

# Kişisel Veri İşleme Rehberi Uyarınca Kişisel Verilerle Çalışma İlkeleri



İnsana  
Değer  
Derneği

## Giriş

Kişisel Verilerin İşlenmesine İlişkin Kılavuzun amacı, tüm IDD çalışanlarının herhangi bir kişisel veri toplamanın etkisini düşünmeye başlaması ve verilerle daha dikkatli çalışmasıdır. İDD'de kişisel verilerle çalışma sürecinde **GDPR**'den (Genel Veri Koruma Yönetmeliği) kaynaklanan gerekliliklere uyulması hedeflenmektedir.

## Uygulama kapsamı

Bu ilkeler, tüm tam ve yarı zamanlı çalışanlar, gönüllüler, stajyerler, danışmanlar ve stajyerlerin yanı sıra IDD'yi temsil etmeleri veya IDD adına hareket etmeleri halinde diğer kişiler (bundan böyle "Çalışanlar" olarak anılacaktır) için de geçerlidir.

Bu İlkelerde yer alan kurallar asgari standartları belirlemektedir. Münferit departmanlar daha katı kurallar uygulayabilir, ancak bu kurallar bu asgari standartlara dayanmalıdır.

## Genel şartlar

### **Kişisel veri nedir:**

E-posta adresi, IP adresi veya çerezler gibi elektronik verilerden isim, adres ve kişisel kimlik numarası gibi daha tipik verilere ve örneğin kişinin sağlık durumu veya etnik kökeni gibi hassas verilere kadar belirli bir bireyin (veri sahibi) tanımlanabileceği her türlü veri. Kişisel verilere fotoğraflar ve ses/video kayıtları da dahildir.

### **Veri toplama:**

Esasen, veriler iki şekilde elde edilebilir - doğrudan veri sahiplerinden veya başka yollarla (İnternet gibi kamuya açık kaynaklardan, bir şirketten veri tabanı satın alarak, vb.)

Her iki durumda da, veri sahibine IDD'nin bu verileri elde ettiğini (ve varsa hangi kaynaktan elde ettiğini) bildirmek, IDD'nin temel iletişim bilgilerini belirtmek, IDD'nin hangi verileri elde ettiğini, bunlarla ne yapmayı planladığını, verilerin ne kadar süreyle elinde kalacağını, hangi yasal gerekçeler olduğunu (aşağıya bakınız), verileri aktarmayı planlayıp planlamadığını (ve kime) ve veri sahiplerinin temel hakları hakkında bilgi vermek zorundayız.

Aradaki fark, verileri doğrudan ilgili kişiden elde ederken, ilgili kişiyi verileri topladığımız sırada bilgilendirmemiz gerekirken, aksi takdirde verileri topladıktan sonraki bir ay içinde bilgilendirmemiz yeterlidir.

Reşit olmayan çocukların kişisel verileri işlenirken, 15 yaş sınırı belirleyicidir - daha küçük çocuklar söz konusu olduğunda, çocuğun yasal vasisi (çoğunlukla bir ebeveyn) bilgilendirilmelidir (yani onay vermelidir).

Kişisel verilerin elde edilmesine ilişkin tipik örnekler: çevrimiçi bir formun doldurulması, bir haber bültenine abonelik, yeni işe alınan çalışanlardan veri elde edilmesi, bir yoklama listesinin doldurulması, bir müşteriyle çalışırken ondan veri elde edilmesi vb.

IDD verileri elde eder etmez, bu verilerle ilgili olarak kontrolör haline gelir (ve bazı durumlarda, IDD verilerle başka bir kişinin amaçları ve talimatları doğrultusunda çalışıyorsa aynı zamanda bir işlemcidir); her iki durumda da, bu kişisel verileri kullanırken bir takım yükümlülükleri vardır.

### **Kişisel verilerle çalışmaya başlamadan önce göz önünde bulundurmanız gereken temel hususlar:**

- Gerçekten kişisel veri olup olmadığı;
- Bu bilgileri nasıl toplayacağız ve doğru olup olmadığını (ve yetkili kişi tarafından bize sağlandığını) nasıl kontrol edeceğiz;
- Ne için ihtiyacımız var / ne için istiyoruz (bu, verilerle çalışmak için yasal gerekçelerin temelidir, aşağıya bakın);
- Buna ne ölçüde ihtiyacımız var (kapsam en aza indirilmelidir);

- Verileri ne kadar süreyle kullanmayı planladığımız (sürenin uzunluğu da en aza indirilmelidir); Verilerle kimlerin çalışacağı (verilere kimlerin erişebileceği);
- Nerede saklanacağı ve izinsiz kullanıma karşı nasıl korunacağı (bu, bir bilgisayara veya buluta kaydetmenin yanı sıra belgeleri kağıt üzerinde sakladığınız yeri, bir yazıcıda ortalıkta bırakmanıza izin verilip verilmediğini, cep telefonunuzun şifre korumalı olup olmadığını vb. içerir);
- IDD dışında birine aktarmak isteyip istemeyeceğimiz (veya IDD için başka birinin işleyip işlemeyeceği);
- Kullanabileceğimiz süre sona erdiğinde verilere ne olacak (süreyi kim izleyecek, verilerin silinmesinden veya anonim hale getirilmesinden kim sorumlu olacak, teknik olarak nasıl yürütülecek).

### **Kişisel verilerle çalışmak için (en sık) yasal gerekçeler nelerdir?**

- Veri sahibinin sözleşmeye taraf olduğu sözleşmenin ifası için gerekli olması; Veri sorumlusu (IDD) için geçerli olan yasal bir yükümlülüğe uymak için gerekli olması;
- Kontrolörün veya üçüncü bir tarafın meşru menfaatleri için gereklidir;
- Veri sahibi, kişisel verilerinin işlenmesine onay vermiştir.

İlk üç durumda, veri sahibinin rızasına ihtiyaç duymayız, sadece onu bilgilendiririz.

Son durumda, veri sahibinin işleme için bize onay vermesi gerekmektedir. Rızanın özgür (yani, ilgili kişi rıza verebilir, ancak rıza verme yükümlülüğü yoktur veya daha sonra ilgili kişiye hizmetlerin sağlanması üzerinde herhangi bir etkisi olmaksızın rızasını geri çekebilir), bilgilendirilmiş (ilgili kişi neyi kabul ettiğini bilmelidir) ve açık (yani, ilgili kişinin imzalamasını, web üzerinde işaretlemesini vb. isteriz) olması gerekir.

### **KİŞİSEL VERİ İÇEREN FİZİKSEL BELGELERLE ÇALIŞMA İLKELERİ:**

- Belgeler kendi kişisel verilerinizi içeriyormuş gibi onlarla çalışın. Belgeleri kilitlenebilecek bir yerde saklayın.
- Belgelerle çalışmayı bitirdiğinizde, lütfen onları tekrar "kilitleyin".
- Mümkünse, belgeleri anonimleştirin (örneğin, kişisel veri içeren kısımların tamamını veya bir kısmını karalayarak).
- Bunları yalnızca açık bir ihtiyacınız varsa ve ideal olarak yalnızca anonimleştirilmiş biçimde kopyalayın.
- Belgeleri kopyalarken veya yazdırırken - her zaman yazıcıdan toplayın - yazıcının "etrafında" durmalarına izin vermeyin.
- Her zaman belgeleri kime ve ne amaçla verdiğinizi düşünün.
- Belgeleri yalnızca kesinlikle gerekli olduğu süre boyunca saklayın ve bu süre sona erdiğinde imha edin. Belgeleri atık kağıt kutusuna atmak doğru bir yöntem değildir - bir öğütücü kullanın.
- Kişisel veri içeren belgelerle karşılaşırsanız ve sahibini tespit edemezseniz, belgeleri imha edin.
- Bu tür bir belgeye nasıl yaklaşacağınız konusunda tavsiyeye veya basit bir danışmanlığa ihtiyacınız varsa, bölümünüzdeki Yetkili Kişi ile iletişime geçmekten çekinmeyin - sayfa 2'deki listeye bakın.
- Lütfen monitörlerinizin de bir dizi hassas ayrıntı içerdiğini ve bir
- kuralına göre, bilgisayarınızdan her ayrıldığınızda "WIN+L" tuşlarını kullanarak kilitleyin.

### **9Verilerin Korunmasına İlişkin Kurallar**

#### **1. BİRE BİR YAKLAŞIM**

Kişisel veriler çağdaş dünyada değerli bir meta haline geliyor. İşimizin doğası gereği, yararlanıcılar, kurs katılımcıları veya sosyal program müşterileri hakkında yığınla veri elde ediyoruz. Bu da kendi kişisel verilerimizi ele aldığımız gibi büyük bir dikkatle ele almamız gereken değerli "mallarla" çalıştığımız anlamına geliyor.

#### **2. YASALLIK, DOĞRULUK, ŞEFFAFLIK**

Kişisel veriler, e-posta adresi, IP adresi veya çerezler gibi elektronik verilerden isim ve adres gibi en yaygın verilere ve hassas verilere kadar belirli bir bireyin tanımlanabileceği her türlü veridir.

kişinin sağlık durumu veya etnik kökenine ilişkin bilgiler gibi veriler. Kişisel veriler fotoğraf ve ses/video kayıtlarını da içerebilir.

Kişisel verileri topladığınız takdirde, ilgili kişi, verileri hangi amaçla topladığınız, ne kadar süreyle saklayacağınız ve bu verilerle ne yapılacağı da dahil olmak üzere her zaman bilgilendirilmelidir. Bazı durumlarda, ilgili kişiden kişisel verilerinin işlenmesi için bilgilendirilmiş bir onay almamız gerekir.

### 3. AMAÇ VE KISITLAMA

Kişisel verileri yalnızca bir nedeniniz varsa toplayabilirsiniz: bir sözleşmenin ifası, yasal bir yükümlülüğe uygunluk, meşru menfaat veya bilgilendirilmiş rıza. Kişisel veriler, önceden bildirilen amaçlar dışında işlenemez - örneğin, bir gazeteciyi çalışmalarımız hakkında bilgilendirmek için edindiğimiz iletişim bilgileri, bağış talep etmek amacıyla kullanılamaz.

### 4. VERİ MINİMİZASYONU

Yalnızca amacınıza ulaşmak için ihtiyaç duyduğunuz minimum miktarda veriyi toplayın ve kullanın. Yönetmelik, yalnızca asgari miktarda veri toplamamızı ve işlememizi zorunlu kılmaktadır. Tüm araçlar ve biçimler, işleme kapsamı ve saklama süresi işleme amacına uygun olmalıdır. Örneğin, bir bağışçı için gıda yardımı alan yararlanıcılara ilişkin bir genel bakış hazırlıyorsanız, büyük olasılıkla dini veya etnik aidiyeti not etmeniz gerekmeyecektir; veya atölyelerimize katılan kişiler hakkında veri toplarken kimlik numaralarını toplamanız için bir neden yoktur.

### 5. DOĞRULUK

Verilerinizin güncel olduğundan emin olun. Kişisel verilerle çalışırken, yanlış veya hatalı verilerin işlenmemesini garanti etmek için önlemler almalısınız. Yanlış veriler sadece yazım hatalarıyla sınırlı değildir; yanlış bilgilerle ilgili olarak resmi olarak yanlış verileri de içerir.

### 6. SINIRLI DEPOLAMA

Verileri gerekenden daha uzun süre saklamayın. Kişisel veriler yalnızca ilgili amaç için gerekli olan asgari süre boyunca işlenebilir ve veri sahibi sürenin uzunluğu hakkında bilgilendirilmelidir (sınırsız bir süre olamaz). Bu sürenin sona ermesinin ardından veriler imha edilmelidir. Özel bir imha durumu, verilerin anonimleştirilmesidir - yani, belirli bir bireyin bunlara dayanarak hiçbir şekilde tanımlanamayacağı şekilde verilerin bir kısmının imha edilmesi (silinmesi).

### 7. BÜTÜNLÜK VE GİZLİLİK

Verileri güvende tutun, parola ile koruyun. Kişisel bilgisayar diskleri herhangi bir kişisel veri içermemelidir. Kişisel veriler her zaman şifrelenmiş yerlerde saklanmalıdır - örneğin sunucularımızda, bölüm Paylaşım Noktalarında veya kişisel One Drive'larda.

Kağıt üzerindeki kişisel veriler her zaman kilitlenebilir bir dolapta veya düzenli olarak kilitlenen bir ofiste saklanmalıdır. Kişisel veri içeren dosyaların ögüle tatili de dahil olmak üzere serbestçe erişilebilir olması iyi bir uygulama değildir.

### 8. KİŞİSEL VERİLERİN AKTARILMASI

Kişisel verileri, IDD içinde bile olsa, erişmemesi gereken kişilere vermeyin. E-posta çok fazla güvenlik garantisi sağlamaz ve bu nedenle daha dikkatli kullanılmalıdır ve ideal olarak hiçbir kişisel veri e-posta ile gönderilmemelidir. Bu tür bilgilerin iletilmesi gerekiyorsa, bölümünüzün Paylaşım Noktası'na veya kişisel One Drive diskinize kaydetmenizi ve "Paylaş" işlevini kullanarak paylaşmanızı öneririz. Diğer bir seçenek de parola korumalı bir arşiv (zip, rar) ve parolanın alıcıya "uçtan uca" şifrelemeli bir mesajlaşma uygulaması (Viber veya Messenger) aracılığıyla gönderilmesidir.

### 9. HESAP VEREBİLİRLİK VE KONTROL

Kişisel verileri nasıl işlediğinizi belgelememiz gerekiyor. Yönetmeliğin bize yüklediği yükümlülük, işleme faaliyetlerinin kaydını tutmaktır. Bu nedenle, kişisel verileri yönetmeliğe uygun olarak işlediğimizi her zaman belgeleyebilmemiz için, bölümünüzün Yetkili Kişisinin kendi programlarımızda kişisel verilerin işlenmesi hakkında önceden bilgilendirilmesi (bu kişinin iletişim bilgilerini operasyon müdürünüzden, lojistik departmanınızdan veya bölümünüzün başkanından alabilirsiniz) ve atılacak diğer adımlarla ilgili olarak Yetkili Kişiyi danışmanız gerekir.