

# ÇOCUKLARIN KİŞİSEL VERİLERİNİN KORUNMASI



*Çocuklar ve  
ebeveynler için!*

İSTANBUL BAROSU  
KİŞİSEL VERİLERİN KORUNMASI KOMİSYONU



# ÇOCUKLARIN KİŞİSEL VERİLERİNİN KORUNMASI

*Ebeveynler için*



İSTANBUL BAROSU  
KİŞİSEL VERİLERİN KORUNMASI KOMİSYONU





# Çocukların Kişisel Verilerinin Korunmasında Temel Kavramlar



## Kişisel Veri:

Bir çocuğun kimliğini belirlemeye yarayan her türlü türlü bilgiye “kişisel veri” denir.

❖ Örnekler: Çocuğunuzun adı, soyadı, fotoğrafı, okul bilgileri, sağlık raporları, adresi.

## Özel Nitelikli Kişisel Veri:

Kişinin pamuk ipliğine bağlı bilgileri bu grupta yer alır; çocuğunuzun sağlık bilgileri, biyometrik ve genetik verileri, ırkı, etnik kökeni, dini, mezhebi gibi KVKK'nın 6. maddesinde sayılan nitelikte kişisel veriler çocuğunuzun özel nitelikli kişisel verileridir.

❖ Örnekler: Sağlık durumu, engellilik bilgisi, dini inancı.



## İlgili Kişi:

Kişisel verileri işlenen kişidir. Yani çocuğunuz KVKK uyarınca “ilgili kişi”dir. İlgili kişi olarak çocuğunuzun KVKK'dan doğan hakları vardır ve siz ebeveynler olarak çocuğunuzun KVKK'dan doğan haklarını Türk Medeni Kanunu'ndan kaynaklanan velayet hakkınız çerçevesinde korumalısınız.

## Veri Sorumlusu:

Kişisel verileri işleyip, toplayıp, saklayan kişi ya da kuruluş. Örneğin çocuğunuzun götürdüğünüz hastane, muayenehanedeki doktor, eğitim gördüğü okul ve hatta siz bile veri sorumlusu olabilirsiniz.

❖ Sharenting sırasında çocuğun verisini sosyal medyada paylaşmanız halinde siz de ebeveyn olmanıza rağmen veri sorumlusu kabul edilebilirsiniz.

## Veri İşleme:

Kişisel verilerin toplanması, kaydedilmesi, saklanması, kullanılması, paylaşılması gibi her türlü işlem.

❖ Çocuğun fotoğrafını çekip Instagram'a yüklemek de bir veri işleme olayıdır.

## Açık Rıza:

İlgili kişinin, yani çocuğun (veya onun yerine karar verecek yasal temsilcisinin) özgür iradeyle verdiği, bilgilendirilmiş onay.

❖ Küçük çocuklar için rızayı ebeveyni verir ama miniklerin fikri de dikkate alınmalı.

## Sharenting:

Ebeveynlerin çocuklarına dair her şeyini (fotoğraf, video, özel bilgi) sosyal medyada paylaşması.

❖ Bu, çocuğun kişisel verilerinin izinsiz ortaya saçılması anlamına gelebilir ve KVKK'ya aykırı olabilir.



# Çocukların Kişisel Verilerinin Korunmasında Temel Kavramlar

## Yasal Temsilci:

Çocukların kişisel verileriyle ilgili haklarını kullanabilecek kişi ya da kişiler.

📌 Genelde ebeveyn olur. Ama yasal temsilci olsalar bile, çocuğun mahremiyet hakkını çiğnememelidirler.

## Dijital Kimlik:

Bir çocuğun internet üzerindeki izleriyle oluşan sanal kimliğidir.

📌 Örnek: Sosyal medya profili, çevrimiçi oyun kullanıcı adı, yorumları, paylaşımları.

🧠 Not: Dijital kimlik zamanla büyür ve kalıcı hale gelir. Çocukların kendi rızaları olmadan bu kimliğin inşa edilmesi, ileride kimlik sorunlarına veya mahremiyet ihlallerine yol açabilir.

## Dijital Ayak İzi:

Çocuğun internette bıraktığı her türlü izdir.

📌 Örnek: Tıkladığı linkler, ziyaret ettiği siteler, arama geçmişi, sosyal medya etkileşimleri.

🔒 Bu veriler genellikle fark edilmeden toplanır ve profillemeye amacıyla kullanılabilir.

## Çevrimiçi Profil:

Bir kişinin dijital ortamdaki görünümüdür; sistemlerin kişi hakkında topladığı bilgilerden oluşur.

📌 Örnek: Google, YouTube veya oyun platformlarının oluşturduğu kullanıcı profilleri.

## Anonimleştirme:

Bir verinin, kime ait olduğu belirlenemeyecek şekilde düzenlenmesidir.

📌 Çocuğun okul verilerinin, ismi çıkarılarak akademik analizde kullanılması gibi.

## Çerezler (Cookies):

Web sitelerinin, kullanıcının davranışlarını takip etmek için cihazına bıraktığı küçük dosyalardır.

📌 Çocukların ziyaret ettikleri siteler üzerinden ilgi alanları tespit edilip reklam gösterilebilir.

🎯 Ebeveynlerin, çocukların kullandığı cihazlarda çerez politikalarını incelemesi önemlidir.

## Profil Oluşturma (Profiling):

Kişisel veriler kullanılarak bireylerin tercih, davranış ve alışkanlıklarına dair tahmin yapılması.

📌 Örneğin bir çocuğun ilgi alanına göre YouTube'da önerilen videolar.





# Çocukların Dijital Kimlik Gelişimi ve Mahremiyet Eğitimi



## Dijital Kimlik Nedir?

Çocukların çevrimiçi ortamlarda (sosyal medya, oyunlar, forumlar vb.) oluşturdukları profiller, paylaşımlar, etkileşimler aracılığıyla oluşan sanal benlikleri ve farklı platformlarda farklı yönlerini sergileyebilme (örneğin, bir oyunda "savaşçı" kimliği, bir sosyal medya platformunda "arkadaş canlısı" kimliği) kabiliyetidir.

Çocuklar, dijital kimliklerini paylaşımlar (fotoğraf, video, yazı vb.) ve etkileşimler (beğeni, yeniden gönderi, takip, yer işareti vb.) yoluyla gösterirler.

Dijital kimlik oluşturma sürecinde empati de oldukça önemli. Bu yüzden çocuklara çevrimiçi ortamda başkalarının haklarına saygı göstermeyi ve empati kurmayı öğretmek gerekiyor.

Çocuklarınıza,

- Karşımızdaki kişinin de "gerçek" bir insan olduğunu,
- Çevrimiçi iletişimde nazik, düşünceli ve saygılı olması gerektiğini,
- Başkalarının haklarına ve mahremiyetine saygı göstermesi gerektiğini hatırlatın.





# Çocukların Dijital Kimlik Gelişimi ve Mahremiyet Eğitimi

Yaşa uygun mahremiyet eğitimi nasıl olur?

## 0-5 Yaş:

- Fiziksel mahremiyete odaklanın ("Vücudunun özel bölgeleri sana ait").
- Dijital mahremiyet konusunda temel farkındalık oluşturun (fotoğraflarının izinsiz çekilemeyeceği).
- Ebeveynlerin rehberliği çok önemli (sharenting'den kaçının).

## 6-9 Yaş:

- "Özel" ve "Herkes Açık" kavramlarını öğretin.
- İzin almanın önemini vurgulayın (fotoğraf çekmek veya paylaşmak için).
- Temel internet güvenliği kurallarını anlatın (şifreleri gizli tutmak).

## 10-12 Yaş:

- Sosyal medyanın risklerini ve fırsatlarını tartışın.
- Çevrimiçi etkileşimlerde dikkatli olmayı öğretin (tanımadıklarla iletişim kurmamak).
- Dijital ayak izi kavramını tanıttın (internet ortamında bıraktığımız izler).

## 13+ Yaş:

- Daha karmaşık mahremiyet konularını ele alın (veri toplama, gizlilik politikaları).
- Eleştirel düşünme becerilerini geliştirin (çevrimiçi bilgileri sorgulamak).
- Dijital vatandaşlık ve etik değerleri vurgulayın.





# Sharenting ile Çocukların Kişisel Veri Mahremiyetini İhlal Etmeyin!

## Sharenting nedir?

Sharenting (İngilizce "share" [paylaşmak] ve "parenting" [ebeveynlik] kelimelerinin birleşimi), ebeveynlerin çocuklarıyla ilgili fotoğraf, video veya özel bilgileri sosyal medyada paylaşması anlamına gelir.

## Riskler neler?



- **Mahremiyetin Kaybolması ve Fazla Bilginin Paylaşılması**

Ebeveynler, farkında olmadan çocuklarının kişisel ve hassas bilgilerini (isim, doğum tarihi, okul, konum gibi) paylaşabilir. Bu bilgiler kötü niyetli kişiler tarafından kimlik hırsızlığı veya dolandırıcılık için kullanılabilir. Örneğin bir doğum günü gönderisinde tam isim ve tarih paylaşılması, kimlik hırsızları için önemli detaylar sağlayabilir veya fotoğraflara yerleştirilen konum bilgisi, çocuğun nerede okuduğunu veya bulunduğunu gösterip güvenlik riski doğurabilir.

- **Onaysız Dijital Ayak İzi**

Sharenting yoluyla çocukların dijital ayak izleri, onların bilgisi ve rızası olmadan oluşturulur. Paylaşılan fotoğraflar veya gönderiler, yıllar sonra utanmaya ya da kötü bir itibara neden olabilir.

- **Suistimal Riskleri**

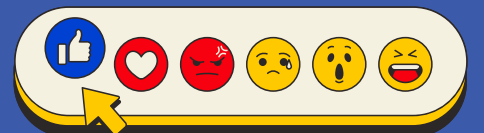
Çocukların masum fotoğrafları bile yanlış kişilerin ellerine geçip uygunsuz şekillerde kullanılabilir ve bu nedenle bazı paylaşımlar, farkında olmadan çocukları istismara açık hale getirebilir.

- **Sosyal Medya Platformları ve Veri Toplama**

Sharenting yapılırken kullanılan platformlar tarafından gönderilerden toplanan meta veriler (konum, beğeniler, ilişkiler vb.) gibi büyük miktarda bilgiyi üçüncü taraflara satılabilir veya profillemeye/hedefli reklam faaliyetlerinde kullanılabilirler.

- **Siber Zorbalık ve Bilgi Sızıntısı (Doxxing)**

İnternete yüklenen içerikler başka kişiler tarafından yanlış anlaşılabilir, manipüle edilebilir ya da farklı bir bağlamda tekrar paylaşılabilir. Bu durum, çocukların siber zorbalığa uğramasına veya kimlik bilgilerinin açığa çıkmasına neden olabilir.





# Sharenting ile Çocukların Kişisel Veri Mahremiyetini İhlal Etmeyin!



Sharenting'in risklerini nasıl azaltabiliriz?

- Paylaşmadan Önce Düşünün

Paylaşmadan önce şu soruları sorun:

Bu bilgiyi bir yabancı görse sorun olur mu?

Bu paylaşım çocuğumun gelecekte utanmasına neden olabilir mi?

- Kişisel Bilgi Paylaşımını Sınırlayın

Çocuğun tam ismi, adresi veya lokasyonu gibi bilgileri paylaşmaktan kaçının.

- Gizlilik Ayarlarını Doğru Kullanın

Sosyal medya hesaplarının gizlilik ayarlarını sıkı bir şekilde kontrol edin. Paylaştığınız gönderilerin sadece güvenilir kişiler tarafından görülebileceğinden emin olun. Özellikle sosyal medya hesabınızdaki gönderiler “herkese açık” ise, “sharenting”i tekrar düşünün!

- Çocuklardan Onay Alın

Çocuklar büyümeye başladıkça, onların fotoğrafları paylaşmadan önce izin istemek önemlidir. Bu, onların mahremiyetine saygı duymayı öğretmektedir.

- Konum Etiketlemeyi Kapatın

Fotoğraflarda veya paylaşımlarda konum etiketlemeyi devre dışı bırakın.

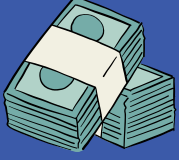
- Düzenli Olarak İçerik Kontrolü Yapın

Daha önce yüklediğiniz içerikleri düzenli olarak gözden geçirerek, hassas bilgiler içerenleri silin.





# Veri İhlalleri ve Siber Güvenlik Risklerine Karşı Koruma



Kişisel Verileri Koruma Kurumu'nun 2024 yılı faaliyet raporuna göre 281 veri ihlal bildirimini Kurul'a intikal etmiş, bu bildirimlerin 63'ü kamuoyuna ilan edilmiş ve yapılan incelemeler sonucunda 552 milyon 668 bin Türk lirası idari para cezası uygulanmış.

2024 yılında, KVK Kurulu tarafından Meta'ya Instagram'daki çocuklara ait hesapların ebeveyn izni olmaksızın (çocuklar tarafından) işletme hesabına çevrilebilmesi; işletme hesaplarının ise bağlı olduğu e-posta adresi ve GSM numaralarının sitenin HTML kodlarında herkesçe erişilebilir şekilde yer alması sebebiyle 11 milyon 500 bin TL tutarında para cezası verilmişti.



2020 yılında bir özel öğretim kurumu, velilerin bilgisi ve onayı dışında öğrencilere CAS testi uygulayarak öğrencilerin zekâ ve bilişsel becerilerinin yanı sıra dikkat eksikliği ve hiperaktivite bozukluğu gibi öğrencinin ruh sağlığına ilişkin özel nitelikli kişisel verilerin de işlenmesi sebebiyle 50.000 TL para cezası verilmişti.



Çocuklar eğitim, sosyalleşme, oyun, araştırma, bilgi edinme, eğlence ve benzeri birçok amaçla İnternette vakit geçiriyor.



Çocuklar, internet üzerinde etkileşimde buldukları kişilerle birçok kişisel verisini paylaşabilir. Bu paylaşım bazen bir platforma üye olmak, bazen bir paylaşım yapmak, beğeni atmak ya da yorum yazmak, bazen çevrimiçi bir oyun oynamak şeklinde olabilir.



Böylece çocuklarınızın kişisel verileri de birçok üçüncü kişiyle paylaşılmış oluyor. Yukarıdaki iki gerçek örnekten de görüleceği üzere veri ihlali dev şirketlerde bile çok olası.

Veri ihlali sonucunda ise çocukların kimlik hırsızlığına, siber zorbalığa, çevrimiçi tacize ve hatta fiziksel güvenlik risklerine ve tüm bunlara bağlı olarak duygusal travmalara maruz kalması kaçınılmaz.



**İstanbul Barosu**  
**Kişisel Verilerin Korunması Komisyonu**

# Veri İhlalleri ve Siber Güvenlik Risklerine Karşı Koruma

Bu sınırsız bilgi alışverişinde bazı temel siber güvenlik kurallarına ebeveynlerin de özellikle dikkat etmesi gerekir. Çünkü çocuklarınızın ne paylaştığını kontrol edemeseniz de paylaşım yaptığı donanımın siber güvenliğini kontrol edebilirsiniz!

## Güçlü Şifreler Oluşturun ve Yönetin:

- Karmaşık şifreler kullanmak çok önemlidir (büyük-küçük harf, rakam, sembol içermeli).
- Farklı hesaplar için farklı şifreler kullanın.
- Şifre yöneticisi araçları kullanın.
- Şifreleri düzenli olarak değiştirin.

## İki Faktörlü Kimlik Doğrulama (2FA):

- Ek bir güvenlik katmanı olarak 2FA'nın ne olduğu ve nasıl etkinleştirildiğini çocuğunuza öğretin ve mutlaka siz de kullanın.

## Yazılım Güncellemelerini Takip Edin:

- İşletim sistemleri, uygulamalar ve cihazlardaki yazılımları güncel tutun. Çünkü bu güncellemeler güvenlik açıklarını kapatarak koruma sağlar.
- Otomatik güncelleme özelliğini etkinleştirin.

## Güvenlik Yazılımları Kullanın:

- Antivirüs ve güvenlik duvarı gibi yazılımları mutlaka kullanın.
- Lisanslı ve güvenilir yazılımlar kullanmanız, tam kapsamlı ve etkili bir koruma için oldukça önemli.
- Yazılımlar vasıtasıyla cihazınızda ve çocuğunuzun kullandığı cihazda düzenli olarak tarama yapın.

## Gizlilik Ayarlarını Yapılandırın:

- Sosyal medya ve diğer platformlardaki gizlilik ayarlarını kontrol edin ve gerektiğinde düzenleyin.
- Konum paylaşımını sınırlayın.
- Profilin görünürlüğünü "herkese açık" olarak ayarlanmamış olduğuna emin olun.
- Erişim ve izin ayarlarını kontrol edin; gerekli olmayan izinleri vermekten kaçının.

## Ağ Güvenliğini Sağlayın:

- Güçlü bir Wi-Fi şifresi kullanın.
- Herkese açık Wi-Fi ağları kullanmamaya; çocuğunuzun bu ağlar üzerinden internete bir kullanıcı hesabı üzerinden bağlanmamasına özen gösterin. Gerekirse dışarıda kendi mobil veriniz üzerinden çocuğunuzun internete bağlanmasını sağlayın.
- Ev ağını güvenlik duvarı ile koruyun.



**İstanbul Barosu**  
**Kişisel Verilerin Korunması Komisyonu**

# Çocuğunuzun Yasal Haklarını Unutmayın!



6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile güvence altına alınan haklar, çocukların dijital dünyadaki varlıklarını koruma altına alırken, bu hakların velisi olarak siz ebeveynlere, çocuklarınızın kişisel verileri üzerinde söz sahibi olma ve onları en iyi şekilde temsil etme sorumluluğu yüklemektedir.

## **KVKK Kapsamında Çocuklarınızın Sahip Olduğu Haklar:**

**Bilgileri İşleniyor mu Öğrenme Hakkı:** Çocuklar (ya da anne babaları/vasileri) bilgilerinin alınıp alınmadığını öğrenme hakkına sahiptir.

**Bilgileri İşleniyorsa Ne Olduğunu Sorma Hakkı:** Eğer bilgileri alınıyorsa, bu konuda bilgi alma hakkı vardır.

**Bilgileri Neden Alınıyor Öğrenme Hakkı:** Bilgilerinin neden alındığını ve ne için kullanıldığını öğrenme hakkı vardır.

**Bilgileri Kimlere Veriliyor Bilme Hakkı:** Bilgilerinin yurt içinde ya da yurt dışında kimlere verildiğini bilme hakkı vardır.

**Yanlış Bilgilerini Düzelttirme Hakkı:** Eğer bilgileri yanlışsa, düzeltilmesini isteme hakkı vardır.

**Bilgilerimin Silinmesini İsteme Hakkı:** Kanunda belirtilen durumlarda, bilgilerinin silinmesini isteme hakkı vardır.

**Düzeltilme ve Silme İşlemlerinin Herkese Söylenmesini İsteme Hakkı:** Bilgileri düzeltildiğinde ya da silindiğinde, bu durumun bilgilerin verildiği herkese söylenmesini isteme hakkı vardır.

**Bilgisayarın Karar Verdiği Bir Şeye Karşı Çıkma Hakkı:** Eğer bilgiler sadece bilgisayar tarafından incelenerek aleyhlerine bir karar alınırsa, buna karşı çıkma hakkı vardır.

**Bilgileri Yanlış Kullanılırsa Zararımın Karşılanmasını İsteme Hakkı:** Eğer bilgileri kanuna aykırı olarak kullanılırsa ve bu yüzden bir zarar görürlerse, bu zararın karşılanmasını isteme hakkı vardır.





# Çocuğunuzun Yasal Haklarını Unutmayın!



Ebeveynler Olarak, Çocuğunuzun KVKK'dan Doğan Haklarını Nasıl Kullanabilirsiniz?

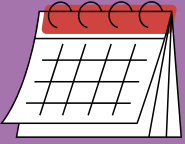
1

Sadece öğrenmek istedikleriniz varsa, veri sorumlusuna başvuru yapabilirsiniz

Bir veri ihlali gerçekleşmişse veya buna dair şüpheleriniz varsa ya da çocuğunuzun kişisel verilerinin işleme süreçleriyle ilgili öğrenmek istedikleriniz varsa, veri sorumlusuna başvurabilirsiniz.



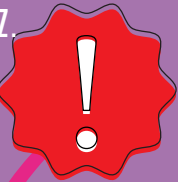
Veri sorumlusu, çocuğunuzun kişisel verilerini işleyen (okul, çocuğunuzun kişisel bilgilerini bulunduran sosyal medya platformları, oyun platformları gibi internet siteleri, Milli Eğitim Bakanlığı ve çeşitli bakanlıklar, SGK, çocuğunuzun götürdüğünüz hastaneler, diş hekimleri gibi) kişilerdir.



Unutmayın, veri sorumluları, yapmış olduğunuz başvurulara en geç 30 gün içinde cevap vermek zorundadır!



Başvurunuzu yazılı olarak (örneğin, dilekçe ile) veya elektronik ortamda (veri sorumlusunun belirttiği e-posta adresi veya başvuru formu aracılığıyla) yapabilirsiniz.



Ancak başvuruda bazı bilgilere yer vermeniz zorunludur; bunlar yer almadığında veri sorumlusu başvurunuzu kabul etmeyebilir; hatta yaptığınız başvuru şartları sağlamadığı için Kişisel Verileri Koruma Kurulu'na da şikayet edemeyebilirsiniz!

Bu yüzden başvurularınızda ad, soyad ve başvuru yazılı ise imza, TC kimlik numaranız (yabancılar için uyruk ve pasaport no), adresiniz, varsa e-posta adresi, telefon ve faks numarası ile başvurunuzda talep ettiğiniz hususun özeti.

Ayrıca başvurunuzda, hangi hakkınızı kullanmak istediğinizi açıkça belirtmeniz ve çocuğunuzun kimlik bilgilerini ve velisi olduğunuzu gösteren belgeleri sunmanız önemlidir.



**İstanbul Barosu**  
**Kişisel Verilerin Korunması Komisyonu**

# Çocuğunuzun Yasal Haklarını Unutmayın!



**Ebeveynler Olarak, Çocuğunuzun KVKK'dan Doğan Haklarını Nasıl Kullanabilirsiniz?**

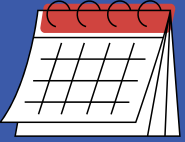
**2**

**Veri sorumlusundan yanıt alamadıysanız veya aldığınız yanıt sizi tatmin etmediyse Kişisel Verileri Koruma Kurulu'na şikayette bulunabilirsiniz**

Eğer veri sorumlusundan zamanında cevap alamazsanız veya veri sorumlusunun cevabını yeterli bulmazsanız, Kişisel Verileri Koruma Kurulu'na (Kurul) şikayette bulunabilirsiniz



Kurul'a şikayette bulunmadan önce veri sorumlusuna başvuruda bulunmuş olmanız gerekmektedir. Bunu unutmayın!



Kurul'a şikayetlerinizi veri sorumlusunun size vereceği cevabı takiben 30 gün içinde (veri sorumlusu hiç cevap vermemiş ise, veri sorumlusuna başvurunuzu takiben 60 gün içinde) yapmalısınız. Yoksa şikayetiniz işleme alınmayacaktır.

Kurul'a yapacağınız şikayetleri yazılı bir dilekçe ile gerçekleştirebileceğiniz gibi, <https://sikayet.kvkk.gov.tr> adresindeki şikayet modülünü kullanarak e-Devlet girişi ile hızlıca gerçekleştirebilirsiniz.



Şikayetinizden sonra Kurul, bir soruşturma başlatacak ve şikayet ettiğiniz veri sorumlusu kuruluştan savunma alacaktır. Daha sonra ise KVKK'ya aykırı bir durum tespit ederse, ihlalin niteliğine ve ağırlığına bağlı olarak 68 bin 83 TL'den 13 milyon 620 bin 420 TL'ye kadar idari para cezası verebilecektir.

Merak etmeyin, şikayetinizle ilgili olarak Kurul tarafından tebligat alıp soruşturma sonucundan haberdar edileceksiniz.





# Çocuğunuzun Yasal Haklarını Unutmayın!



Ebeveynler Olarak, Çocuğunuzun KVKK'dan Doğan Haklarını Nasıl Kullanabilirsiniz?

3

**Kişisel verilerin hukuka aykırı şekilde işlendiğini düşünüyorsanız tazminat davası açabilirsiniz**

Çocuğunuzun kişisel verilerinin güvenliği ihlal edilmişse veya kişisel verileri hukuka aykırı şekilde işlenmişse maddi ve manevi zararların tazminini çocuğunuz adına velayeten açacağınız bir tazminat davasıyla talep edebilirsiniz. Bunun için ikamet ettiğiniz bölgedeki ya da davalının ikamet ettiği bölgedeki yetkili asliye hukuk mahkemesine bir dava dilekçesi sunmanız gerekiyor.



Ayrıca devam eden bir veri ihlali ya da kişisel verilerin hukuka aykırı bir şekilde işlenmesi durumu söz konusu ise, tazminat talebinin yanı sıra söz konusu hukuka aykırı veri işlemenin durdurulmasını da davada isteyebilirsiniz.

4

**Kişisel veriler hukuka aykırı yöntemlerle ele geçirilmiş veya ifşa edilmiş ise savcılığa şikayette bulunabilirsiniz**

Kişisel verilerin hukuka aykırı bir şekilde işlenmesi, elde edilmesi ve üçüncü kişilerle paylaşılması halinde bazı eylemler Türk Ceza Kanunu'nda suç olarak tanımlanmıştır.

Kişisel verilerin hukuka aykırı olarak kaydedilmesi, ele geçirilmesi, bir başkasına verilmesi, yayılması ya da gerekli sürelerin geçmiş olmasına rağmen silmekle yükümlü olan kişiler tarafından silinmemesi halinde sorumlular hapis cezasıyla cezalandırılabilir.



Çocuğunuzun kişisel verilerinin Türk Ceza Kanunu'nun 135, 136, 137 ve 138'inci maddelerinde tanımlanan şekilde bir suça konu olduğunu düşünüyorsanız ikametinize en yakın adliyeye gidip savcılıkta şikayetçi olabilirsiniz. Unutmayın, bazı suçlar şikayete bağlıdır ve öğrenildikten sonra 6 ay içinde şikayetçi olmazsanız zamanaşımına uğrayabilir!



# ÇOCUKLARIN KİŞİSEL VERİLERİNİN KORUNMASI

*Çocuklar için*



İSTANBUL BAROSU  
KİŞİSEL VERİLERİN KORUNMASI KOMİSYONU





# Çocuklar Nelere Dikkat Etmelisiniz ?

## Çocuklar, Kişisel Verilerinizi Korumak İçin Nelere Dikkat Etmelisiniz?

1

### Kişisel Bilgilerin Ne Demek?

Adın, soyadın, adresin, telefon numaran, okulun ve fotoğrafların gibi bilgiler sadece sana aittir. Bu tür bilgilere "kişisel veri" denir. Bu bilgileri herkesle paylaşmak güvenli olmayabilir.

### Şifrelerini Sakla

Oyun, uygulama veya cihaz şifrelerini kimseye paylaşma. Bu şifreler senin gizliliğini korur. Sadece güvendiğin büyüklerinle paylaşabilirsin.

2

### Fotoğraflarını Paylaşmadan Önce Düşün

İnternete fotoğraf yüklemeyen önce bir büyüğüne danış. Fotoğrafların nerede ve kimler tarafından görüleceğini bilmek önemlidir.

### Tanımadığın Kişilere Bilgi Verme

İnternette tanımadığın biri sana sorular sorarsa, kişisel bilgilerini paylaşma. Bu tür durumlarda hemen bir büyüğüne haber ver.

4

### Uygulama ve Oyunları Seçerken Dikkatli Ol

Yeni bir oyun veya uygulama indirmeden önce, içeriğini ve güvenliğini kontrol et. Ebeveynlerinden veya öğretmenlerinden yardım iste.

5





# Çocuklar Nelere Dikkat Etmelisiniz?

## Çocuklar, Kişisel Verilerinizi Korumak İçin Nelere Dikkat Etmelisiniz?

1

### Herkes Dostun Olmayabilir!

İnternette tanıştığın kişiler her zaman iyi niyetli olmayabilir. Sana “adresini gönder”, “fotoğrafını yolla” gibi şeyler söylediklerinde hemen bir büyüğüne haber ver ve o bilgileri paylaşma.

### Paylaştığın Şeyler Sonsuza Kadar Kalabilir

İnternette “sildim” desen bile, o bilgiler bir yerde kalır. Sonradan pişman olabileceğin bir fotoğrafı ya da videoyu paylaşmadan önce bir kez daha düşün.

2

3

### Başkalarının Fotoğraflarını da Korumalısın

Bir arkadaşının fotoğrafını ya da videosunu paylaşmadan önce ona mutlaka sor. Herkes kendi görüntüsünün paylaşılmasından hoşlanmayabilir. Saygılı olmak çok önemli!

### Biri Bilgini İstiyorsa, Sana Açıklama Yapmalı

Adını, yaşını, fotoğrafını ya da adresini isteyen bir uygulama ya da kişi varsa, önce neden istediklerini sana açıklamaları gerekir. Anlamadığın bir şey olursa güvendiğin bir büyüğüne danış. Bilgilendirilmeden hiçbir bilgini paylaşma!

4

5

### Bilgilerin Haberin Olmadan Paylaşılıyorsa Mutlaka Söyle!

Eğer biri senin adına sosyal medya hesabı açmışsa ya da senin fotoğrafını senden habersiz paylaştıysa hemen bir büyüğüne haber ver. Bu doğru değil ve senin bu konuda hakların var.





**İstanbul Barosu**  
**Kişisel Verilerin Korunması Komisyonu**

# Katkı Sunanlar

**Av. Arda Altınok**

**Av. Benay Çaylak**

**Av. Damlanur İpek**

**Av. Dilanur Pampal**

**Av. Necati Alp Çelebi**

**Av. Sevgi Erarslan**

