VERİ İŞLEME, YÖNETME ve KORUMA
KVKK ve GDPR UYUMLULUĞU

BURÇAK ÜNSAL
burcak@unsal.com

ÜNSAL

- New York ve İstanbul Baroları
- CIPP-M, CIPP-E, CIPP-US
- Boğaziçi Üniversitesi Bilgi Sistemleri Araştıma Merkezi
- Doktora ve yüksek lisans dereceleri
- Hukuk, Fen Bilimleri, Bilgisayar Mühendisliği, İşletme, Şehir Planlaması, Felsefe
- ABD, AB, Japonya ve Türkiye'de fiili hukuk uygulaması

Dell / EMC, SAS, Logo Yazılım, Mikro Yazılım, WiseTech/Ulukom AirTies

Xanadu, Odeon, Wyndham Levent, Özdilek, ISG Hotel, Otium

Diageo Mey İçki, Tuborg, Coca Cola

Gen İlaç, Gen Era,Sophia Genetics Genetik Teşhis, Analiz Labratuvarları, Omron, BectonDickinson

Sabiha Gökçen Havalimanı, ICA Yavuz Sultan Selim Köprüsü ve Bağlantı Yolları

Dentsu Aegis, EuroMessage

Huobi Crypto Currency Borsası, Marsh Sigorta

Rollmech Otomotiv, Faydasıçok

NEC, Minerva

Google, YouTube, Yandex, Videomite, MobileX

METODOLOJİ

ÜNSAL

1. Veri niye önemli?
2. Mevzuat ne amaçlıyor?
3. Cezalar neler?
4. Kişisel Veri Koruma Kurumu Kim?
5. Mevzuat çerçevesinde kişisel veri ve temel kavramlar
6. Veri Sorumlusunun Yükümlülükleri
7. **Kanuna uyum gerçekten mümkün mü, nasıl?**
8. AB Genel Veri Koruma Yönetmeliği

VERİ NİYE ÖNEMLİ

ÜNSAL

Bırakılan dijital ayak izi

Veriyi nasıl ve ne karşılığı sağlıyoruz?

Nasıl ticari meta haline geliyoruz?

Nasıl siyasi profillemeye tabi tutuluyoruz?

Devlet niye müdahil oluyor?

Sadece KVKK bilmek yeterli mi?

MEVZUAT NE AMAÇLIYOR

6698 sayılı Kişisel Verilerin Korunması Kanunu (**"KVKK"**)
7 Nisan 2016 tarihinde yürürlüğe girmiştir.

KVKK, başta özel hayatın gizliliği olmak üzere **KİŞİLERİN TEMEL HAK VE ÖZGÜRLÜKLERİNİN KORUNMASI** ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları usul ve esasları belirlemektir.

KVKK'da belirtilen yükümlülüklere ve kurallara uyulmaması halinde kişilere **1.000.000 TL'ye kadar varan idari para cezası** ve/veya **1 ve 4,5 yıl arası hapis cezası** öngörülmektedir.

CEZALAR NELER?

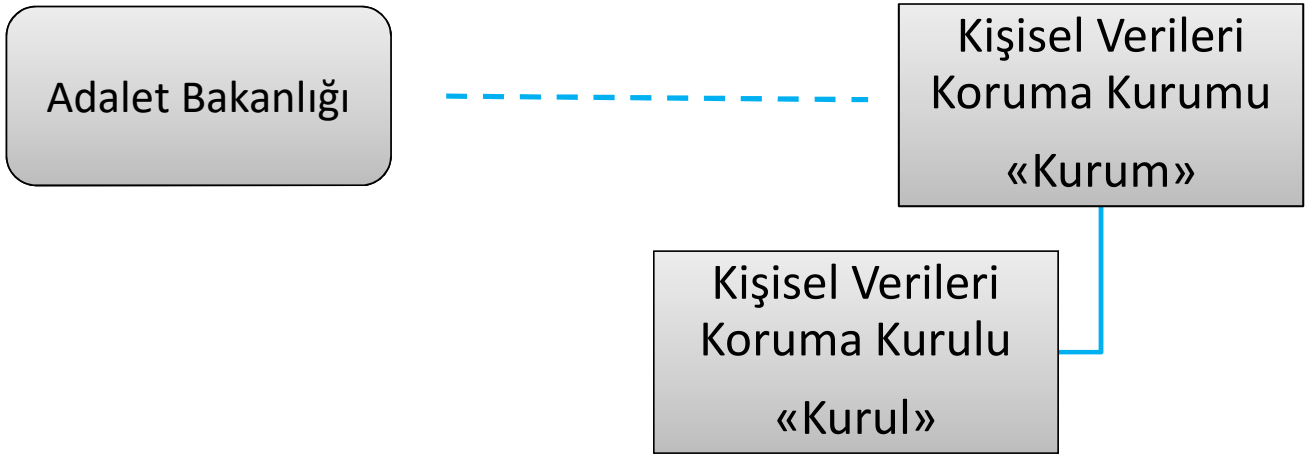
SUÇLAR

- Aşağıdaki suçların işlenmesi halinde Türk Ceza Kanunu'nda **en az bir en fazla dört buçuk yıl** olmak üzere hapis cezaları öngörülmüştür:
- Kanun hükümlerine aykırı olarak kişisel verileri kaydetme suçunun işlenmesi,
- Kanun hükümlerine aykırı olarak kişisel verileri bir başkasına verme, yayma veya ele geçirme suçunun işlenmesi,
- Kanun hükümlerine aykırı olarak kişisel verileri depolama, muhafaza etme, değiştirme, yeniden düzenleme, açıklama, elde edilebilir hale getirme, sınıflandırma ya da kullanılmasını engelleme ya da üçüncü kişilere aktarma suçlarının işlenmesi,
- Veri sorumlusunun kanun hükümlerine aykırı olarak kişisel verileri silmemesi veya anonim hale getirmemesi,

KABAHATLER

- Aydınlatma yükümlülüğüne aykırılık halinde 1.000 ila 100.000 TL,
- Veri güvenliğine ilişkin yükümlülüklere aykırılık halinde 15.000 ila 1.000.000 TL,
- Kurul tarafından verilen kararları yerine getirmeme halinde 25.000 ila 1.000.000 TL,
- Sicile kayıt ve bildirim yükümlülüğüne aykırı hareket etme halinde 20.000 ila 1.000.000 TL idari para cezası.

KİŞİSEL VERİLERİ KORUMA KURUMU



- Kurum Adalet Bakanlığı ile ilişkilidir.
- Kurum'un merkezi Ankara'dadır.
- İdari ve mali özerkliğe sahip kamu tüzel kişisidir.
- Kurum'un 9 Kurul üyesi bulunmaktadır.

Kurum’un Ana Binası

Kurum’un Resmi İnternet Sitesi

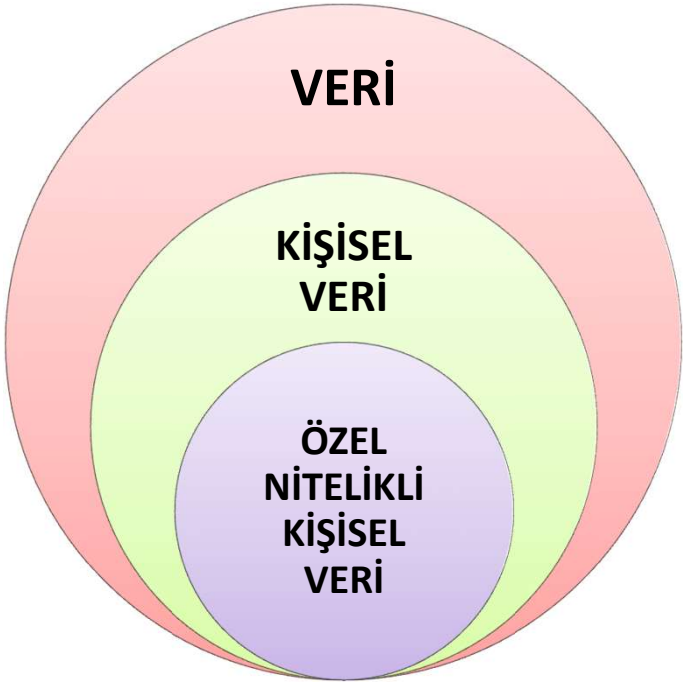
KİŞİSEL VERİLERE İLİŞKİN TEMEL KAVRAMLAR

ÜNSAL

- **KİŞİSEL VERİ:** Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir. Örneğin; ad, soyad, e-posta adresi, telefon numarası, çalışan sicil numarası, doğum tarihi, hobileri, iş deneyimleri, IP adresi, ayakkabı numarası vs. **Önemli olan o veri üzerinden kişinin tespit edilebilmesidir.**

- **ÖZEL NİTELİKLİ KİŞİSEL VERİ:** Hassas nitelikleri itibarıyla özel korumaya muhtaç verilerdir. Özel nitelikli kişisel veriler kanunda sınırlı olarak sayılmıştır:

  - Irk
  - Etnik köken
  - **Siyasi düşüncesi**
  - **Felsefi inancı**
  - **Dini, mezhebi veya diğer inançları**
  - **Kılık, kıyafet**
  - **Dernek, vakıf ya da sendika üyeliği**
  - **Kişinin sağlığı veya cinsel hayatıyla ilgili veriler:** *Hastalığı, engellilik durumu, kan grubu bilgisi*
  - Ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler: *Adli sicil kaydı*
  - Biyometrik veri: *Retina, iris, parmak izi bilgisi, yüz taraması, avuç içi izleri*
  - Genetik veri: *Gen haritası, DNA dizilimi*

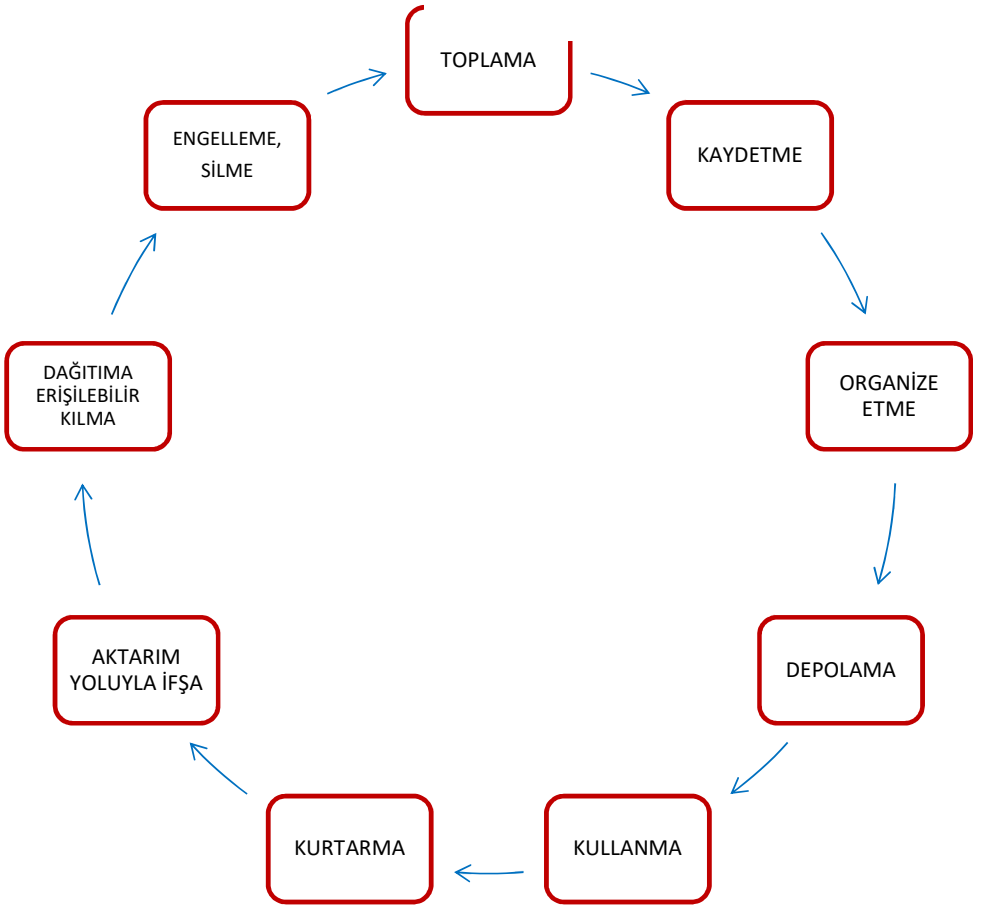


KİŞİSEL VERİLERİN İŞLENMESİ:

Kişisel verilerin elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi kişisel veriye "temas edilen" her faaliyet, kişisel verilerin işlenmesi anlamına gelmektedir.

Kişisel verilerin işlenmesine örnekler:

- Şirketin sitesinden iletişime geçmek isteyen kişilerden iletişim bilgilerinin alınması (toplama)
- Şikayette bulunan müşterilerin talep ve şikayet bilgilerinin iş ortakları ile paylaşılması (paylaşma)
- Personel veya üçüncü taraf kişilerin ad, soyad ve iletişim bilgilerinin Excel dosyasında tutulması (saklama)



Kanun Kimlere Yükümlülük Getirmektedir?

Kanun, kişisel verileri işleyen Veri Sorumlusuna ve Veri İşleyenlere birtakım yükümlülükler getirmektedir.

İlgili Kişi	Veri İşleyen	Veri Sorumlusu
		
Kişisel verisi işlenen gerçek kişiyi ifade etmektedir.	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

Örnek: Şirket, insan kaynakları faaliyetlerini gerçekleştirmek amacıyla çalışanlara ait kişisel verileri işlerken **veri sorumlusu** olacaktır. Şirketin bu verileri bulut ortamında saklamak istemesi halinde **bulut hizmeti sağlayıcısı firma veri işleyen** olacaktır. Firma, şirket adına ve şirketin belirlediği yetkiye dayanarak bu verileri işlemektedir.

VERİ SORUMLUSU YÜKÜMLÜLÜKLE

ÜNSAL

1. Kişisel Verileri Kanuna Uygun Olarak İşleme (Genel İlkelere, İşleme ve Aktarma Şartlarına Uyma)
2. İlgili Kişileri Aydınlatma
3. İlgili Kişilerin Başvurularını Yanıtlama
4. VERBİS-Veri Sorumluları Siciline Kaydolma (**Kişisel Veri Envanterinin devamlı güncel tutulması)**
5. Kişisel Verileri İmha Etme
6. Veri Güvenliğini Sağlama
7. Kurul Kararlarına Uyma

İŞLENME İLKELERİ VE ESASLARI

Şirket çalışanları, Şirket içerisinde ticari ve idari faaliyetlerin yerine getirilmesi kapsamında; müşterilerin, diğer çalışanların, üst düzey yöneticilerin, iş ortaklarının, hissedarların kişisel verilerine erişebilmekte ve bu verileri işleyebilmektedir.

Şirket çalışanları elde ettikleri kişisel verileri aşağıdaki **genel ilkelere** uygun olarak işlemelidir.

1. Hukuka ve dürüstlük kuralının öngördüğü biçimde işlemelidir.
2. İşlenme amaçları ile bağlantılı, sınırlı ve ölçülü olarak işlemelidir. *(**Örn.** İşe başvuran adaylardan, sadece başvurusunu değerlendirebilmek için gerekli olan bilgiler alınmalıdır.)*
3. Doğru ve gerektiğinde güncel olarak işlemelidir. *(**Örn**. Müşteri irtibat kişilerinin kimlik ve iletişim bilgileri doğru ve güncel olmalıdır.)*
4. Belirli açık ve meşru işleme amaçları ile işlemelidir. *(**Örn.** Çalışanlar,* şirket *süreçleri üzerinden elde ettikleri kişisel verileri kişisel amaçları için kullanmamalıdır.)*
5. Saklama süresine uygun olarak işlemelidir.

KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN ŞARTLAR

ÜNSAL

Şirket çalışanları aşağıdaki şartlardan birinin bulunması halinde ilgili kişilerin kişisel verilerini işleyebilecektir.

1) KİŞİNİN AÇIK RIZA VERMESİ

Açık rıza, herhangi bir şekil şartı olmaksızın (sözlü, yazılı, kutucuğun işaretlenmesi vs.) kişilerden alınabilmektedir. Açık rızanın geçerli olabilmesi için rızanın,

- Belirli bir konuya ilişkin olması (belirli bir konu ile sınırlı olması, açık uçlu veya belirsiz olmaması)
- Bilgilendirmeye dayanması (kişinin konu ve sonuçları üzerinde tam bilgi sahibi olması)
- Özgür iradeyle açıklanması (kişinin iradesini sakatlayan cebir, tehdit ve hile gibi fiiller olmaması, kişinin onay vereceği kısmın önceden onaylanmış/tikli/işaretlenmiş olmaması) gerekmektedir.

Örnek: Şirket internet sayfasından telefon numarasını giren ziyaretçilere şirket hakkında pazarlama e-postalarının yollanabilmesi için bu kişilerin açık rıza vermesi gerekmektedir.

☑ Kişisel verilerimin Açık Rıza Metninde belirtilen şirkete ilişkin pazarlama, tanıtım ve bilgilendirme yapılması amacıyla işlenmesine açık rıza veriyorum.

KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN ŞARTLAR

ÜNSAL

2) KANUNLARDA AÇIKÇA ÖNGÖRÜLMESİ

Örnek: Şirket, İş Kanunu uyarınca çalışanların özlük dosyasını tutmakla yükümlüdür. Bu yükümlülüğünü yerine getirmek amacıyla çalışanların birtakım kişisel verilerini işleyebilecektir.

3) FİİLİ İMKANSIZLIK SEBEBİYLE İLGİLİNİN AÇIK RIZASININ ALINMAMASI

Örnek: Şirket, ofislerinde kaza geçiren veya bayılan kişilerin kimlik bilgileri sağlık hizmetinin verilebilmesi için sağlık mensuplarına verebilecektir. Kendinde olmayan kişinin sağlığına kavuşması adına yapılan bu paylaşım için açık rıza alınmasına gerek yoktur.

4) SÖZLEŞMENİN KURULMASI VEYA İFASIYLA DOĞRUDAN İLGİLİ OLMASI

Örnek: Müşteriler ile yapılan sözleşmedeki yükümlülüklerin yerine getirilmesi kapsamında müşterilerin ad-soyad, telefon numaralarının işlenmesi bu kapsamda değerlendirilebilecektir.

KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN ŞARTLAR

ÜNSAL

5) HUKUKİ YÜKÜMLÜLÜĞÜN YERİNE GETİRME GEREKLİLİĞİ

Örnek: Şirket, şirketin internetini kullanan misafirlerin erişim loglarını 5651 sayılı Kanun uyarınca tutmakla yükümlüdür. Bu logların tutulması için ziyaretçilerden açık rıza alınmasına gerek yoktur.

6) KİŞİSEL VERİLERİN İLGİLİ KİŞİ TARAFINDAN ALENİLEŞTİRİLMESİ

Örnek: Şirketin potansiyel iş ortakları, iletişim bilgilerini internet sitelerinde yayınlaması (alenileştirmesi) halinde, ilgili sitede bu bilgiler bulunduğu sürece şirket bu kişilerin iletişim bilgileri iş ilişkisine girmek amacıyla işleyebilecektir.

7) BİR HAKKIN TESİSİ VE KORUNMASI İÇİN VERİ İŞLEMENİN GEREKLİ OLMASI

Örnek: Şirket, ödemenin yapıldığına dair kanıt oluşturacak belgeleri saklayabilir. Böylece şirket, ödemeyle ilgili ortaya çıkabilecek uyuşmazlıklarda, ödemeyi yaptığına dair kanıtı mahkemeye sunarak kendini savunabilir.

8) ŞİRKETİN MEŞRU MENFAATİ İÇİN VERİ İŞLEMENİN ZORUNLU OLMASI

Örnek: Şirket, bina ve tesislerinin güvenliğini sağlamak amacıyla bu yerleri CCTV ile izleyebilir.

KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN ŞARTLAR

ÜNSAL

İlgili kişinin açık rızası var ise**; özel nitelikli kişisel verisi (ÖNKV)** işlenebilmektedir.

İlgili kişinin **açık rızası yok ise**;

- *İlgili kişinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel veriler*, ***kanunlarda öngörülen hallerde*** *işlenebilmektedir.*

- *İlgili kişinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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 işlenebilmektedir.*

Örnek: İşe başvuran kişilerin CV'lerinde dernek ve vakıf üyeliği bilgisi yer alabilmektedir.

KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASI

ÜNSAL

Kişiler açık rıza verdiği takdirde, kişisel verileri üçüncü kişiler ile paylaşılabilecektir.

Aşağıdaki halde, kişilerden **açık rıza alınmasına gerek olmayacaktır**:

Kişisel verilerin aktarılmasına ilişkin hukuki şartlardan birinin varlığı (örneğin sözleşmenin kurulması için gerekli olması vs.)

+

Kişisel verinin aktarılacağı yabancı ülkenin **güvenli ülke ilan edilmesi**

veya

Kişisel verinin aktarılacağı ülkede yeterli koruma bulunmaması halinde o ülkedeki veri sorumlularının yazılı taahhütte bulunması ve Kurul'un aktarıma izin vermesi

Açık rıza aranmaz.

Güvenli ülkeler henüz ilan **EDİLMEDİ!!**

AYDINLATMA YÜKÜMLÜLÜĞÜ

Çalışanlar ilgili kişilerden açık rıza alınıp alınmadığına bakılmaksızın kişisel verileri işledikleri her süreç ile ilgili kişileri bilgilendirmelidir.

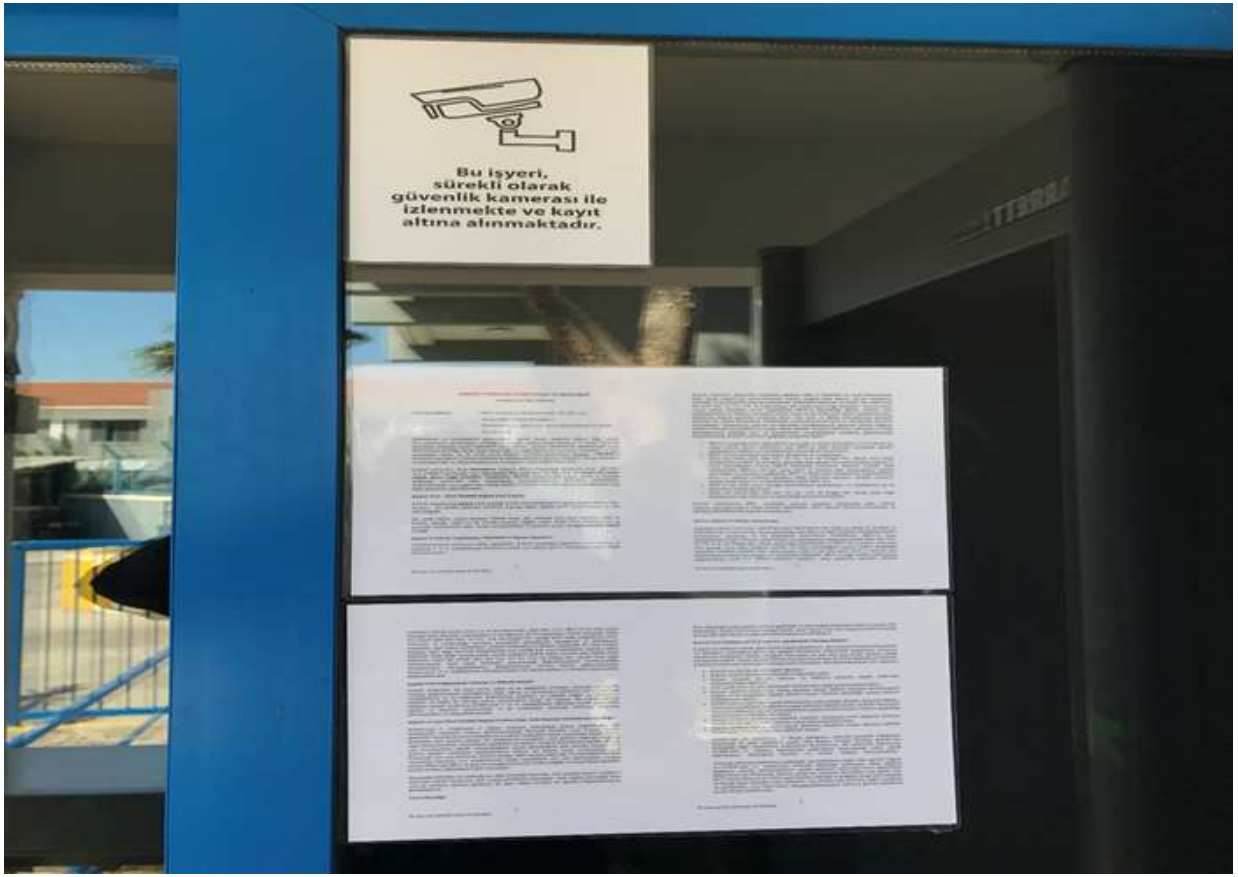
Aydınlatma metinleri şirket internet sitesi üzerinden ulaşılabilir hale getirilebilecektir.

Aydınlatma ve açık rıza metinlerinin veya bu metinlerin bulunduğu internet sayfası linklerinin, şirketin talimatlarına uygun olarak ilgili kişiler ile paylaşılması gerekmektedir.

Örnek: Müşterilere ait kişisel verileri işleyebilmek için bu müşterilere Aydınlatma Metni sunulmalıdır.

AYDINLATMA YÜKÜMLÜLÜĞÜ

ÜNSAL



İLGİLİ KİŞİLERİN BAŞVURULARINI YANITLAMA

ÜNSAL

Bilgi edinme	• Kişiler, verilerinin işlenme amacına ilişkin de bilgi talep edebilecektir.
Zararın giderilmesini isteme	• Kanuna aykırı olarak veri işlenmesi sonucunda maddi veya manevi zarar görenler, genel hükümlerine uygun olarak tazminat talep edebilirler.
Eksik veya yanlışlığın düzeltilmesi	• Bireyler, kişisel verilerinin eksik veya yanlış işlenmiş olması hâlinde düzeltme talep etme hakkını elde edecektir. Veriler yalnızca otomatik yöntemlerle işleniyorsa, kişiler sonuca itiraz edebilecektir.
Verilerin aktarıldığı üçüncü kişileri öğrenme	• Herkes, kendisine ait verilerin yurt içinde veya yurt dışında aktarıldığı üçüncü kişileri bilme hakkına sahip olacaktır.
Üçüncü kişilere bildirim yapılması	• Herkes, verileri hakkında düzeltme veya silme gerektiren hallerin ilgili üçüncü taraflara bildirilmesini isteyebilir.
Silinme, anonimleştirilme veya yok edilmeyi talep etme	• Herkes, kanunda öngörülen şartlara uygun olarak işlenmeyen verilerin silinmesini veya yok edilmesini talep edebilecektir.

İlgili kişiler bu haklarına ilişkin şirkete başvurabilecektir. Bu başvurular, alındıktan sonra en geç 30 gün içinde yanıtlanmalıdır.

Çalışanlar, bu tür bir başvuru aldıklarında *kvkk@xxxxx.com* adresine e-posta ile, şirket KVK Komitesi üyesine haber vermelidir.

İLGİLİ KİŞİLERİN BAŞVURULARINI YANITLAMA

Şirket, ilgili kişi başvurularını **30 gün içinde** yanıtlamakla yükümlüdür. Aksi takdirde **KURULA ŞİKAYET!**

İlgili kişiler, başvuruları yapmak için

- İlgili Kişi/Veri Sahibi Başvuru Formunu dolduracak ve
- Formu belirtilen kanallar üzerinden gönderecek.

Aksi takdirde başvuru geri gönderilecektir ve kişi doğru kanallara yönlendirilecektir.

İLGİLİ KİŞİLERİN BAŞVURULARINI YANITLAMA

Başvuru usulünün ve içeriğinin incelenmesi için **azami 2 günlük süre**;

- Usulüne uygun gönderildi mi?
- İçeriğe uygun gönderildi mi?

Başvurunun ilgili departmanlara gönderilmesi için **azami 3 günlük süre**;

İlgili departmanların gelen talebi değerlendirmesi ve elde ettiği bilgileri şirket Kişisel Veri Koruma Komitesinin göndermesi için **azami 1,5 hafta süre**;

Şirket Kişisel Veri Koruma Komitesi (Veri Yönetimi Birimi)'nin e-posta adresinden, departmanlardan gelen değerlendirmeler üzerine cevap hazırlaması ve Veri Sahibine göndermesi için **azami 1,5 hafta süre**.

VERBİS'E KAYDOLMA

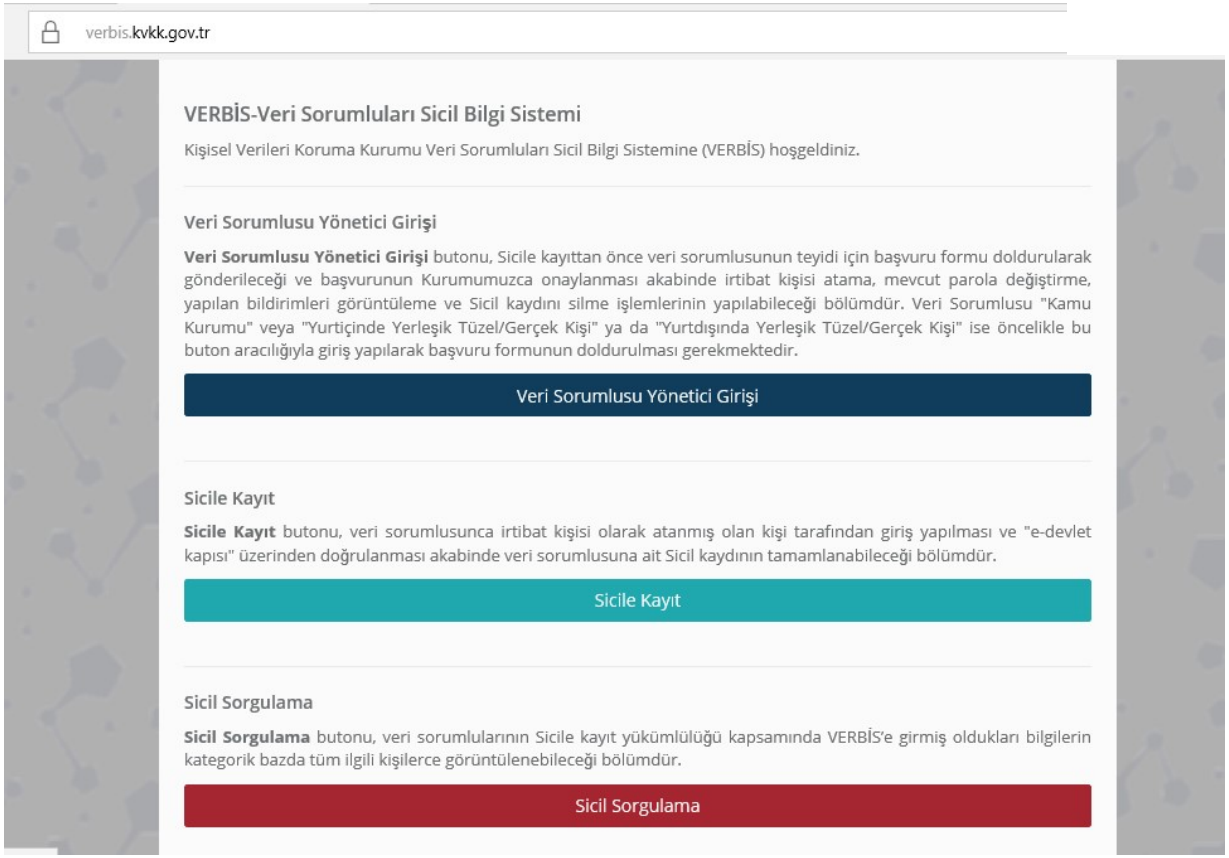
Kişisel Veri Envanteri; veri sorumlusu ve varsa yetkisinin kimlik ve adres bilgileri + kişisel verinin hangi amaçla işleneceği + veri konusu kişi ve veri kategorisi hakkında bilgi + kişisel verilerin aktarılabileceği alıcı veya alıcı grupları + yabancı ülkelere aktarımı öngörülen kişisel veriler + kişisel veri güvenliğine ilişkin alınan tedbirler + kişisel verilerin işlendikleri amaç için gerekli olan azami süre belirtilecek.

Sicile Kaydolunması: Şirket, VERBİS'te kayıt oluşturarak ve envanterdeki süreçlerini buradaki Sicil'e girecektir.

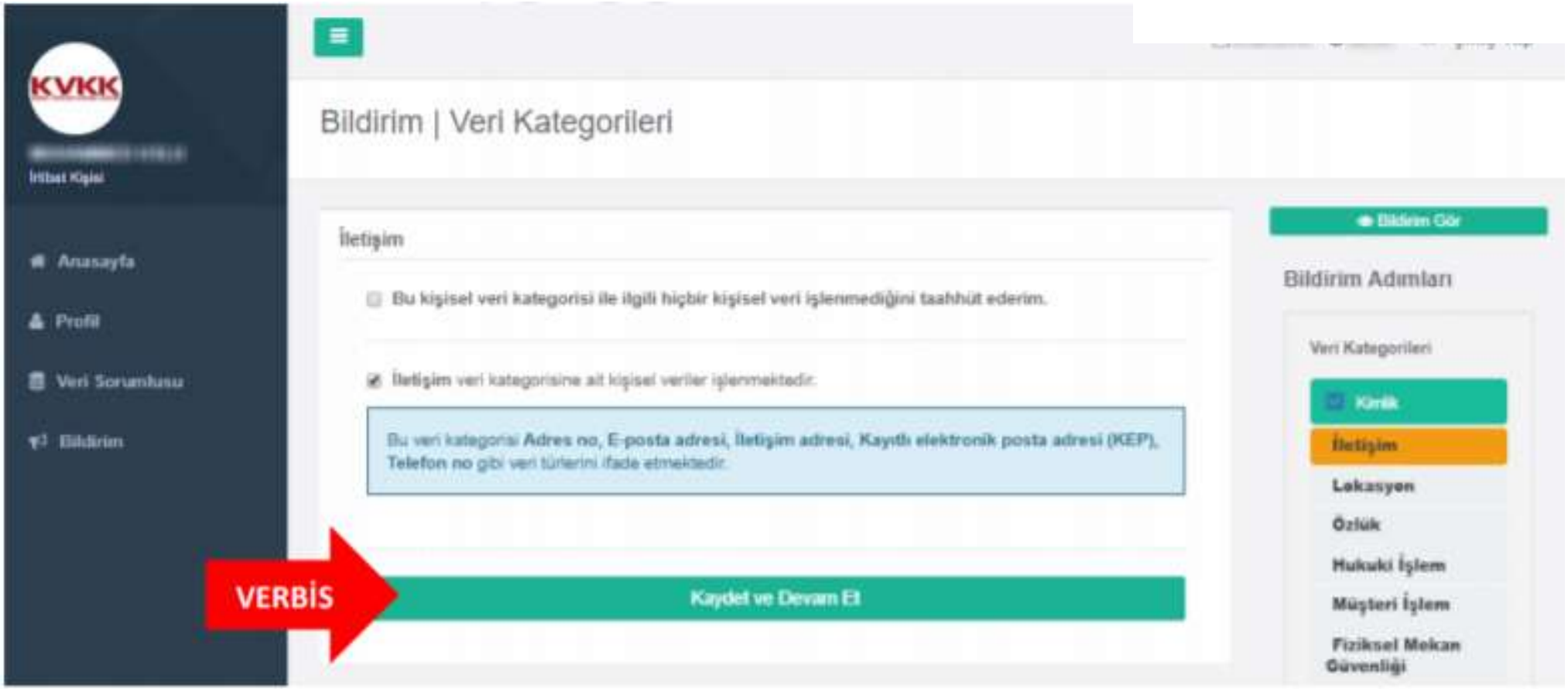
Envanterin Güncellenmesi: Envanterde değişiklik meydana gelirse derhal VERBİS'E bildirilecektir.

Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları bakımından
VERBİS'e kayıt için son tarih
30 Eylül 2019

VERBİS'E KAYDOLMA



VERBİS'E KAYDOLMA

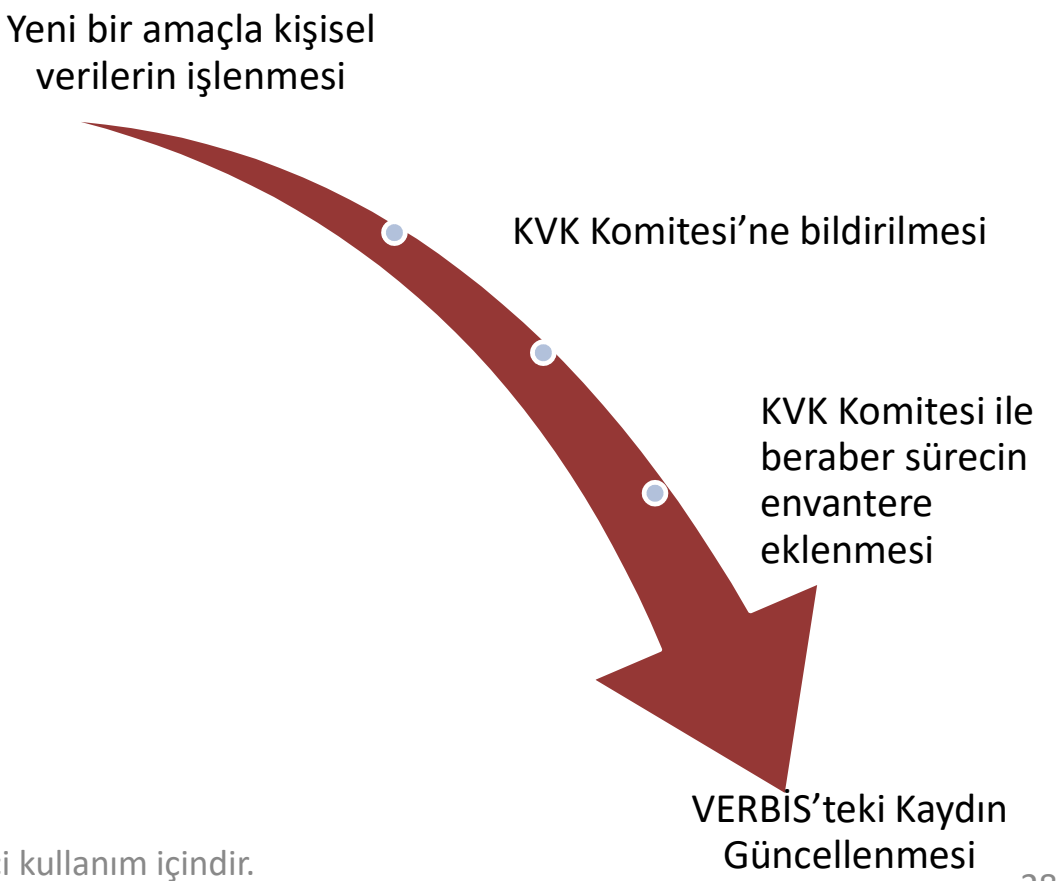


VERİ İŞLENEN YENİ SÜREÇLERİN BİLDİRİLMESİ

Departman bünyesinde
- yeni bir amaçla kişisel veri işlenmesi veya
- mevcut işleme sürecinde değişiklik meydana gelmesi halinde

İlgili KVK Komite üyesine veya KVK Komitesine bildirilmesi gerekmektedir.

Bu bildirim yapıldıktan sonra, çalışanlar envanter ve VERBİS kaydının yapılması için gerekli desteği ve işbirliğini göstermelidir.



KİŞİSEL VERİLERİ İMHA ETME

ÜNSAL

Hukuki yükümlülük

- Kişisel veri işleme amacı sona eren kişisel veriler silinmeli, yok edilmeli veya anonim hale getirilmelidir.

Süre matrisi

- Kişisel verilerin saklama amaçları, KVKK ve ilgili mevzuata uygun olarak, kişisel verileri saklama süreleri belirlenmelidir.

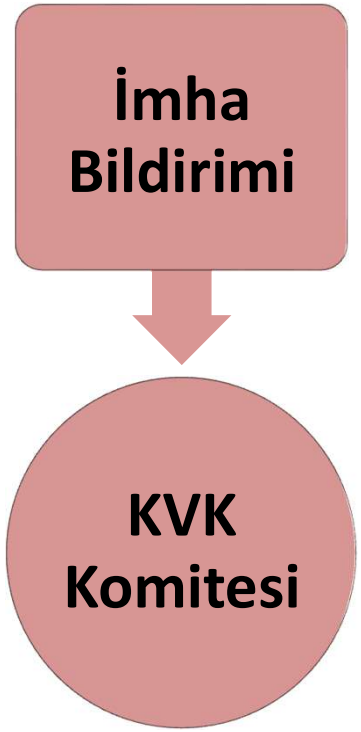
İmha işlemi

- Saklama süresi sona erdiği tespit edilen kişisel veriler imha edilmelidir.

KİŞİSEL VERİLERİ İMHA ETME

ÜNSAL

Şirket çalışanları, kendisine belirtilen saklama sürelerini dikkate alarak imha edilmesi gereken kişisel verileri tespit etmeli ve KVK Komitesini bilgilendirmelidir. Departman çalışanları ve Komite üyeleri bu süreçte beraber çalışmalı ve birbirlerini gerekli desteği vermelidir.



SÜRE MATRİSİ ÖRNEĞİ

KİŞİSEL VERİ KATEGORİSİ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Sözleşme ilişkilerinde (TBK genel zamanaşımı süresi)	Ticari ilişkinin sona ermesinden itibaren 10 yıl	Sürenin sona ermesinden itibaren 6 ayda bir gerçekleşen ilk periyodik işlemde
Tüketiciye mal/hizmet verilmesi ilişkilerinde	Malın tüketiciye verilmesi ve/veya hizmetin ifa edilmesinden itibaren 2 yıl	aynı
Çalışan adaylarının iş başvuruları	2 yıl	aynı
Personel özlük işleri	İş ilişkisinin sona ermesinden itibaren 10 yıl	aynı
İş sağlığı ve güvenliği faaliyetleri	İş ilişkisinin sona ermesinden itibaren 10 yıl, sağlık raporları iş ilişkisinin sona ermesinden itibaren 15 yıl	aynı
Çalışanların ücrete ilişkin haklarına dair kişisel veriler	5 yıl	aynı
Erişim Kayıtları/Trafik Bilgileri (İnternet Toplu İnternet Kullanım Sağlayıcısı olarak)	2 yıl	aynı

VERİ GÜVENLİĞİNİ SAĞLAMA YÜKÜMLÜLÜĞÜ

ÜNSAL

Kanunun veri güvenliğine ilişkin 12. maddesine göre veri sorumlusu,

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- Kişisel verilerin muhafazasını sağlamak ile yükümlüdür.

Bu kapsamda:

- Veri sorumlusu, güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.
- Veri sorumlusu, kendi kurum veya kuruluşunda Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

OLASI VERİ İHLALLERİNİN BİLDİRİLMESİ

ÜNSAL

Olası İhlal ve İhlal Şüphelerinin Bildirimi :

- **KVK Komitesine derhal bildirim**: Kişisel verilerin yetkisiz erişimi, ifşa edilmesi, kaybolması veya çalınması halinde durumun derhal KVK Komitesi'ne bildirilmesi gerekmektedir. (*örnek2@unsallaw.com*)

KVKK ve GDPR: 72 saat içinde Kuruma bildirim!

VERİ İHLALİ BİLDİRİM FORMU

Verilerin, başkaları tarafından elde edilmesi hâlinde, VERİ SORUMLUSU en kısa sürede ilgilisine ve Kurul'a bildirimde bulunması gerekir.

Buna istinaden Kurul tarafından "Kişisel Veri İhlal Bildirim Form"unun kullanılmasına karar verilmiş olup söz konusu formun sadece veri ihlali gerçekleşen VERİ SORUMLULARI tarafından doldurulması gerekmektedir.

VERİ İHLALİ BİLDİRİM FORMU

ÜNSAL

KİŞİSEL VERİ İHLALİ BİLDİRİMİ

A) HAKKINIZDA

1. Veri sorumlusunun unvanı/ ismi:
2. Veri sorumlusunun adresi:
3. Bu bildirimi hazırlayan kişinin
   Adı ve Soyadı:
   Görevi:
   E-postası:
   Telefonu:

B) İHLAL HAKKINDA

1. Bildirim türü : ☐ İlk bildirim ☐ Takip bildirimi:.....
   (Takip Bildirimlerinde varsa takip numarasını ekleyeniz)
2. İhlalin gerçekleşme tarihi ve saati :
3. İhlalin tespit tarihi ve saati:
4. İhlal hakkında bilgi veriniz.

5. İhlalin kaynağı *(Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz)*

- ☐ Kişisel verilerin yanlış alıcılara gönderilmesi
- ☐ Belge/cihaz hırsızlığı veya kaybolması
- ☐ Verilerin güvensiz ortamlarda depolanması
- ☐ Zararlı yazılımlar
- ☐ Sosyal mühendislik
- ☐ Sabotaj
- ☐ Kaza/ İhmal
- ☐ Diğer (Cevabınızı detaylandırınız) :

6. İhlalden etkilenen kişisel veri kategorileri
(Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz)

Kişisel Veri	*Özel Nitelikli Kişisel Veri*
☐ Kimlik	☐ Irk ve Etnik Köken
☐ İletişim	☐ Siyasi Düşünce
☐ Lokasyon	☐ Felsefi İnanç, Din, Mezhep ve Diğer İnançlar
☐ Özlük	☐ Kılık ve Kıyafet
☐ Hukuki İşlem	☐ Dernek Üyeliği
☐ Müşteri İşlem	☐ Vakıf Üyeliği
☐ Fiziksel Mekan Güvenliği	☐ Sendika Üyeliği
☐ İşlem Güvenliği	☐ Sağlık Bilgileri
☐ Risk Yönetimi	☐ Cinsel Hayat
☐ Finans	☐ Ceza Mahkumiyeti ve Güvenlik Tedbirleri
☐ Mesleki Deneyim	☐ Biyometrik Veri
☐ Pazarlama	☐ Genetik Veri
☐ Görsel ve İşitsel Kayıtlar	
☐ Diğer (Detayları belirtiniz) :	

4. İyileşme zamanı ile ilgili bilgiler

☐ Normal	Var olan kaynaklarınızı kullanacaksınız ve iyileşme zamanınızı öngörebiliyorsunuz.
☐ Destekli	Ek kaynaklar kullanacaksınız ve iyileşme zamanınızı öngörebiliyorsunuz.
☐ Uzatılmış	Ek kaynaklara ihtiyacınız var ve iyileşme zamanınızı öngöremiyorsunuz
☐ Geri Dönülmez	Saldırıdan geri dönüş imkansız (örn. yedekler yok edilmiş)
☐ Tamamlanmış	İyileşme tamamlandı

D) VARSA SİBER SALDIRIYA ÖZGÜ SONUÇLAR

1. Bilgi sistemleriniz siber saldırıdan etkilendi mi?
   ☐ Evet
   ☐ Hayır

2. Evet seçeneğini işaretlediyseniz, siber saldırı sonucu gerçekleşen ihlal unsurunu belirtiniz. *(Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz)*
   ☐ Veri gizliliği ☐ Veri bütünlüğü
   ☐ Veriye erişim ☐ Diğer (Cevabınızı detaylandırınız) :

3. Siber saldırıların organizasyonunuza olan etkileri

Etkisi	*Açıklama*
☐ Yüksek	Tüm kullanıcılarınıza bilgi sistemleri aracılığıyla vermiş olduğunuz hizmetleri sunma yetinizi kaybettiniz.
☐ Orta	Bazı kullanıcılarınıza bilgi sistemleri aracılığıyla vermiş olduğunuz hizmetleri sunma yetinizi kaybettiniz.
☐ Düşük	Herhangi bir etkinlik kaybı söz konusu değil ya da çok düşük bir etkinlik kaybı var ve tüm kullanıcılarınıza bilgi sistemleri aracılığıyla vermiş olduğunuz hizmetleri sunabiliyorsunuz.
☐ Bilinmiyor	

4. İyileşme zamanı ile ilgili bilgiler

☐ Normal	Var olan kaynaklarınızı kullanacaksınız ve iyileşme zamanınızı öngörebiliyorsunuz.
☐ Destekli	Ek bilişim kaynakları kullanacaksınız ve iyileşme zamanınızı öngörebiliyorsunuz.
☐ Uzatılmış	Ek bilişim kaynaklarına ihtiyacınız var ve iyileşme zamanınızı öngöremiyorsunuz
☐ Geri Dönülmez	Saldırıdan geri dönüş imkansız (örn. yedekler yok edilmiş)
☐ Tamamlanmış	İyileşme tamamlandı

E) ÖNLEMLER

1. İhlal ile ilgili olan çalışanlar son bir yıl içerisinde kişisel veri koruma eğitimi aldı mı?
   ☐ Evet ☐ Hayır

2. Bu tür ihlalleri engellemek için ihlalin gerçekleşmesinden önce almış olduğunuz idari ve teknik tedbirlerini belirtiniz.

3. İhlalin sonucu olarak almış olduğunuz veya almayı planladığınız idari ve teknik tedbirleri belirtiniz. *(Problemi çözmek ve olumsuz etkilerini ortadan kaldırmak adına almış olduğunuz önlemleri belirtiniz. örneğin yanlışlıkla gönderilmiş olan verilerin yok edilmesi, parolaların güvenliğinin sağlanması, veri güvenliği eğitimi planlanması vb.)*

KURUL KARARLARINA UYMA

Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlaıın yaygın olduğunun tespit edilmesi hâlinde Kurul, bu konuda ilke kararı alır ve bu kararı yayımlar.

Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası uygulanabilecektir.

Örneğin, Teknik Servis Hizmeti Veren Bir Firma'ya Kanun'un 15. maddesine aykırı olarak ilgili kararı yerine getirmemesi üzerine 50.000 TL para cezasına ve sorgulama yapılan sistemin ivedilikle kapatılmasına karar verilmiştir.

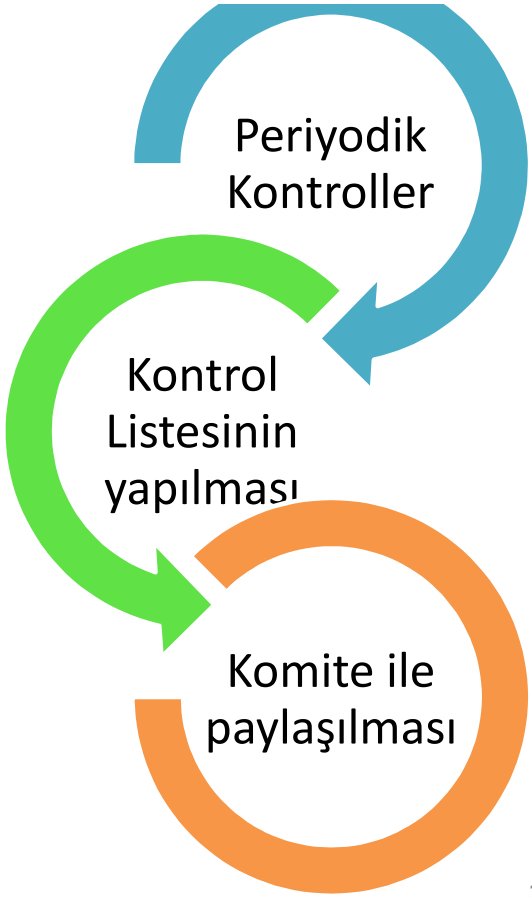
KANUNA UYUM KAPSAMINDA ÖNERİLERİMİZ

ÜNSAL

1. Şirket İçerisinde KVKK Komitesi'nin Kurulması
2. Komitenin ve yöneticilerin sürekli eğitimi
3. Çalışanların sürekli eğitimi
4. Veri haritalandırmasının yapılması ve etki analizinin yapılması
5. Riskli Süreçler İçin Veri Koruma Etki Analizi Uygulanması
6. Verilerin elektronik ve fiziksel güvenliğinin sağlanması
7. İhlal ve sızmaların engellenmesi için teknik ve idari tedbirlerin alınması
8. Veri işleme ve yönetim süreçlerinin ve enstrümanlarının kullanılması

ŞİRKET KİŞİSEL VERİLERİ KORUMA KOMİTESİ

- **Komite**, Kişisel Verilerin Korunması Kanunu'na uyumluluğunun sürekliliğini sağlamak ve bunu denetlemekle görevlidir.
- Kişisel verilerin işlenmesi ve korunması süreci **yaşayan bir süreç** olması sebebiyle **YENİ DURUMLAR** ile karşılaşılabilecektir.
- Bu durumların sürece uygun yürütülmesi amacıyla **periyodik kontroller** yapılması gerekmektedir.
- Bu kontrolleri gerçekleştirme amacıyla bir **Kontrol Listesi oluşturulmalıdır.**

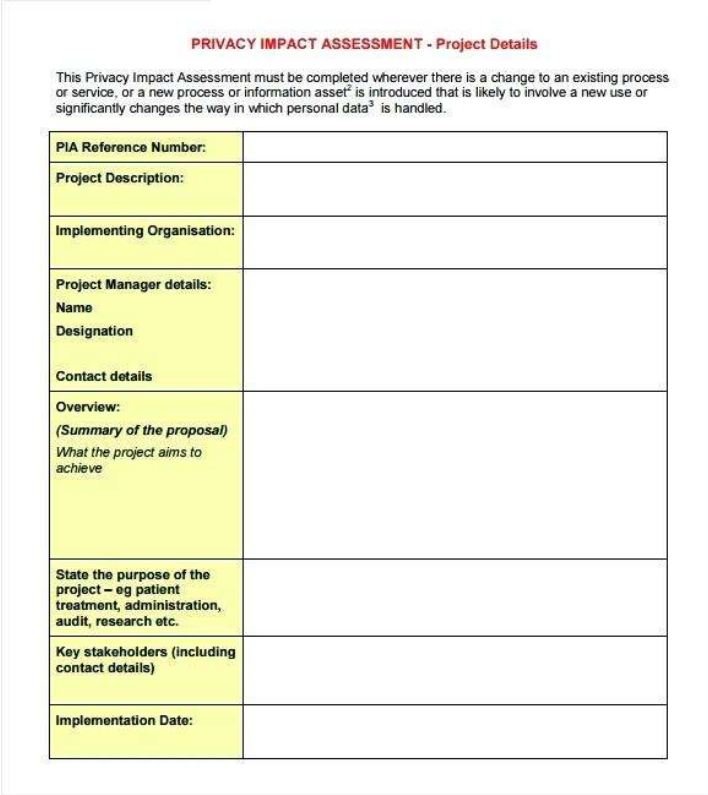


VERİ KORUMA ETKİ ANALİZİ

ÜNSAL

Büyük ebatta veya yeni bir amaçla kişisel veri işlenecek olması durumunda sözleşme aşamasında **Veri Koruma Etki Analizi** (DPIA-Data Privacy Impact Assessment) yapıldığından emin olunuz.

Örnek: Şirket yapılacak büyük ebattaki veri paylaşımlarında bu etki analizinin yapılması gerekebilecektir.



PRIVACY IMPACT ASSESSMENT - Project Details

This Privacy Impact Assessment must be completed wherever there is a change to an existing process or service, or a new process or information asset[2] is introduced that is likely to involve a new use or significantly changes the way in which personal data[3] is handled.

PIA Reference Number:	
Project Description:	
Implementing Organisation:	
Project Manager details: **Name** **Designation** **Contact details**	
Overview: ***(Summary of the proposal)*** *What the project aims to achieve*	
State the purpose of the project – eg patient treatment, administration, audit, research etc.	
Key stakeholders (including contact details)	
Implementation Date:	

ÇALIŞANLARIN EĞİTİMİ & TUTUMU

Kişisel Verilerin Korunmasına ilişkin gerekli eğitimlerin verilmesi, veri gizliliği konularında talimatların uyulması ve oryantasyonun sağlanması konusunda çalışanları teşvik ediniz.

- Çalışanlara KVKK eğitimlerinin verilmesi
- Çalışanların talimatlara uygun hareket etmesi
- Yeni çalışanların oryantasyonu

İŞLEME SÜREÇLERİ & ENSTRÜMANLARI

Kanuna uyumluluk kapsamında hazırlanan süreçlerin ve dokümanıarın Departman KVK Klasörü altında saklanması ve uygulamaya alınması gerekmektedir.

Ayrıca, Şirketin KVKK Dokümanlarını lütfen takip ediniz.

- Kişisel Veriler Aydınlatma Metinleri
- Kişisel Verilerin İşlenmesi ve Korunması Politikası
- Çalışanlara Yönelik Kişisel Verilerin İşlenmesi Ve Korunması Politikası
- Kişisel Verileri Saklama ve İmha Politikası
- Kişisel Veri Güvenliği Politikası
- Kişisel Verilerin İşlenmesine İlişkin Sözleşmeler veya Ek Maddeler
- Veri Sahibi Başvuru Formu

TEKNİK VE İDARİ TEDBİRLERİN ALINMASI

ÜNSAL

Kişisel verilerin güvenli ortamlarda saklanması için gerekli teknik ve idari tedbirleri alınız.

Tedbirlerin uygulanması ile ilgili çalışanların sorun yaşaması halinde ve/veya tedbir önerileri varsa, lütfen KVK Komitesine yönlendiriniz.

AB GENEL VERİ KORUMA YÖNETMELİĞİ (GDPR)

ÜNSAL

TARİHÇE:

Veri Koruma Direktifi, AB içerisinde farklı uygulamalara yol açtığı için Avrupa Komisyonu yeni bir düzenleme yapılmasını gerekli görmüştür.

14 Nisan 2016 tarihinde AB Genel Veri Koruma Regülasyonu kabul edilmiştir.

GDPR, 25 Mayıs 2018 tarihinde yürürlüğe girmiştir. AB üye ülkeleri için bağlayıcıdır. Uygulama farklılıkları ortadan kalkmış ve veri koruma kuralları yeknesaklaşmıştır.

AB GENEL VERİ KORUMA YÖNETMELİĞİ (GDPR)

ÜNSAL

Avrupa Birliği dışında bulunan işletmeler;

(i) AB'deki kişilere **hizmet ya da ürün sağlıyorsa** veya
(ii) AB'deki kişilerin **davranışlarını izliyorsa**

bu faaliyetleri için GDPR'a tabi olacaklardır. Ancak AB mukimlerine her ürün ve hizmet sağlayan şirket, GDPR'da tabi olmayacaktır. Aşağıdaki unsurları taşıyan şirketlerin, AB'de kişilere ürün/hizmet verdiği kabul edilebilecektir.

AB GENEL VERİ KORUMA YÖNETMELİĞİ (GDPR)

ÜNSAL

GDPR'A AYKIRILIK:

Hafif hukuka aykırılıklar

- DPO'nun görevlerini yerine getirememesi, Sertifika kurumlarının kurallarına uyulmaması vs.
- **€10m** ya da **önceki mali yılın toplam global cirosunun %2'si (hangisi yüksekse)**

Ağır hukuka aykırılıklar

- Veri işleme şartlarına, veri sahibinin haklarına ve diğer tüm kurallara aykırılık
- **€20m** ya da **önceki mali yılın toplam global cirosunun %4'ü (hangisi yüksekse)**

AB GENEL VERİ KORUMA YÖNETMELİĞİ (GDPR)

ÜNSAL

GDPR İLE GETİRİLEN YENİ İLKELER:

GDPR'da, kişisel verilerin işlenmesi bağlamında gerçek kişilerin hak ve özgürlüklerinin korunması amacıyla gerekli teknik ve idari önlemlerin alınması gerektiği ifade edilmektedir. Bu kapsamda veri sorumluları başlangıçtan ve tasarımdan itibaren gizlilik ilkeleri uyarınca gerekli önlemleri almalıdır.

Tasarımdan–itibaren-gizlilik (privacy by design)	• Bu ilke gereğince şirketler işlemenin planlama, yürütme ve diğer aşamalarında kişisel veri ihlallerini azaltmaya yardımcı olan yeni ürünler, hizmetler veya teknolojiler kullanmalılardır.
Başlangıçtan - itibaren- gizlilik (privacy by default)	• Bu ilkeye göre şirketler, gerekli kişisel verilerin işlenmesini sağlamak için uygun teknik ve idari önlemleri almalılardır.
Bulanıklaştırma (Pseudonymisation)	• Kişisel veriye takma ad, kod, işaret vs. vererek bulanıklaştırılması işlemidir. Böylece bu bulanık veriler ele geçirilse bile ele geçiren tarafça anlaşılamayacaktır.

AB GENEL VERİ KORUMA YÖNETMELİĞİ (GDPR)

ÜNSAL

GDPR İLE VERİ SAHİBİNE GETİRİLEN YENİ HAKLAR:

İlgili kişilerin hakları GDPR ile daha detaylı düzenlenerek, ilgili kişinin kişisel verileri üzerinde daha çok kontrole sahip olmasını sağlayan yeni haklar getirildi. Bu haklar veri taşınabilirliği ve unutulma hakkıdır.

Veri taşınabilirliği hakkı (right to data portability)

Bu hak, kullanıcılara kişisel verilerini bir veri sorumlusundan diğerine aktarma olanağı sağlar.
Veri sorumluları, ilgili kişinin talebi üzerine, o kişinin verilerini *yapılandırılmış, «yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta»* ve hiçbir engelleme olmadan doğrudan ilgili kişiye veya onun gösterdiği bir başka veri sorumlusuna aktarmakla yükümlüdür.

Unutulma hakkı (right to be forgetten)

Kullanıcılar bu hak kapsamında kendilerine ait kişisel verilerin silinmesini talep edebilme hakkını haizdir.
Veri sorumluları, bu talep doğrultusunda kişiye ait verileri gecikmeden silmekle yükümlüdür. Ayrıca veri sorumlularının, kişisel veriyi başka veri sorumlularıyla paylaşmış veya kullanımlarına açmış olması durumunda söz konusu verilere ilişkin kısa yol, kopya veya çoğaltılmış versiyonları silmeleri bakımından da sorumludurlar.

AB GENEL VERİ KORUMA YÖNETMELİĞİ (GDPR)

ÜNSAL

VERİ KORUMA ETKİ DEĞERLENDİRMESİ (DATA PROTECTION IMPACT ASSESSMENT)

Veri sorumlusu, işleme faaliyetinin ilgili kişilerin temel hak ve özgürlüklerine yönelik yüksek derecede risk oluşturduğu hallerde bir Veri Koruma Etki Değerlendirmesi hazırlamakla yükümlüdür. Bu değerlendirme ile riskin kaynağı, niteliği ve derecesi belirlenecektir. Veri sorumluları bu değerlendirme sonucu riski azaltmak veya ortadan kaldırmak amacıyla uygun güvenlik tedbirlerini almakla yükümlüdür.

Veri Koruma Etki Değerlendirmesinin hazırlanacağı bazı durumlar:

- Özel nitelikli kişisel verilerinin büyük ölçekte işlenmesi,
- Birden çok kaynaktan toplanan verilerin birleştirilmesi, karşılaştırılması ve eşleştirilmesi,
- Kişisel verileri, bireylere hiçbir bildirimde bulunmaksızın işlemek,
- Kişisel verileri, bireylerin çevrimiçi veya çevrimdışı konumlarını veya hareketlerini izlemeyi içerecek şekilde işlemek veya büyük ölçüde profilleme,
- Güvenlik ihlali durumunda fiziksel zarar riski ile sonuçlanabilecek kişisel veri işleme faaliyetleri,
- Çocukların kişisel verilerini, profil oluşturma, otomatik karar verme, pazarlama amaçlarına uygun olarak işleme veya onlara doğrudan çevrimiçi hizmetler sunabilmek adına işlenmesi,
- Savunmasız ilgililere ilişkin verilerin işlenmesi.

AB GENEL VERİ KORUMA YÖNETMELİĞİ (GDPR)

ÜNSAL

KİŞİSEL VERİLERİN ULUSLARARASI AKTARIMI

GDPR kişisel verilerin Avrupa Ekonomik Bölgesi ("EEA") dışındaki aktarımları için birtakım kurallar getirmiştir. Buna göre, şirketler EEA dışına veri aktarabilmek için aşağıdaki yollardan birini seçebilir:

- *Binding Corporate Rules* uygulamak (iştirakleri için geçerli),
- AB Komisyonu tarafından hazırlanan standart veri koruma maddelerini *(standart model clauses)* uygulamak,
- Veri Koruma Kurumu tarafından hazırlanan ve Komisyon tarafından onaylanan standart veri koruma maddelerini uygulamak,
- Madde 40 uyarınca onaylı uygulama kurallarını *(code of conduct)* oluşturmak,
- Madde 42 uyarınca onaylı sertifika mekanizmalarını uygulamak veya
- Yetkili veri koruma kurumu tarafından bu amaç için onaylan veri sorumlusu ve veri işleyen arasında sözleşme akdetmek.

AB GENEL VERİ KORUMA YÖNETMELİĞİ (GDPR)

ÜNSAL

VERİ İŞLEYENE GETİRİLEN EK YÜKÜMLÜLÜKLER:

KVKK uyarınca veri işleyenler veri sorumlusunun talimatlarına uymaları ve verilerin güvenliğine sağlamalıdır. GDPR, bunlara ek olarak veri işleyenlere yönelik GPDR, veri işleyenlere birtakım yükümlülükler getirmiştir.

- Veri sorumlusuna destek sağlama
- Sözleşmenin sona ermesiyle kişisel verileri silmesi veya iade etmesi
- Veri sorumlusuna uyumluluğunu göstermesi ve denetime izin vermesi
- Alt veri işleyen ile arasında sözleşme akdetmesi
- Veri işleme faaliyetlerinin yazılı kaydını tutma
- Veri Koruma Kurumu ile işbirliği içinde olma
- Veri sorumlusuna kişisel veri ihlalini bildirme
- Gerekli hallerde DPO atama
- Uluslararası veri aktarımı şartlarına uyma

ÜNSAL

TEŞEKKÜRLER

İLETİŞİM:

BURÇAK ÜNSAL
burcak@unsal.com

M. MERT YAŞAR
mert.yasar@unsallaw.com

MUTLU ŞEYMA KÖMÜR
mutlu.komur@unsallaw.com

KAAN ÖZDEMİR
kaan.ozdemir@unsallaw.com

BEHİÇ BENTÜRK
behic.benturk@unsallaw.com