 29677 sayılı Resmi gazetede yayımlanarak yürürlüğe girmiştir.

Avrupa Birliği’ni Kişisel Verilerin Korunması “Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Direktifi (95/46/EC)” ile güvence altına alınmıştır. KVKK da bu AB Direktifi’ne dayanılarak ve bu direktif hükümleri doğrultusunda hazırlanmıştır.

Kanuna uyum süreci zorunluluğunun **Nisan 2018** de başlamıştır.

5237 sayılı Türk Ceza Kanununu kapsamında **İdari ve hapis cezaları** uygulanır.

Kişisel veri nedir?

Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder. Bir gerçek kişinin; adı, soyadı, doğum tarihi, doğum yeri, telefon numarası, adresi, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmişi, resim, görüntü ve ses kayıtları, parmak izleri, e-posta adresi, hobileri, tercihleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veridir.

Özel Nitelikli kişisel veri: Özel nitelikli kişisel veriler; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza ve adli sicil ile ilgili verileri ile biyometrik ve genetik verilerdir.

Veri sorumlusu kimdir?

Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. Tüzel kişiler, kişisel verileri işleme konusunda gerçekleştirdiği faaliyetler kapsamında bizatihi kendileri “veri sorumlusu” olup, ilgili düzenlemelerde belirtilen hukuki sorumluluk tüzel kişinin şahsında doğacaktır. Bu konuda kamu hukuku tüzel kişileri ve özel hukuk tüzel kişileri bakımından bir farklılık gözetilmemiştir. Bu çerçevede gerek cezai gerekse de hukuki sorumluluk bakımından, tüzel kişilerin sorumluluğuna ilişkin özel hukuk ve kamu hukukundaki genel hükümler uygulanır.

Veri işleyen kimdir?

Veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiler olarak tanımlanmaktadır. Bu kişiler, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen, veri sorumlusunun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği ayrı bir gerçek veya tüzel kişidir. Herhangi bir gerçek veya tüzel kişi aynı zamanda hem veri sorumlusu, hem de veri işleyen olabilir. Örneğin, bir muhasebe şirketi kendi personeliyle ilgili tuttuğu verilere ilişkin olarak veri sorumlusu sayılırken, müşterisi olan şirketlere ilişkin tuttuğu veriler bakımından ise veri işleyen olarak kabul edilecektir.

(Pazar Araştırması Şirketleri, Posta Dağıtım Şirketleri, Ödeme Servisleri, Bulut Hizmeti Sağlayıcıları, Bilgi Teknolojileri Hizmetleri, Avukatlar, Turizm ve Seyahat Firmaları...)

KVKK-genel ilkeler

MADDE 4 - (1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

- a) Hukuka ve dürüstlük kurallarına uygun olma.
- b) Doğru ve gerektiğinde güncel olma.
- c) Belirli, açık ve meşru amaçlar için işlenme.
- ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
- d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Kişisel veri işleme şartları

- ❑ MADDE 5- (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.
- ❑ (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:
 - ❑ a) Kanunlarda açıkça öngörülmesi.
 - ❑ b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
 - ❑ c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

Kişisel veri işleme şartları

- ❑ MADDE 5
- ❑ ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- ❑ d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- ❑ e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- ❑ f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Özel nitelikli kişisel veri işleme şartları

- ❑ MADDE 6- (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.
- ❑ (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

Özel nitelikli kişisel veri işleme şartları

- ❑ MADDE 6-
- ❑ (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.
- ❑ (4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

HES kodu

TOPLU ULAŞIMDA HES KODU KULLANIMI

T.C. İçişleri Bakanlığının 29/09/2020 tarih, 89780865-153-E-15993 sayılı "Şehiriçi Toplu Ulaşımında HES Kodu Sorgulaması" başlıklı genelgesi uyarınca toplu ulaşım sisteminde HES Kodu kullanılması zorunlu hale getirilmiştir.



Hes Kodu
Nasıl Alınır?



ESHOT Çağrı
Merkezi
320 0 320



Öneri İstek Şikayet
Talebi



İzmirim Kartınıza
HES Kodu

Kaydetmek İçin Tıklayınız.

Duyurular

30.09.2020

İzmirim Kartınıza tanımlanacak olan HES kodunuzun **geçerlilik süresi en az 6 ay** olmalıdır.

Bilgilendirme

Sn. İzmirim Kart kullanıcısı;

T.C. İçişleri Bakanlığının, Koronavirüs salgınıyla mücadele çalışmaları kapsamında 30 Eylül'de çıkardığı "Şehir İçi Toplu Ulaşımında HES Kodu Sorgulama Başlıklı Genelgesi" ve İzmir Valiliği İl Hıfzıssıhha Kurulu'nun, bu genelgeye istinaden aldığı karar gereğince, toplu ulaşımında elektronik HES Kodu kontrolü uygulaması başlamıştır.

Açık rıza nedir?

- ❑ Kanununun 3. maddesinde açık rıza; “belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlanmıştır.
- ❑ Açık rızanın 3 önemli unsuru bulunmaktadır:
 - ❑ Belirli bir konuya ilişkin olması,
 - ❑ Rızanın bilgilendirmeye dayanması,
 - ❑ Özgür iradeyle açıklanması.

Açık rızada dikkat edilmesi gerekenler

- ❑ Ayrıca Anayasanın 20. maddesinin 3. fıkrasında, kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebileceği hüküm altına alınmıştır. Açık rıza, Kanunda hem özel nitelikli kişisel veriler, hem de özel nitelikli olmayan kişisel veriler bakımından temel hukuka uygunluk sebebi olarak öngörülmüştür.
- ❑ 95/46/EC sayılı Avrupa Birliği Direktifine göre açık rıza; ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüte yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır.
- ❑ Açık rızanın bu anlamda, rıza veren kişinin “olumlu irade beyanı”nı içermesi gerekmektedir. Diğer mevzuatlardaki düzenlemeler saklı kalmak üzere, açık rızanın yazılı şekilde alınmasına gerek yoktur. Elektronik ortamda alınması da mümkündür.

Silme, Yok Etme, Anonimleřtirme

- ❑ **MADDE 7- (1)** Bu Kanun ve ilgili dięer kanun h k mlerine uygun olarak iřlenmiř olmasına raęmen, iřlenmesini gerektiren sebeplerin ortadan kalkması h linde kiřisel veriler resen veya ilgili kiřinin talebi  zerine veri sorumlusu tarafından silinir, yok edilir veya anonim h le getirilir.
- ❑ **(2)** Kiřisel verilerin silinmesi, yok edilmesi veya anonim h le getirilmesine iliřkin dięer kanunlarda yer alan h k mler saklıdır.
- ❑ **(3)** Kiřisel verilerin silinmesine, yok edilmesine veya anonim h le getirilmesine iliřkin usul ve esaslar y netmelikle d zenlenir.

Kişisel Verilerin Aktarılması

- ❑ MADDE 8- (1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.
- ❑ (2) Kişisel veriler;
 - ❑ a) 5 inci maddenin ikinci fıkrasında,
 - ❑ b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında,
- ❑ belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.
- ❑ (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır..

Kişisel Verilerin Yurtdışına Aktarılması

- ❑ MADDE 9- (1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.
- ❑ (2) Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;
 - ❑ a) Yeterli korumanın bulunması,
 - ❑ b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.
- ❑ (3) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.
- ❑ (4) Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine;
 - ❑ a) Türkiye'nin taraf olduğu uluslararası sözleşmeleri,

Kişisel Verilerin Yurtdışına Aktarılması

- ❑ MADDE 9- b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,
- ❑ c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işleme amaç ve süresini,
- ❑ ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,
- ❑ d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.
- ❑ (5) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.
- ❑ (6) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

Aydınlatma yükümlülüğü

- ❑ MADDE 10- (1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;
- ❑ a) Veri sorumlusunun ve varsa temsilcisinin kimliği,
- ❑ b) Kişisel verilerin hangi amaçla işleneceği,
- ❑ c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı,
- ❑ ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- ❑ d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.

Kişinin bilgi isteme hakkı

- ❑ MADDE 11- (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;
- ❑ a) Kişisel veri işlenip işlenmediğini öğrenme,
- ❑ b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- ❑ c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- ❑ ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- ❑ d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- ❑ e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme

Kişinin bilgi isteme hakkı

- ❑ MADDE 11-
- ❑ f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- ❑ g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- ❑ ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.

Bilgi ve g¼ncelleme talepleri

T¼rk Telekom

Sayın HAKAN GENEL,
5552529642 nolu hattınızın ¼deme bilgileri aŐaĐıdadır.

Ad Soyad	HAKAN GENEL
Fatura ID	BC22020034363678
Son ¼deme Tarihi	18/11/2020
¼denecek Tutar	37,75 TL

Bilgi ve g¼ncelleme talepleri

Hakan Genel <hakangene@gmail.com>

to ttmobilkvkk ▾

Merhaba,

Ařađıda numarası (5458478440) bulunan kiři ile ismimiz sanırım aynı.
Bir řekilde e-posta adresi sisteminize yanlış girilmiř.

Benim bilgilerim;

TCKN: 103[REDACTED]40.

Ad Soyad: Hakan Genel

Dođrum Yılı: 1970

L¼tfen kayıtlardan bu e-posta adresini kaldırınız.

Teřekk¼rler,

İyi alıřmalar,

Best Regards

Hakan Genel

90-532-615-3559

BGYS ↔ Kanuna uyum süreci

HUKUKİ



İDARİ



TEKNİK



Kanuna uyum süreci

- Yönetmeliğe uygun Kişisel Veri Envanteri hazırlanması
- Kişisel Veri İşleme Politikası oluşturulması ve yayınlanması
- Bilgilendirme metinlerinin hazırlanması
- Açık rıza alınması
- Yetkilendirme yapılması
- Veri toplama, işleme, aktarma/paylaşım, saklama, arşivleme ve imha prosedürlerinin hazırlanması
- Sözleşmelerin ve taahhütlerin düzenlenmesi
- Teknik önlemlerin alınması
- Yurtdışına aktarım ve yurtdışında işleme
- Aydınlatma yükümlülüğü için iletişim ve sistem oluşturulması
- Verbis kaydının yapılması ve resmi bildirim formlarının doldurulması

Cezalar

- ❑ Kurumun arařtırmasına gre kurumlar ve bireylerin **%50** si konu hakkında bilgi sahibi deęil.
- ❑ Kurul Kararları kesin ve uygulanması zorunludur.
- ❑ Trk Ceza Kanunu uygulanır. Her gerek kiři ihlali iin ayrı ceza verilebilir.
- ❑ Verbis ykmllk ihlali: (2020) Alt Sınır: **36,000** - st Sınır: **1,800,000**
- ❑ Aydınlatma ykmllk ihlali: (2020) Alt Sınır: **9,000** - st Sınır: **180,000**
- ❑ Veri gvenlięi ykmllk ihlali: (2020) Alt Sınır: **27,000** - st Sınır: **1,800,000**
- ❑ Kurul kararlarına uymama: (2020) Alt Sınır: **45,000** - st Sınır: **1,800,000**

Cezalar

SUÇLAR	HAPİS CEZALARI		
	ASGARI	AZAMI	AĞIRLAŞTIRICI HAL
(TCK md.135) Hukuka aykırı olarak kişisel verileri kaydetme	1 yıl	3 yıl	<p>Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkraya uyarınca verilecek ceza yarı oranında artırılır.</p> <p>Bu suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, verilecek ceza yarı oranında artırılır.</p>

Cezalar

SUÇLAR	HAPİS CEZALARI		
	AŞGARI	AZAMI	AĞIRLAŞTIRILMI HAL
(TCK md.136) Kişisel verileri, hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme	2 yıl	4 yıl	Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, verilecek ceza yarı oranında artırılır.
(TCK md.158) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmeme	1 yıl	2 yıl	Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması halinde verilecek ceza bir kat artırılır.
(KVK Kanunu md.17) KVK Kanunu md. 7 hükmüne aykırı olarak kişisel verileri silmeme veya anonim hale getirmeme	1 yıl	2 yıl	Kanunun 7. maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hale getirmeyenler 5237 sayılı Kanunun 138. maddesine göre cezalandırılır.

Teknik Önlemler

- ❑ Yetki Matrisi, Yetki Kontrol
- ❑ Erişim Logları
- ❑ Kullanıcı Hesap Yönetimi
- ❑ Ağ Güvenliği
- ❑ Uygulama Güvenliği
- ❑ Bulut Güvenliği
- ❑ Şifreleme
- ❑ Sızma Testi
- ❑ Saldırı Tespit ve Önleme Sistemleri
- ❑ Mobil ve Taşınabilir Cihaz Güvenliği
- ❑ Veri Maskeleyme
- ❑ Veri Kaybı Önleme Yazılımları
- ❑ Yedekleme
- ❑ Güvenlik Duvarları
- ❑ Güncel Anti-Virüs Sistemleri
- ❑ Silme, Yok Etme veya Anonim Hale Getirme
- ❑ Kriptografik Anahtar/e-imza Yönetimi
- ❑ Tedarikçi Yönetimi
- ❑ ...

Fiziksel Güvenlik

- ❑ Bilgi güvenliğinin ve Kişisel Verilerin korunmasının en önemli konularından birisi fiziksel güvenlik bilincidir.
- ❑ Şirket sınırları içerisine giren tüm kişiler (ziyaretçi, tedarikçi çalışanı) sürekli kontrol edilmelidir.
- ❑ Şirket içerisinde refakatsiz dolaşmaya izin vermemeliyiz
- ❑ Tüm Kişisel Verileri ve gizli bilgileri kapalı ve kilitli, kontrollü ve yetkililer tarafından erişilen arşivde saklamalıyız.



Müşterilerin korunması-güvenliği

- ❑ Bilgi güvenliğinin ve Kişisel Verilerin korunmasının en önemli konularından birisi fiziksel güvenlik bilincidir.
- ❑ Şirket sınırları içerisine giren tüm kişiler (müşteriler, ziyaretçiler, tedarikçiler) sürekli kontrol edilmelidir.
- ❑ Kişisel Verileri ve gizli bilgileri kapalı ve kilitli, kontrollü ve yetkililer tarafından erişilen yerlerde saklamalıyız.



Temiz masa temiz ekran prensibi

- ❑ Belirli bir süre uzaklaşıldığında üzerinde kişisel bilgi barındıran doküman, belge, kimlik vb. bırakılmamalıdır.
- ❑ Ctrl+Alt+Del tuşlarına basılarak ekran kilitlenmelidir.
- ❑ Ekran koruyucu şifreli olarak 3-5 dakika arasında devreye girmelidir.
- ❑ Kişisel veriler ve gizli bilgiler kilitlenerek dolap ve çekmecelere konmalıdır.
- ❑ Müşterilerin bilgilerinin başkaları tarafından görülmemesi ve duyulmaması sağlanmalıdır.



Kullanıcı kimliđi ve şifreler

- ❑ Bilgisayara girerken şifrenin başkaları tarafından görülmemesi sağlanmalıdır.
- ❑ Şifreler kimse ile paylaşılmamalı, hatırlatma amacı ile bir yere yazılmamalıdır.
- ❑ Başkasının şifresi ile işlem yapılmamalı, kimseye şifre verilmemelidir.
- ❑ Şifreler en az **8** haneli ve karmaşık olmalı, tahmini zor olmalıdır.
- ❑ Yani **12345678** gibi olmamalı, **L8kws,?3** gibi olmalıdır.
- ❑ Şifre kişisel bilgilerle ilişkili olmamalıdır.
- ❑ Kişisel şifreler ve şirket şifreleri farklı olmalıdır.
- ❑ Özel uygulama ve e-posta şifreleri farklı seçilmelidir.
- ❑ Şifreler düzenli olarak deđiştirilmelidir. (6 hafta, 3 ay, 6 ay gibi)

Kullanıcı kimliği ve şifreler

ONE TIME PASSWORD



Two-Factor Authentication



Use two-factor authentication

On • We'll ask for a security code if we notice a login from an unusual device

Edit



Authorized Logins

Review a list of devices where you won't have to use a login code

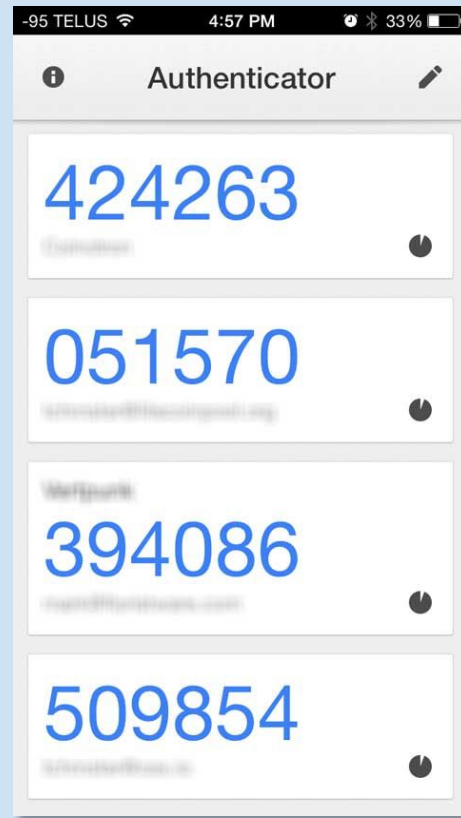
View



App passwords

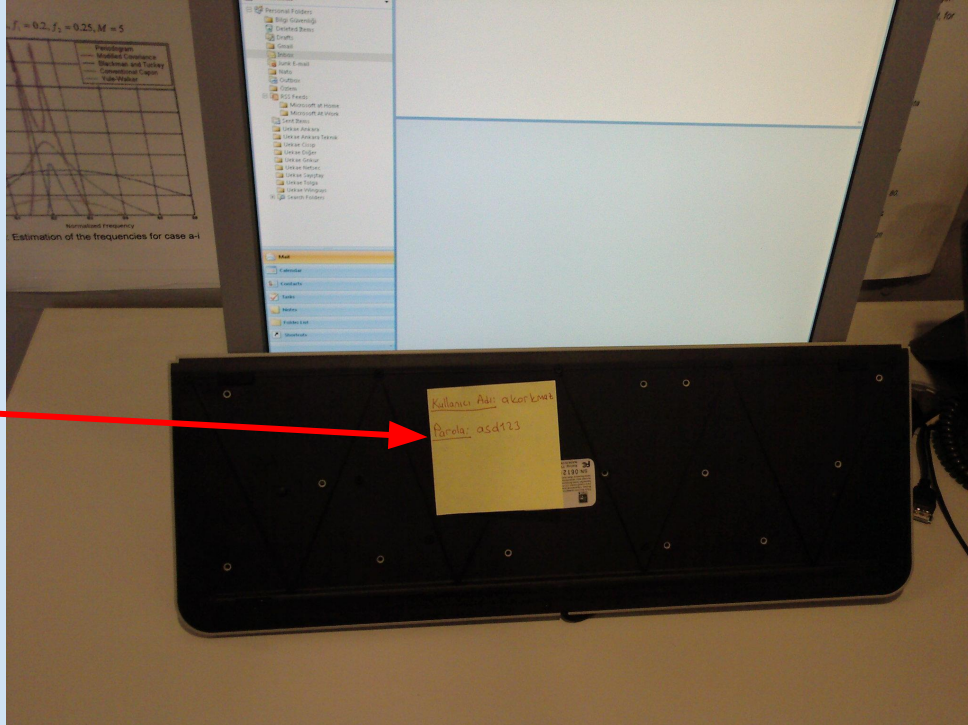
Use special passwords to log into your apps instead of using your Facebook password or login codes.

Add



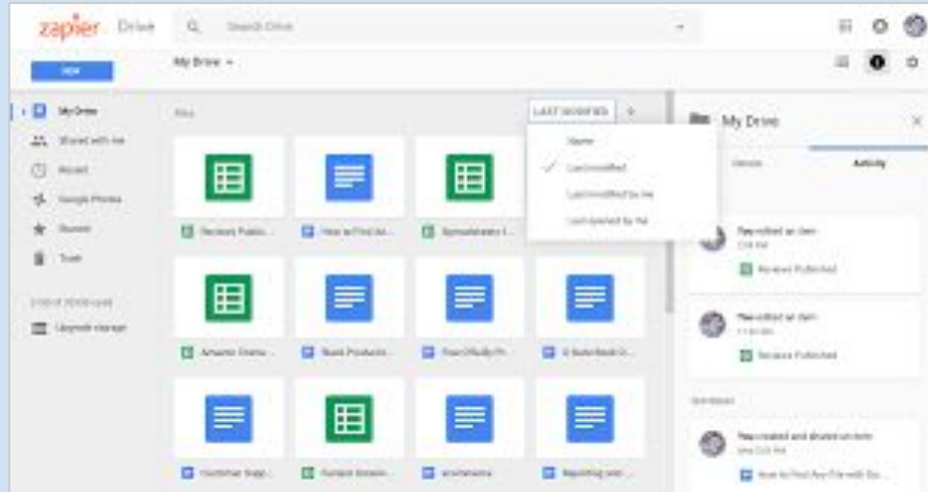
Kullanıcı kimliđi ve Őifreler

Őifre



Dosya Eriřim ve Paylařımı

- ❑ Dosyalarımızı Ortak Paylařımda tutmalıyız.
- ❑ Dosya yetkilendirmesine dikkat etmeliyiz.
- ❑ Yetkisiz eriřime izin vermemeliyiz. Kendimiz de yapmamalıyız.
- ❑ Önemli bilgileri (Özellikle Kiřisel Verileri) Őfreleyerek paylařmalıyız.



e-postalar

- ❑ Virüslerin en az %30 u e-postalardan bulaşır.
- ❑ Gelen e-postaların adreslerinin doğruluğu kontrol edilmelidir.
- ❑ e-postalarda en sıklıkla yapılan hata: Gönderdiğimiz kişiyi seçerken dikkat etmemek.
- ❑ Yanlış adrese göndermek kişisel/gizli bilgileri açığa çıkarır. Hukuken sorumluluk bulunmaktadır.
- ❑ Linkler tehlikelidir.
- ❑ Dosya ekleri virüs içerebilir.
- ❑ Sıkıştırılmış dosyalar tehlikelidir.
- ❑ Gizli dosyalar (özellikle Kişisel Veriler)şifrelenerek gönderilmelidir.



Mobil cihazlar

- ❑ Mobil telefonlardaki uygulamalardaki reklamlar virüs bulaştırabilir.
- ❑ Mobil telefonlarımızın ekran şifresi çok önemlidir.
- ❑ Günümüzde günlük yaşamımızdaki bir çok ihtiyacımızı ve işlemlerimizi mobil telefonlar ile karşılıyoruz. Her gün onlarca uygulama kullanıyoruz.
- ❑ En tehlikeli bilgi güvenliği riskleri ve açıklıkları mobil telefonlardadır.
- ❑ Mobil cihazlarımızı ortada bırakmamalıyız. Notebooklarımızı araç bagajında taşımamız gerekir.



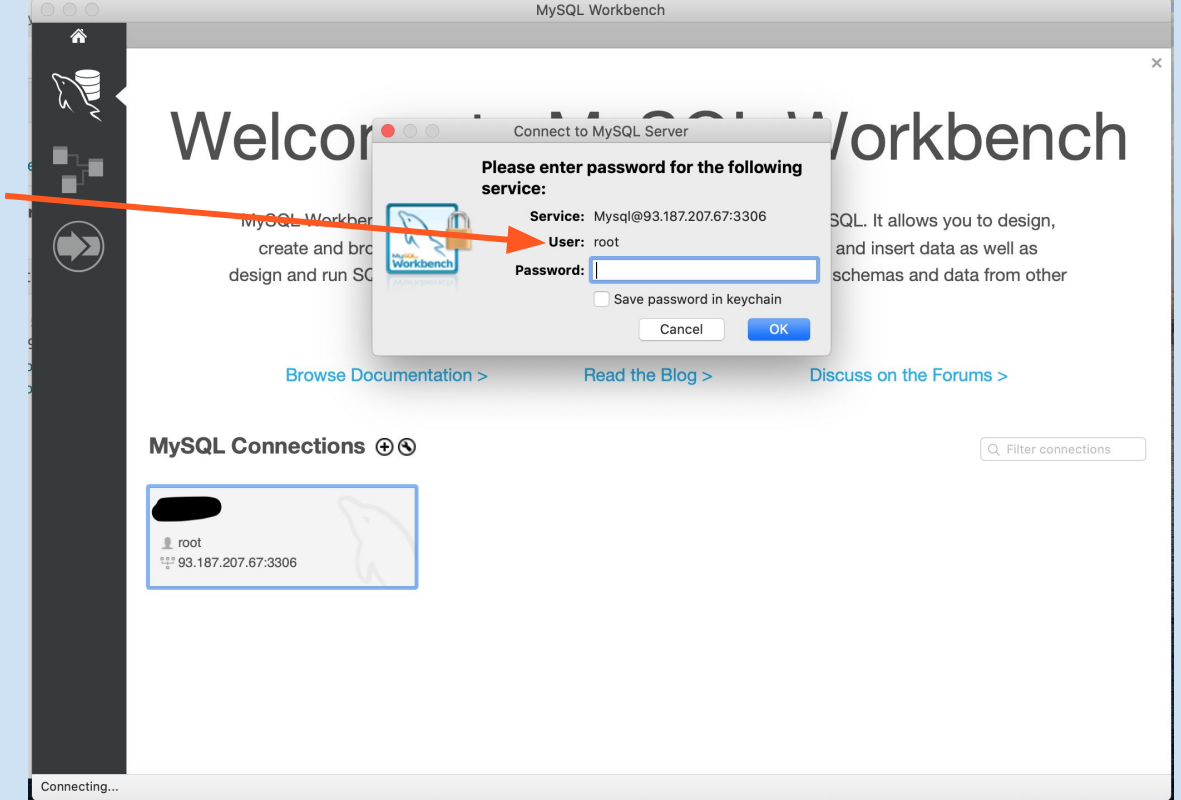
Halka açık aęlar

- ❑ Halka açık aęlar tehlikelidir.
- ❑ İzlenebilir, hırsızlık yapılabilir.
- ❑ Kopyalanabilir



Uzaktan Eriřim

- ❑ Sadece gerekli kişiler uzaktan erişmelidir.
- ❑ Sadece gerekli uygulama ve hizmetlere erişim sağlanmalıdır.
- ❑ Sadece güvenli bir VPN bağlantı yolu ile erişime izin verilmelidir.
- ❑ Mümkün olduğu durumlarda OTP/OAUTH şifreleme kullanılmalıdır..



USB Bellek Kullanımı

- ❑ USB bellekler virüs bulaştırılması ve bilgi hırsızlığı için en ideal araçtır.
- ❑ USB bellekler çalınabilir.
- ❑ USB bellekler kolaylıkla arızalanabilir.
- ❑ En az ölçüde USB bellek kullanımı sağlanmalıdır.



Kağıt öğütücü kullanımı

- ❑ Kişisel veri/gizli veri içeren dokümanları imha ederken kağıt öğütücü kullanmalıyız.
- ❑ Müsvedde yaptığımız kullanılmış dokümanları kontrol etmeliyiz.



Depo ve Sevkiyat Güvenliđi

- ❑ Depo ve sevkiyat güvenliđi Őirketimizin envanter kontrolünün sađlanması iin ok nemlidir.
- ❑ Depo ve sevkiyat alanına grevliler dıŐında kimse izinsiz giremez.
- ❑ Girenler uyarılır ve Ynetici bilgilendirilir.



Yazıcı kullanımı

- ❑ Doküman çıktılarını tam aldığımızı, eksik olmadığını kontrol etmeliyiz.
- ❑ Yazıcı hatası veya vazgeçme olabilir. Yine de gönderdiğimiz dokümanı iptal etmeli ve yazıcıdan basılmadığını kontrol etmeliyiz.
- ❑ Çıktının yazıcıda basılması anında cihazın başında bulunmalıyız.
- ❑ Yazıcıdan çıktıları alırken yanlışlıkla kendimize ait olmayan dokümanları almadığımızı kontrol etmeliyiz.



Internet tehditleri

- ❑ Mutlaka adresi elle yazmalıyız.
- ❑ Reklamlardaki linklere dikkat etmeliyiz.
- ❑ Anahtar işaretime dikkat etmeliyiz.
- ❑ Kredi kartlarımızı bilmediğimiz sitelerde kullanmamalıyız.
- ❑ Banka kartlarımıza alışveriş limiti koymalı, SMS ile bilgilendirme istemeliyiz.
- ❑ Alışverişlerde 3D sistemini kullanmalıyız.



trendyol.com

hepsiburada

Siber saldırı



KVKK ve ISO 27001 Standardı İlişkisi

- ❑ ISO 27001 kurumsal bilgi varlıklarının kişilerden korunmasını ele alır.
- ❑ KVKK kişilerin verilerini bilgi varlığı olarak kabul eder. Kurumun bu varlıkları korumasını ele alır.
- ❑ ISO 27001 uygulamaları gönüllülük esasi ya da kurumsal tercihler ile belirlenir.
- ❑ KVKK uygulamaları zorunludur.
- ❑ Her ikisi de sistematik bir organizasyon gerektirir.
- ❑ Veri koruma açısından her ikisi de çok sayıda ortak önlem almayı gerektirir.
- ❑ ISO 27001 yasalara uyum gerektirir, KVKK ise yasanın kendisidir

Kişisel Verileri Koruma Kurulu



VERBİS-Veri Sorumluları Sicil Bilgi Sistemi

Kişisel Verileri Koruma Kurumu Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) hoşgeldiniz.

Veri Sorumlusu Yönetici Girişi

Veri Sorumlusu Yönetici Girişi butonu, Sicile kayıttan önce veri sorumlusunun teyidi için başvuru formu doldurularak gönderileceği ve başvurunun Kurumumuzca onaylanması akabinde irtibat kişisi atama, mevcut parola değiştirme, yapılan bildirimleri görüntüleme ve Sicil kaydını silme işlemlerinin yapılabileceği bölümdür. Veri Sorumlusu "Kamu Kurumu" veya "Yurtiçinde Yerleşik Tüzel/Gerçek Kişi" ya da "Yurtdışında Yerleşik Tüzel/Gerçek Kişi" ise öncelikle bu buton aracılığıyla giriş yapılarak başvuru formunun doldurulması gerekmektedir.

Veri Sorumlusu Yönetici Girişi

Kurul Yaptırım Gücü

- ❑ Veri sorumlusu nezdinde buldukları pozisyon veya görev itibariyle kişisel verilere erişime yetkisi olanlar tarafından, yetkilerini aşarak ve işleme amacı dışında söz konusu verilerin işlendiği hususunda Kuruma intikal eden ihbar ve şikayetlere ilişkin yapılan değerlendirme sonucunda, uygulamada yaşanan problemlerin önüne geçilebilmesini teminen;
- ❑ Bir veri sorumlusu nezdinde buldukları pozisyon veya görev itibariyle kişisel verilere erişme yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılması 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil edeceğinden, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği hususunda veri sorumlularının bilgilendirilmesine,
- ❑ Kanunun 15 nci maddesinin (6) numaralı fıkrası uyarınca alınan bu ilke kararının Resmi Gazete ile Kurumun internet sitesinde yayımlanmasına, oy birliği ile karar verilmiştir.

Kurul kararları

1. [Marriott](#)
2. [Holiday Inn İstanbul Şişli](#)
3. [Halk Sigorta](#)
4. [Penti](#)
5. [Yalova Belediyesi](#)
6. [Aviva Sigorta](#)
7. [N11.com](#)
8. [Denizbank](#)
9. [Vodafone](#)
10. [Vatan Bilgisayar](#)
11. [Kariyer.net](#)
12. [Hukuka aykırı işleme](#)
13. [İş Bankası](#)
14. [Telefon mesajı](#)

İhlallerin bildirilmesi yasal zorunluluktur.

- ❑ Kişisel Verilerin ihlali görülmesi durumunda,
- ❑ Bir arkadaşımızın hatalı davranışını gördüğümüz zaman,
- ❑ Şüpheli SMS, e-posta mesajları alıyorsak,
- ❑ Bilgilerimize birilerinin eriştiğinden şüpheleniyorsak,
- ❑ Bilgisayarımız aniden yavaşladı veya ekranımızda beklenmedik pencereler açılıyorsa,
- ❑ Sorumluları bilgilendirmeliyiz.



Sosyal medya kullanımı

- ❑ Her gün eğlence ve sosyalleşme amaçlı ortalama 4 saat internet/sosyal medya kullanılıyor. Gençlerde bu süre yaşlılara göre en az iki kat fazla.
- ❑ Sosyal medya kullanım oranları
 - ❑ %89 Facebook
 - ❑ %82 Instagram
 - ❑ %70 Youtube
 - ❑ %55 Twitter
 - ❑ %20 LinkedIn
 - ❑ %17 Pinterest
 - ❑ %14 Çeşitli blog siteleri/uygulamaları
 - ❑ %13 Snapchat
- ❑ Global ölçekte her gün ortalama 68 Milyar Whatsapp mesajı atılıyor. Giderek artıyor.

KVKK biliniyor mu?

❑ KVKK hakkında ne kadar bilgi sahibiyiz?

- ❑ %15 Hiç duymamış
- ❑ %29 Sadece ismini duymuş
- ❑ %37 Çok az bilgi sahibi
- ❑ %14 Bilgi sahibi
- ❑ %5 Çok iyi biliyor

Şirketlere güveniliyor mu?

- Şirketlerin-Kurumların KVKK ya uyacağını düşünüyor musunuz?
 - %12 Kesinlikle güvenmiyor
 - %26 Güvenmiyor
 - %44 Nötr-Ne güveniyor ne güvenmiyor
 - %15 Güveniyor
 - %3 Kesinlikle güveniyor

Kişisel verileri paylaşmak istiyor muyuz?

- ❑ Kişisel verilerin kurum ve şirketler ile paylaşılmasına izin vermek istemeyenlerin oranı **%70**
- ❑ Buna rağmen SMS, telefon ve e-posta ile hiç ilişkisi olmadığı şirketlerden bildirim ve reklam alanların oranı **%86**


Kamu kurumları da uymalıdır





Kişisel veriler internet-Peru örneği



E-devlet, adli işlemler-olaylar

 **türkiye.gov.tr**


Bu hizmet Adalet Bakanlığı İşbirliği ile e-Devlet Kapısı altyapısı üzerinden sunulmaktadır.

Size nasıl yardım edebiliriz?   2


[Abonelik İptali](#) [Yazdır](#)

Bu sayfada, UYAP SMS Bilgi Sistemi'nde kayıtlı olan aboneliğiniz görüntülenir. Bu hizmeti kullanarak, yeni abonelik başvurusunda bulunabilir ve mevcut aboneliğinizi iptal edebilirsiniz.

UYAP SMS Bilgi Sistemi Abonelik Bilgileriniz

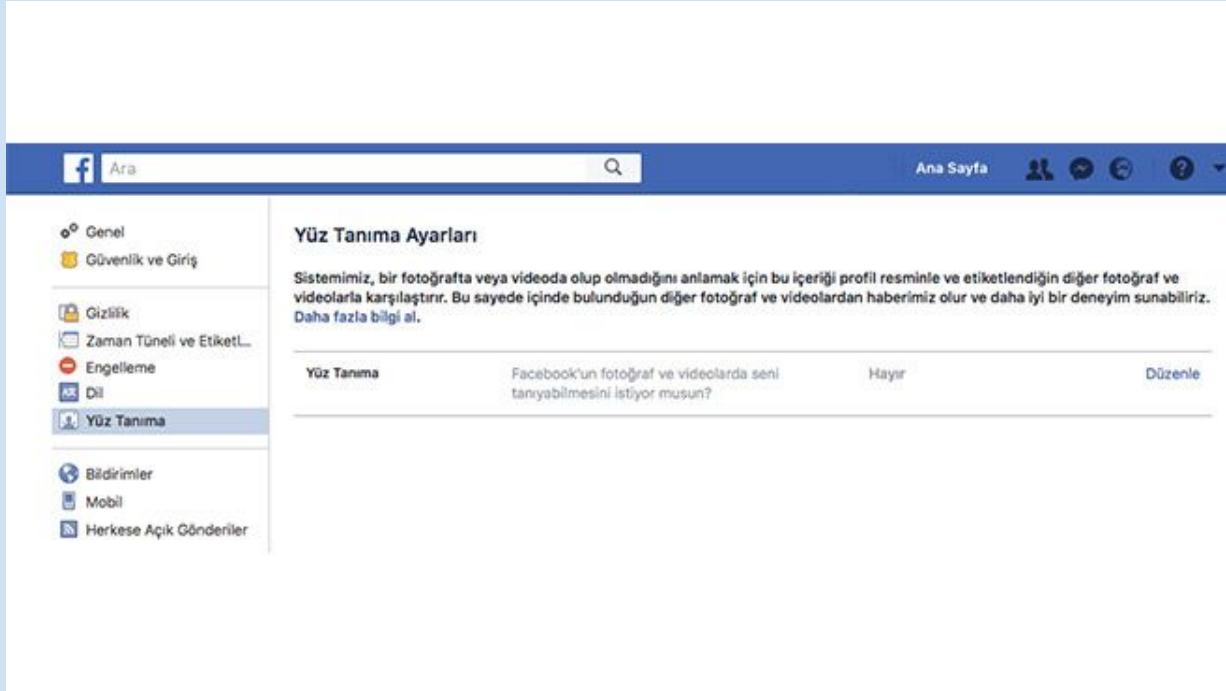
Cep Telefonu Numaranız	
Operatör Adı	TURKCELL
Paket Türü	Tam Paket
Bilgilendirme Seçeneği	Sadece Kendimle İlgili Yapılan İşlemler
SMS Ücreti	1 TL

TAM PAKET

 SMS Bilgi Sisteminin Tamamı TAM PAKET Abonelerine Hizmet Olarak Sunulmakta olup, TAM Pakete Abone Olan Kullanıcılara Sorgu SMS ile Erişilebilen Tüm Bilgiler Otomatik Bilgi Mesajı Gönderilecektir.

- SMS İçerikleri: <http://www.sms.uyap.gov.tr/icerikler.html>

Sosyal medya, facebook



The screenshot shows the Facebook settings page for 'Yüz Tanıma' (Face Recognition). The left sidebar contains various settings categories, with 'Yüz Tanıma' selected. The main content area displays the 'Yüz Tanıma Ayarları' section, which includes a description of the feature and a table of settings.

Yüz Tanıma Ayarları

Sistemimiz, bir fotoğrafta veya videoda olup olmadığını anlamak için bu içeriği profil resminle ve etiketlendiğin diğer fotoğraf ve videolarla karşılaştırır. Bu sayede içinde bulunduğun diğer fotoğraf ve videolardan haberimiz olur ve daha iyi bir deneyim sunabiliriz. [Daha fazla bilgi al.](#)

Yüz Tanıma	Facebook'un fotoğrafta ve videolarda seni tanıyabilmesini istiyor musun?	Hayır	Düzenle

PAYLAŞIM AYARLARI

Hiçbir hekim verilerimi görmesin (SMS kodu veya şifrematik ile onay zorunlu) ∨

Bu kutucuğu işaretlediğiniz takdirde, ayrıca bir paylaşım talebinde bulunmadığınız sürece aile hekiminiz ve diğer doktorlar sağlık kayıtlarınıza onayınız olmadan erişemez.

Dilediğiniz zaman bu seçeneği kapatarak ilgili erişimi onayınıza bağlayabilirsiniz.

Aile hekimim verilerimi görsün (Önerilen) ∧

Muayene olduğum hekim verilerimi görsün (Önerilen) ∧

Muayene olduğum hastanedeki tüm hekimler verilerimi görsün ∧

Sağlık Bakanlığındaki tüm hekimler verilerimi görsün ∧



Son



Teşekkürler.