Avrupa Birliği Genel Veri Koruma Tüzüğü

Almanya Uyumlaştırmalı

-Uygulamalı Açıklamalar-

20.05.2025

Av. Derman Kanal

(Almanya-Köln Barosu Üyesi)

00491735402756 / 00905494974901

Kaynak:

Federal Veri Koruma ve Bilgi Özgürlüğü Görevlisi

Metinler ve Açıklamalar Kitapçığı

Mayıs 2022, 2. Baskı

İçindekiler:

Giriş:

Genel Veri Koruma Tüzüğü (GDPR – DSGVO), dijital dünyada insanları korumaya yönelik Avrupa genelinde geçerli olan ortak yasal çerçevedir. AB'deki 433 milyondan fazla vatandaş için ortak bir veri koruma standardı oluşturur. GDPR'nin AB üye ülkelerinde daha fazla hayata geçirilmesini uyumlaştırmak, uluslararası bilişim şirketleriyle eşit düzeyde mücadele edebilmek adına öncelikli bir hedeftir.

Dijital dünyada da bireyin anayasal olarak korunan bilgiye dayalı özgür iradesi (özyönetimi) esas alınmalıdır. Zira kişisel verilerin her türlü işlenmesi bu hakka bir müdahaledir ve ancak açık bir rıza ile veya yasal bir izinle meşrulaştırılabilir.

GDPR, güçlü veri sahibi hakları sağlar; örneğin şirketler ve kamu kurumları için şeffaflık zorunlulukları ve kapsamlı bilgilendirme ve bildirim yükümlülükleri getirir. Veri taşınabilirliği hakkı veya "unutulma hakkı" gibi haklar, bireylerin verilerinin işlenmesi üzerinde etkili olmalarını sağlar.

GDPR ayrıca tüketiciler üzerinde önemli etkileri olan dijital konuları da ele alır; örneğin, puanlama (scoring) ve profil oluşturma (profiling). Ancak özellikle bu alanda, GDPR'nin uygulanmasında ve geliştirilmesinde tüketici haklarının daha da güçlendirilmesine ihtiyaç vardır. GDPR zaten 2020 yılında ilk kez değerlendirilmiştir.

Modern bir veri koruma hukukuna, veri minimizasyonu ilkeleri, tasarım yoluyla gizlilik (privacy by design) ve varsayılan olarak gizlilik (privacy by default) ilkeleri ile veri güvenliğinin sağlanması da dâhildir. GDPR bu noktada önemli standartlar koyar ve farkındalık yaratmaya katkıda bulunur. Veri koruması yalnızca kullanıcılar açısından değil, teknolojinin geliştirilmesi aşamasında da temel bir rol oynamalıdır.

Dijitalleşmenin getirdiği ciddi veri koruma riskleri nedeniyle, herkes dijital kimliğini korumaya yönelik önlemler almakla yükümlüdür. Bu zorluk yaşamın tüm alanlarını ve tüm yaş gruplarını ilgilendirmektedir. GDPR ise buna cevaplar bulmaya çalışmakta ve örneğin çocuklara özel bir önem atfetmektedir. Özellikle çocuklarla ilgili verilerin yasal işlenmesinde kişilik haklarının korunması ön planda tutulur. Toplumsal olarak bu, okullarda ve ailelerde veri koruma konusunda daha fazla bilgilendirme yoluyla dijitalleşmeye ayak uydurma hedefiyle örtüşür. Kendi verilerini güvenli bir şekilde kullanma, veri güvenliği ve veri koruma bilinci eğitimin doğal bir parçası hâline gelmelidir.

Tüm hedef grupların dijital okuryazarlığının artırılması esastır. Bu yalnızca çocuklar, ebeveynler ve öğretmenleri değil, aynı zamanda işletmeleri, çalışanları ve yaşlıları da kapsar. Herkes teknolojinin gelişimini anlayabilmeli ve kendi haklarını koruyabilmelidir. Bu yetkinlik, yalnızca güvenli şifre seçimiyle sınırlı kalmaz.

Bu bilgilendirme broşürü, GDPR ve Alman Federal Veri Koruma Yasası (BDSG) düzenlemeleri hakkında genel bir bakış sunmaya yardımcı olmayı amaçlamaktadır. Broşürde yasa metinlerinin yanı sıra GDPR'nin gerekçeleri, belirli konu başlıklarına ve belirsiz hukuk terimlerine ilişkin açıklamalar da yer almaktadır.

1. Veri Koruma Hukuku

1.1 Almanya ve Avrupa'da veri koruma açısından bir dönüm noktası olarak Genel Veri Koruma Tüzüğü (GDPR / *DSGVO (Almanca)*)

25 Mayıs 2018 tarihinden bu yana, Avrupa Genel Veri Koruma Tüzüğü (GDPR – DSGVO) yürürlüktedir. Aynı gün, yürürlükteki Federal Veri Koruma Yasası (BDSG) ile Sosyal Güvenlik Kanunu'nun Onuncu Kitabı'nda (SGB X) ve Vergi Usul Kanunu'nda (AO) geniş kapsamlı değişiklikler yürürlüğe girmiştir. 26 Kasım 2019 tarihinde ise, yaklaşık 150 federal yasanın DSGVO'ya uyarlanmasını sağlayan İkinci Veri Koruma Uyumlaştırma ve Uygulama Yasası (DSAnpUG-EU) yürürlüğe girmiştir.

Bu düzenlemelerle birlikte, Avrupa'da ve Almanya'da veri koruma hukuku tamamen yeni bir temele oturtulmuştur. Bu durum, veri koruma hukukunun tarihinde adeta bir **dönüm noktası** anlamına gelmektedir.

Önceki Alman veri koruma hukuku esas olarak iki gelişmeyle şekillenmiştir:

- Bir yandan, temel hak olarak güvence altına alınmış **bilgiye dayalı öz irade hakkı** (informationelle Selbstbestimmung) temel alınmıştır. Bu hakkın içeriği büyük ölçüde Alman Federal Anayasa Mahkemesi tarafından şekillendirilmiştir. Başlangıçta bu hak, devlet müdahalelerine karşı bir savunma mekanizması olarak görülürken, artık kişisel verilerin işlenmesinde **ekonomik çıkarlar ile bireyin kişilik hakları arasında denge** sağlanması da aynı derecede önemli hâle gelmiştir.
- Öte yandan, önceki veri koruma hukuku büyük ölçüde, ulusal hukuka aktarılması gereken **95/46/EC sayılı AB Veri Koruma Yönergesi**ne (EU Datenschutzrichtlinie) dayanıyordu. Bu yönerge, 25 Mayıs 2018 tarihi itibarıyla yürürlükten kaldırılmış ve doğrudan geçerli olan GDPR ile değiştirilmiştir. BDSG ve Almanya'daki sektöre özgü veri koruma düzenlemeleri artık yalnızca GDPR'nın izin verdiği ölçüde **tamamlayıcı** olarak geçerlidir.

GDPR, BDSG ve sektöre özgü veri koruma hükümleri, kişisel verilerin işlenmesiyle ilgili kuralları belirler. Kişisel verilerin her türlü işlenmesi, **yasal bir düzenleme** veya **ilgili kişinin açık rızası** ile **açıkça izin verilmiş** olmalıdır. Bu yasaların tümü, kişisel verilerin korunmasına yönelik kuralları içerir. Bunlar arasında, **veri işleme faaliyetinden etkilenen kişilerin hakları** da yer alır.

GDPR ve ulusal yasalar, veri işleyen taraflara, veri işlemenin yasal "oyun kurallarına" uymak ve **veri sahibini bilgilendirmek** gibi yükümlülükler getirir. Aynı zamanda, **veri sahibi kişilere de çeşitli haklar** tanır.

Veri korumanın temel amacı, **kişilik haklarının tehlikeye atılmasını önlemek**; bunun için de kişisel verilerin işlenmesine ilişkin kuralların belirlenmesi ve bilgi teknolojisinin kullanımının buna uygun olarak tasarlanmasıdır.

GDPR, **veri koruması dostu bilgi teknolojilerinin** önemini vurgular. Bu bağlamda, yalnızca **veri minimizasyonu** (veri miktarının olabildiğince az tutulması) ilkesi değil, aynı zamanda **teknik tasarım yoluyla veri koruma** (privacy by design) ve **varsayılan ayarlarla veri koruma** (privacy by default) ilkeleri de yasal olarak düzenlenmiştir (Madde 25 GDPR). Ayrıca, Madde 32 GDPR'ye göre alınması gereken teknik ve organizasyonel önlemlerle,

kişisel verilerin **gizliliği**, **bütünlüğü**, **erişilebilirliği**, **dayanıklılığı** ve **geri izlenebilirliği** güvence altına alınmalıdır.

Veri koruma denetim makamlarının rolü yalnızca denetleyici ve yaptırım uygulayıcı olmakla sınırlı değildir. Günümüzde bu makamların en önemli görevlerinden biri, **önleyici danışmanlık** sunmaktır. Kurumlar, şirketler ve vatandaşlar, veri koruma otoritelerine danışmaktan çekinmemelidir.

Veri işlemenin birçok farklı şekilde ve giderek artan biçimde gerçekleştiği günümüzde, denetim makamlarının her yerde bulunması mümkün değildir. Bu nedenle, yasal hakların ve teknik imkânların işe yaraması ancak vatandaşların bunları **bilmesi**, **kullanması** ve **veri kötüye kullanımına karşı kendilerini korumasıyla** mümkündür.

Bu noktada veri koruma otoritelerinden destek alınabilir. Aynı zamanda, kamu kurumları ve özel şirketlerin de sorumluluk alması gerekir. Bu kurumlar, yasal çerçevede **kendi kendini düzenleyen davranış kuralları** geliştirmeye çağrılır – bu hem ulusal hem de uluslararası düzeyde geçerlidir. GDPR, bu konuda davranış kuralları ve sertifikasyon için uygun bir **hukuki çerçeve** sunmaktadır.

Kurum ve işletmelerdeki **veri koruma görevlileri** (Datenschutzbeauftragte) ise son derece önemli bir rol oynamaktadır. Bu kişiler, kurum ve işletmelerde veri koruma bilincini yaygınlaştırır, veri koruma yükümlülüklerinin uygulanmasını kolaylaştırır ve denetim makamlarını destekler. Aynı zamanda çalışanlara ve vatandaşlara **danışmanlık ve uzmanlık** hizmeti sunarlar.

Veri koruma hukukuna aykırı bir eylem sonucu **zarar** oluşmuşsa, bu durum **cezasız kalmaz**. GDPR, denetim makamlarına veri koruma hukukunu etkin şekilde uygulamaları için güçlü araçlar sunar.

Bu araçlar arasında, **uyarılar**, **ikazlar**, **emirler** ve **yasaklamalar** gibi idari önlemler yer alır. GDPR uygulama alanında artık bu önlemler **kamu kurumları** için de geçerlidir. Bu sayede denetim makamlarının yalnızca etkisiz eleştirilerde bulunması yeterli olmaz; **yetkileri önemli ölçüde artırılmıştır**.

Ayrıca, GDPR'ye aykırı hemen her türlü ihlal için **önemli miktarda para cezası** öngörülmüştür. Bu cezalar, şirketlerin **küresel yıllık cirosunun %4'üne kadar** çıkabilir. Bu nedenle tüm şirketlere, GDPR yükümlülüklerine uymaları ve denetim makamlarının tavsiye ve talimatlarına uymaları şiddetle tavsiye edilir.

1.2 DSGVO, BDSG ve Alan Özel Hukuk – Bu Düzenlemeler Birlikte Nasıl İşler?

1.2.1 DSGVO'nun Önceliği

Yasal düzenlemeler: Avrupa Birliği'nin İşleyişine Dair Antlaşma (AEUV) Madde 288, DSGVO Madde 99, BDSG § 1

Almanya'da DSGVO'nun uygulama alanında, yasal temeller açısından üçlü bir sistematik geçerlidir. DSGVO bir **Avrupa Tüzüğü** olarak, üye devletlerde doğrudan uygulanabilir hukuktur. Bu nedenle, **ülke hukukuna üstünlük (Anwendungsvorrang)** ilkesi uyarınca, ulusal düzenlemeler karşısında önceliği vardır. Ulusal yasa koyucular, DSGVO hükümleriyle

çelişen düzenlemeler yapamaz, hatta bu hükümleri tekrar dahi edemez. Ancak **anlaşılabilirlik amacıyla**, istisnai olarak DSGVO hükümleri ulusal hukukta **tekrar edilebilir** (bkz. Gerekçe 8 – Erwägungsgrund 8 DSGVO). Bu nedenle, kişisel verilerin işlenmesinin hukuka uygunluğu değerlendirileceğinde **ilk bakılması gereken yer DSGVO'nun kendisidir**, çünkü doğrudan uygulanır.

BDSG ve DSGVO'nun özel kurumlara uygulanabilirliği:

Özel kurumlar, DSGVO ve BDSG'ye **ancak aşağıdaki durumlarda** tabidir:

- Verileri **kısmen de olsa otomatik yollarla işliyorlarsa** veya
- Verileri otomatik olmayan yollarla, ama **bir dosyalama sistemi içinde depoluyorlarsa ya da depolamak istiyorlarsa**

Aşağıdaki durumlar **veri koruma hukukunun dışında** tutulur (ev içi istisna – „Haushaltsausnahme"):

- Yalnızca **kişisel veya ailevi amaçlarla veri işlenmesi**

Örnek:

- Elektronik bile olsa, **kişisel bir adres defteri** tutmak veya bir hobi için kişisel verileri toplamak veri koruma hukukuna tabi değildir.
- **Özel amaçlı kamera sistemleriyle** (örneğin sadece kendi arsasını izlemek için) yapılan video gözetimi veri koruma hukukunun dışında olabilir. Ancak bu gözetim, **komşunun arsasına** yönelirse, **medeni hukuk kapsamında tazminat ve durdurma talebi** gündeme gelebilir.
- Eğer bir kişi **kamusal alana bakan bir kamerayla gözetim yapıyorsa**, bu artık kişisel faaliyet sayılmaz ve veri koruma hukukuna tabidir.
- Sosyal medya kullanıcıları, **yalnızca ailevi ya da kişisel çerçevede veri işliyorsa**, ev içi istisna kapsamında değerlendirilebilir (bkz. Gerekçe 18 DSGVO). Ancak sosyal medya **platform sağlayıcıları** için bu geçerli değildir – onlar tümüyle veri koruma hukukuna tabidir.

Ayrıca BDSG § 1 Abs. 8 uyarınca, **kamu alanında** belgelerdeki ve diğer yazılı kayıt ortamlardaki veriler de DSGVO ve BDSG kapsamındadır.

Bu kapsama giren federal kamu kurumlarına örnekler:

- **Federal Kriminal Dairesi (Bundeskriminalamt – BKA)**
- **Federal Polis (Bundespolizei)**
- **Federal Başsavcılık (Generalbundesanwalt)**
- **Gümrük Kriminal Dairesi (Zollkriminalamt)**
- **Kabahatler hukukuna göre idari makamlar olarak faaliyet gösteren diğer kamu kurumları**

JI Yönergesi doğrudan geçerli bir hukuk normu **olmadığı** için, ulusal hukuka **aktarılması (transpoze edilmesi)** gerekmektedir. Bu aktarma işlemi, **BDSG'nin 1. ve 3. bölümleri** ile gerçekleştirilmiştir.

Doğal olarak, burada da **alan özel veri koruma hukuku önceliklidir**. Örneğin:

- Federal Kriminal Dairesi Kanunu (BKAG)
- Ceza Muhakemesi Kanunu (StPO)
- Federal Polis Kanunu (BPolG)

Bu yasalarda yer alan veri koruma düzenlemeleri, JI Yönergesi kapsamındaki veri işleme faaliyetlerinde önceliklidir.

Eyaletler bakımından durum:

Eyalet düzeyinde de durum benzerdir. Burada da öncelikle **eyaletlerin kendi alan özel veri koruma hükümleri** (örneğin polis yasaları) uygulanır. Tamamlayıcı olarak, **eyalet veri koruma yasaları** devreye girer.

1.2.2 AB Hukuku Kapsamı Dışında Kalan Kamu Kurumları

Avrupa Birliği hukukunun uygulama alanı dışında kalan kamu kurumları için yalnızca **ulusal veri koruma hukuku** geçerlidir. Bu durum özellikle aşağıdaki alanları ilgilendirir:

- **Federal istihbarat servisleri**
- **Savunma alanı**

1.3 Veri Korumanın Amacı

Yasal dayanaklar: AB Temel Haklar Şartı Madde 8, AB'nin İşleyişine Dair Antlaşma (AEUV) Madde 16, DSGVO Madde 1, Alman Anayasası (Grundgesetz – GG) Madde 1 ve 2

Genel Veri Koruma Tüzüğü (DSGVO), veri korumasını **öncekine kıyasla çok daha güçlü bir şekilde Avrupa düzeyinde şekillendirmektedir.** Ancak bu, veri korumanın hedeflerinin esaslı şekilde değiştiği anlamına gelmez. Zira Avrupa veri koruma hukuku, **özgün bir temel hak biçimi olarak Alman hukuk geleneğinden etkilenmiştir**.

Avrupa düzeyinde veri koruma bir temel haktır

Kişisel verilerin korunması hakkı yalnızca Alman hukukuna özgü değildir; bugün artık **Avrupa düzeyinde bir temel haktır**:

- **AB Temel Haklar Şartı Madde 8**
- **AB'nin İşleyişine Dair Antlaşma (AEUV) Madde 16**

Temel Haklar Şartı Madde 8'e göre:

Her bireyin, kendisini ilgilendiren kişisel verilerin korunmasına hakkı vardır. Bu verilerin işlenmesi ancak:

- **dürüstlük ve iyi niyet ilkesi** (Treu und Glauben),
- **belirli amaçlarla**
- ve ya **ilgili kişinin rızasına** ya da
- **yasal bir temele** dayanarak gerçekleşebilir.

Ayrıca bu maddede, bireylerin **bilgi edinme** ve **düzeltme** hakkı ile, **bağımsız makamlar tarafından denetim hakkı** da garanti altına alınmıştır.

Lizbon Antlaşması ile birlikte Temel Haklar Şartı, yalnızca AB kurumları için değil, **üye devletler için de bağlayıcı hale gelmiştir.**

Avrupa Adalet Divanı (EuGH) kararları

Son yıllarda **Avrupa Adalet Divanı**, kişisel verilerin korunması hakkının önemini çeşitli kararlarıyla tekrar tekrar vurgulamıştır. Mahkeme, **özel hayatın gizliliği** ve **veri koruma** haklarının, kişisel verilerin işlenmesine yönelik **ekonomik çıkarlardan genellikle daha üstün** olduğunu belirtmiştir. Bu durum, veri işlemenin ancak **özel bir gerekçeye** dayanması gerektiği anlamına gelir.

EuGH, kamu kurumları ile özel şirketler arasında veri işleme bakımından **temel bir fark gözetmez** – her iki taraf da aynı yükümlülüklere tabidir.

AEUV Madde 16

- **1. fıkra**: Kişisel verilerin korunması hakkını tekrar ifade eder.
- **2. fıkra**: Kişisel verilerin korunmasına ilişkin düzenlemelerin çıkarılması konusunda **yasama yetkisini** belirler.

Bu madde, DSGVO'nun hazırlanmasının **birincil hukuk temelini** oluşturur. AEUV'nin genel hükümleri arasında yer aldığı için, veri koruma hukukunun **bir yan alan değil, tüm AB politikalarını yatay olarak etkileyen bir konu** olduğu anlaşılır.

DSGVO Madde 1

- **1. ve 2. fıkraları**: Veri koruma hakkının temel hak olduğunu vurgular ve DSGVO'nun, kişilerin **temel hak ve özgürlüklerini** korumaya hizmet ettiğini açıkça belirtir.
- **1. ve 3. fıkraları**: DSGVO'nun bir diğer amacının, **AB içindeki kişisel verilerin serbest dolaşımını** sağlamak olduğunu açıklar.

Bu serbest dolaşım, kişisel verilerin **sınırsız şekilde aktarılabileceği** anlamına gelmez. Elbette tüm aktarımlar temel haklara tabidir. Ancak amaç, AB içinde **her yerde aynı kuralların geçerli olması** ve **üye devletlerin ek kısıtlamalar getirmemesidir.**

Başka bir deyişle: Almanya, kişisel verilerin diğer üye ülkelerde işlenmesini kısıtlayan kurallar koyamaz.

Bu yaklaşımın temelinde, AB içindeki ülkelerin **üçüncü ülke (Drittstaat)** veya **yabancı ülke** olarak değerlendirilmemesi anlayışı yatar.

1.4 Veri Koruma Hukukunun Temel İlkeleri

Yasal dayanak: DSGVO Madde 5

Veri koruma hukukunun temel ilkeleri, **DSGVO'nun 5. maddesinde** açıkça belirtilmiştir. Bu ilkeler, veri işlemenin **hukuka uygun** olmasının vazgeçilmez ön koşullarını oluşturur. Her veri işleme faaliyeti, bu temel ilkelerle **uyumlu olmak zorundadır.** Aksi takdirde, bu faaliyet hukuka aykırı sayılır.

Aşağıdaki temel ilkeler, aynı zamanda veri koruma denetim makamlarının ve mahkemelerin değerlendirme ölçütlerini oluşturur:

1. Hukuka uygunluk, dürüstlük ve şeffaflık (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz)

Veri işleme faaliyetleri, sadece **yasal bir gerekçeye** dayandığında hukuka uygun sayılır. Bu işleme faaliyeti, aynı zamanda **dürüstlük ilkesine uygun** yürütülmeli ve veri sahipleri için **anlaşılır ve şeffaf** olmalıdır.

2. Amaçla sınırlılık (Zweckbindung)

Kişisel veriler, yalnızca **açıkça belirlenmiş, meşru bir amaç** için toplanmalı ve **bu amaçla uyumlu** şekilde işlenmelidir. Verilerin toplanmasından sonra **amaç değiştirilecekse**, bu durum ancak **DSGVO'nun 6. maddesine uygun olarak** ve genellikle ilgili kişinin **ayrıca bilgilendirilmesiyle** mümkündür.

3. Veri minimizasyonu (Datenminimierung)

İşlenecek kişisel veriler, sadece **gerekli olanla sınırlı** tutulmalıdır. Gereksiz veriler toplanmamalı ve işlenmemelidir. İşleme faaliyeti için **ne kadar az veri gerekiyorsa**, o kadar az veri kullanılmalıdır.

4. Doğruluk (Richtigkeit)

Kişisel veriler **doğru ve güncel** olmalıdır. Yanlış veriler düzeltilmeli, gerekli değilse silinmelidir. Veri sahibi bu kapsamda **düzeltme hakkına** sahiptir (DSGVO Madde 16).

5. Saklama süresiyle sınırlılık (Speicherbegrenzung)

Kişisel veriler, yalnızca **ilgili amaç için gerekli olduğu süre boyunca** saklanmalıdır. Amaç sona erdiğinde, veriler ya **silinmeli** ya da **anonimleştirilmelidir**.

6. Bütünlük ve gizlilik (Integrität und Vertraulichkeit)

Veriler, yetkisiz veya hukuka aykırı işlemeye karşı ve kazara kayba, yok edilmeye ya da zarar görmeye karşı uygun **teknik ve organizasyonel önlemlerle korunmalıdır**. Bu ilke, **veri güvenliğini** teminat altına alır.

7. Hesap verebilirlik (Rechenschaftspflicht)

Veri sorumlusu (örneğin bir kurum veya şirket), yukarıdaki tüm ilkelerin **uygulanmasını sağlamakla yükümlüdür** ve bunu **belgeleyebilmelidir**. Bu yükümlülüğe "**hesap verebilirlik yükümlülüğü**" denir (accountability). DSGVO'nun 5. maddesinin 2. fıkrası, bu ilkeyi açıkça düzenler.

Bu ilkeler yalnızca yasal yükümlülükler değil, aynı zamanda **veri koruma kültürünün temel taşlarıdır.** Tüm veri işleme süreçlerinin bu ilkeler ışığında tasarlanması ve yürütülmesi gerekir.

1.5 Veri Sahiplerinin Hakları

Yasal dayanaklar: DSGVO Madde 12–23

Veri sahiplerinin hakları, veri koruma hukukunun **en önemli yapı taşlarından biridir**. Bu haklar, bireylerin kendi kişisel verileri üzerindeki kontrolünü **güvence altına alır** ve veri sorumluları (örneğin şirketler veya kamu kurumları) ile daha **eşit düzeyde bir ilişki** kurulmasını sağlar.

Bu haklar özellikle **DSGVO'nun 3. bölümünde (Madde 12–23)** ayrıntılı biçimde düzenlenmiştir. Aşağıda, bu hakların kısa açıklamaları yer almaktadır:

1. Bilgilendirilme hakkı (Informationsrecht)

(DSGVO Madde 13 ve 14)

Veri sahibi, kişisel verileri toplandığında veya üçüncü bir kaynaktan elde edildiğinde, **veri sorumlusu tarafından ayrıntılı olarak bilgilendirilmelidir.** Bu bilgilendirme genellikle gizlilik beyanları (Datenschutzerklärungen) yoluyla yapılır.

Verilmesi gereken bilgiler şunlardır:

- Veri sorumlusunun kimliği ve iletişim bilgileri
- İşleme amacı ve yasal dayanağı
- Alıcı veya alıcı kategorileri
- Veri sahibinin hakları
- Veri aktarımı planlanıyorsa, bu konudaki bilgiler
- Otomatik karar verme/profil oluşturma olup olmadığı
- Gerekirse veri kaynağı

2. Erişim hakkı (Auskunftsrecht)

(DSGVO Madde 15)

Veri sahibi, veri sorumlusundan kendi hakkındaki işlenen kişisel verilerle ilgili **bilgi talep etme hakkına sahiptir.**

Verilmesi gereken bilgiler şunlardır:

- İşleme amaçları
- İlgili veri kategorileri
- Alıcılar veya alıcı kategorileri
- Saklama süresi
- Düzeltme, silme, işleme kısıtlaması, itiraz hakkı
- Şikâyet hakkı (örneğin veri koruma makamına)
- Verilerin kaynağı

- Otomatik karar verme olup olmadığı

Bu bilgiler genellikle **bir ay** içinde ve **ücretsiz** olarak sağlanmalıdır.

3. Düzeltme hakkı (Recht auf Berichtigung)

(DSGVO Madde 16)

Veri sahibi, **yanlış veya eksik** kişisel verilerin düzeltilmesini talep edebilir.

4. Silme hakkı ("Unutulma hakkı") (Recht auf Löschung)

(DSGVO Madde 17)

Veri sahibi, belirli koşullar altında kişisel verilerinin **silinmesini** talep edebilir. Bu hak, "**unutulma hakkı**" olarak da adlandırılır.

Silme hakkı aşağıdaki durumlarda geçerlidir:

- Veri işleme amacı sona erdiyse
- Veri sahibinin rızası geri çekildiyse
- Veri işleme hukuka aykırıysa
- Veri sahibi meşru şekilde itiraz ettiyse
- Veriler yasal bir yükümlülük gereği silinmek zorundaysa
- Veriler çocuklarla ilgiliyse

İstisna: Verilerin silinmesi, yasal yükümlülükler veya kamu yararı gereği mümkün olmayabilir (örneğin arşivleme amacıyla veri saklama).

5. İşlemenin kısıtlanması hakkı (Recht auf Einschränkung der Verarbeitung)

(DSGVO Madde 18)

Veri sahibi, belirli durumlarda verilerinin **işlenmesinin kısıtlanmasını** talep edebilir. Bu durumda veriler yalnızca **saklanır**; başka işlem yapılamaz.

6. Veri taşınabilirliği hakkı (Recht auf Datenübertragbarkeit)

(DSGVO Madde 20)

Veri sahibi, kendisiyle ilgili verileri **yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta** alma ve bu verileri başka bir veri sorumlusuna **aktarma** hakkına sahiptir.

Bu hak yalnızca şu durumlarda geçerlidir:

- İşleme **rızaya veya sözleşmeye** dayanıyorsa
- İşlem **otomatik yollarla** gerçekleştiriliyorsa

7. İtiraz hakkı (Widerspruchsrecht)

(DSGVO Madde 21)

Veri sahibi, kendi **özel durumu** ile ilgili gerekçelerle, veri sorumlusunun **meşru menfaatine dayanan** veri işlemeye **itiraz** edebilir.

İtiraz halinde:

- Veri sorumlusu, veri işlemeyi durdurmak zorundadır
- Ancak üstün gelen meşru gerekçeler varsa, işleme devam edebilir

Doğrudan pazarlama amacıyla veri işlenmesine her zaman **koşulsuz şekilde** itiraz edilebilir.

8. Otomatik karar verme ve profil oluşturma hakkı (Automatisierte Entscheidungen, einschließlich Profiling)

(DSGVO Madde 22)

Veri sahibi, yalnızca otomatik işlemeye dayanan ve **hukuki veya benzer şekilde önemli sonuçlar doğuran** bir karara tabi tutulmama hakkına sahiptir. Örneğin: kredi reddi, iş başvurusunun reddi.

İstisnalar sadece belirli şartlarla mümkündür – örneğin:

- Karar açıkça bir sözleşmenin ifasıyla ilgiliyse
- Veri sahibinin açık rızası varsa
- Ulusal hukuk böyle bir işleme açıkça izin veriyorsa

Bu durumda bile, veri sahibinin **insan müdahalesi talep etme, görüşünü açıklama ve karara itiraz etme hakkı** vardır.

9. Rızanın geri çekilmesi hakkı (Recht auf Widerruf einer Einwilligung)

(DSGVO Madde 7 Abs. 3)

Veri sahibi, herhangi bir zamanda daha önce verdiği **rıza beyanını geri çekebilir**. Geri çekme işlemi, geri çekmeden önceki işlemleri **hukuka aykırı hâle getirmez.**

10. Şikâyet hakkı (Beschwerderecht)

(DSGVO Madde 77)

Veri sahibi, kişisel verilerinin işlenmesinin **DSGVO'ya aykırı olduğunu düşünüyorsa**, yetkili **veri koruma denetim makamına şikâyette** bulunma hakkına sahiptir.

1.6 Görevli Makamlar ve Denetim Yapıları

Yasal dayanaklar: DSGVO Madde 51–67, BDSG §§ 8–22

Veri koruma denetimi, DSGVO'nun önemli bir parçasıdır. Bu kapsamda, hem **bağımsız denetim makamları** hem de veri sorumlularının **kendi iç yapılarındaki veri koruma görevlileri** önemli roller üstlenir. Kontrol sistemi iki düzeyde işler:

1.6.1 Kamu Kurumlarında ve Şirketlerde: Veri Koruma Görevlileri (Datenschutzbeauftragte)

Kamu kurumları ve pek çok özel şirket, **veri koruma görevlisi (DSB)** atamak zorundadır. Bu kişiler, veri koruma uygulamalarının **iç denetiminden** sorumludur ve aynı zamanda **danışmanlık** sağlarlar.

Görevleri:

- Veri işleme faaliyetlerinin **DSGVO ve BDSG'ye uygunluğunu izlemek**
- Çalışanlara **veri koruma eğitimi vermek**
- Yeni projelerde **veri koruma etkisi değerlendirmelerine** destek olmak
- Veri sahiplerinin haklarını kullanmaları konusunda **yardımcı olmak**
- Veri koruma ihlallerinde **bildirim sürecini desteklemek**
- Denetim makamları ile **iletişimi yürütmek**

Bağımsızlık ve koruma:

Veri koruma görevlileri, görevlerini yerine getirirken **bağımsızdır.** Şirketin karar organlarından etkilenmeden çalışmalıdırlar.

Atanma zorunluluğu:

- **Kamu kurumlarında** her zaman zorunludur.
- **Özel sektörde** ise aşağıdaki durumlarda zorunludur (BDSG § 38):
    - Kurumda **20 veya daha fazla kişi** sürekli veri işliyorsa
    - **Özel risk barındıran işleme faaliyetleri** varsa (örneğin hassas veriler, izleme sistemleri)
    - **Profil oluşturma** yapılıyorsa
    - **Ticari amaçla veri aktarımı** söz konusuysa

1.6.2 Federal Düzeyde: Federal Veri Koruma Görevlisi (BfDI)

Federal Veri Koruma ve Bilgi Özgürlüğü Görevlisi (BfDI), Almanya'daki federal kamu kurumlarının denetiminden sorumludur.

Yetki alanı:

- Federal otoriteler
- Federal düzeyde kamu hukukuna tabi diğer kuruluşlar
- Telekomünikasyon ve posta hizmeti sağlayıcıları (özel sektör dahil – örneğin Deutsche Telekom, Deutsche Post)

Görevleri:

- Kurumlara **danışmanlık** sunmak

- **Denetimler** yapmak
- Vatandaşların **şikâyetlerini değerlendirmek**
- **Uyarı, yasaklama ve para cezası** gibi önlemler almak (gerekli durumlarda)
- Federal Parlamento'ya **rapor sunmak**

1. **Bağımsızlık:**

BfDI, **tamamen bağımsız** çalışır. Hiçbir makamdan emir almaz. Ancak Federal Parlamento'ya karşı **sorumludur** ve görev süresi boyunca **görevden alınamaz** (BDSG § 9–11).

1.6.3 Eyalet Düzeyinde: Eyalet Veri Koruma Görevlileri

Her eyalet, kendi eyalet kamu kurumları için **bağımsız bir denetim makamı** belirlemiştir. Bunlar genellikle "**Eyalet Veri Koruma ve Bilgi Özgürlüğü Görevlisi**" adını taşır.

Görevleri:

- Eyalet düzeyinde veri işlemenin denetlenmesi
- Eyalet kurumlarına ve vatandaşlara danışmanlık
- Şikâyetlerin işleme alınması
- Gerekirse yaptırımlar uygulanması

Özel sektör denetimi:

Eyaletlerin büyük çoğunluğunda özel sektördeki şirketlerin denetiminden de **eyalet veri koruma makamları** sorumludur. Bu nedenle, şirketlerin denetim makamı çoğu zaman **bulundukları eyalete göre değişir**.

1.6.4 Avrupa Düzeyinde: EDPB ve Avrupa Komisyonu

Avrupa Veri Koruma Kurulu (EDPB)

(European Data Protection Board)

DSGVO kapsamında oluşturulmuş, tüm AB ülkelerinin denetim makamlarını bir araya getiren bağımsız bir organdır. Görevi, **DSGVO'nun tutarlı şekilde uygulanmasını sağlamaktır.**

Görevleri:

- Rehberler, tavsiyeler ve en iyi uygulama belgeleri hazırlamak
- Çapraz sınır veri işlemede denetim makamları arasında **uyum sağlamak**
- Uyuşmazlık durumlarında **bağlayıcı kararlar** vermek

Avrupa Komisyonu

- Üye devletlerin DSGVO'yu uygulayıp uygulamadığını izler
- Gerektiğinde **ihlal prosedürleri başlatabilir**
- Üçüncü ülkelere veri aktarımı için **uygunluk kararları** verir

2. DSGVO ve BDSG'nin Uygulama Alanı

2.1 DSGVO'nun Uygulama Alanı

Yasal dayanaklar: DSGVO Madde 2 ve 3

2.1.1 Maddi (konusal) uygulama alanı

DSGVO, yalnızca **"kişisel verilerin tamamen ya da kısmen otomatik işlenmesi"** için geçerlidir. Otomatik olmayan işlemler (örneğin kağıt belgeler) yalnızca **belirli bir dosyalama sisteminin** parçasıysa kapsama girer.

Örnekler:

- Bilgisayar veya cep telefonundaki müşteri verileri (otomatik)
- El yazısıyla yazılmış ve soyadına göre alfabetik sıralanmış personel listesi (otomatik olmayan, ama dosyalama sistemi parçası olduğu için kapsamda)
- Dağınık şekilde tutulmuş el yazısı notlar (kapsam dışında)

Ayrıca **DSGVO Madde 2 (2)**'ye göre aşağıdaki işlemler kapsam dışıdır:

- **Kişisel veya ev içi amaçlarla yapılan veri işleme**
  (örneğin: arkadaş doğum günü listesi, kişisel adres defteri)
- **Ceza muhakemesi veya cezaların infazı amacıyla veri işleme**
  (bu alan AB Yönergesi 2016/680 kapsamında düzenlenmiştir)
- **AB dışı kapsamda gerçekleştirilen faaliyetler**
  (örneğin: dış politika, ulusal güvenlik)

2.1.2 Kişi bakımından uygulama alanı

DSGVO, **veri sorumluları** ve **veri işleyenler** için geçerlidir:

- **Veri sorumlusu:** Kişisel verilerin işlenme amaç ve yöntemlerini belirleyen gerçek veya tüzel kişi (örneğin bir şirket)
- **Veri işleyen:** Veri sorumlusu adına veri işleyen kişi veya kuruluş (örneğin dış hizmet sağlayıcısı)

2.1.3 Mekânsal (coğrafi) uygulama alanı

DSGVO yalnızca AB içinde geçerli değildir. Madde 3 DSGVO, uygulama alanını **şirketlerin merkezi veya veri işleme yerinden bağımsız olarak** düzenler:

- AB içinde merkezi olan veri sorumluları/işleyenler: DSGVO her durumda uygulanır
- AB dışında merkezi olanlar da DSGVO kapsamındadır, **eğer**:
  - Veri işlemesi AB'deki kişilere ürün veya hizmet sunulmasıyla ilgiliyse
  - AB'deki kişilerin davranışları izleniyorsa (örneğin web sitesi analizleri)

Örnek:

Bir Amerikan şirketi, Avrupa'daki müşterilere çevrimiçi alışveriş sunuyor ve reklam amacıyla kullanıcı davranışlarını analiz ediyorsa, bu şirket **DSGVO'ya tabidir.**

3. Kişisel Veriler – Tanımlar ve İşleme Kapsamı

3.1 Kişisel Veriler Nedir?

Yasal dayanaklar: DSGVO Madde 4 No. 1

Kişisel veriler, kimliği belirli veya belirlenebilir gerçek bir kişiye ilişkin tüm bilgilerdir.

Bir kişi doğrudan (örneğin isim) veya dolaylı olarak (örneğin müşteri numarası, IP adresi, takma ad, telefon numarası) tanımlanabiliyorsa, bu bilgi kişisel veri sayılır. Verinin kişisel olup olmadığı, **bilginin tek başına yeterli olup olmamasına göre değil**, **başkaca bilgilerle bir araya getirildiğinde tanımlama yapılabiliyor mu** sorusuna göre değerlendirilir.

Örnek kişisel veriler:

- Ad, soyad
- Adres
- E-posta adresi
- Kimlik numarası
- Konum verisi
- Çevrimiçi tanımlayıcılar (örneğin çerezler, IP adresleri)
- Fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğe ilişkin bilgiler

Örnek olmayan (kişisel olmayan) veriler:

- Anonimleştirilmiş veriler (eğer kimlik belirlenemiyorsa)
- İstatistiksel veriler (örneğin: "Berlin'de 1 milyon kişi metro kullanıyor")

Ancak dikkat:
Eğer anonim veri, ek bilgilerle yeniden bir kişiye bağlanabiliyorsa, bu veriler **kişisel veri** sayılır (örneğin takma adlar veya şifrelenmiş veriler, eğer çözülmeleri mümkündeyse).

Özel kategorideki kişisel veriler (hassas veriler):

DSGVO Madde 9, aşağıdaki veri türlerini **özel koruma altına alır:**

- Irk veya etnik köken
- Politik görüş
- Dini veya felsefi inanç
- Sendika üyeliği
- Genetik veriler
- Biyometrik veriler
- Sağlık verileri
- Cinsel yaşam veya cinsel yönelim verileri

Bu veriler, **temel hak ve özgürlükler açısından yüksek risk** barındırdığı için yalnızca **istisnai durumlarda** işlenebilir (örneğin açık rıza varsa, yasal zorunluluk varsa veya kamu sağlığı gerekçesiyle).

3.2 Kişisel Verilerin İşlenmesi

Yasal dayanak: DSGVO Madde 4 No. 2

"İşleme (Verarbeitung)" terimi, DSGVO'da oldukça geniş anlamda tanımlanmıştır. Kişisel verilerle ilgili **her türlü işlem**, işleme kapsamında değerlendirilir – bu, yalnızca aktif işlemleri değil, **pasif durumları da** kapsar (örneğin sadece verinin saklanması bile bir işlemedir).

İşleme kavramına giren bazı faaliyet örnekleri:

- Verilerin toplanması (örneğin bir form aracılığıyla)
- Kaydedilmesi (örneğin veri tabanına girilmesi)
- Düzenlenmesi veya yapılandırılması
- Saklanması (örneğin dijital arşivde)
- Uyarlanması veya değiştirilmesi
- Sorgulanması veya erişilmesi
- Kullanılması (örneğin e-posta gönderimi)
- Açıklanması (aktarılması, yayılması, başka bir şekilde sağlanması)
- Eşleştirilmesi veya birleştirilmesi
- Sınırlandırılması (kısıtlama getirilmesi)
- Silinmesi veya yok edilmesi

Bu tanım, hem **otomatik** hem de **otomatik olmayan** veri işlemlerini kapsar, eğer veriler belirli bir sistem dâhilindeyse (örneğin dosyalama sistemi gibi).

Otomatik ve otomatik olmayan işleme örnekleri:

- Bir müşteri ilişkileri yazılımında müşteri bilgileri girilmesi → **otomatik**
- Bir klasörde alfabetik olarak sıralanmış kâğıt faturalar → **otomatik olmayan**, ama dosyalama sistemi içinde → DSGVO kapsamındadır
- El yazısıyla düzensiz notlar, konuya göre sıralanmamış → **işleme sayılmaz**

Yasal sonuç:

Kişisel veri ile yapılan **her türlü faaliyet**, açıkça düzenlenmiş bir **hukuki temele** dayanmak zorundadır (örneğin DSGVO Madde 6). Bu temel yoksa işleme **hukuka aykırıdır.**

3.3 Pseudonimleştirme (Takma Ad verme) ve Anonimleştirme

Yasal dayanaklar: DSGVO Madde 4 No. 5, Madde 5 (1) harf e, Madde 6 (4), Madde 25

Kişisel verilerin korunması kapsamında, verilerle çalışırken **pseudonimleştirme** (takma ad verme) ve **anonimleştirme** yöntemleri önemli bir rol oynar. Bu teknikler, veri koruma risklerini azaltmaya ve veri sahiplerinin haklarını güvence altına almaya yardımcı olur.

Pseudonimleştirme nedir?

Pseudonimleştirme, kişisel verilerin artık **doğrudan bir kişiye atfedilemeyeceği** şekilde işlenmesini ifade eder. Ancak, bu verilerin **ek bilgilerle** (örneğin bir kod çözme anahtarıyla) **yeniden kişiye bağlanması mümkündür.**

Örnek:

- Bir çalışanın adı sistemden çıkarılır ve yerine "Çalışan 1035" gibi bir kod yerleştirilir.
- Bu kodun hangi çalışana ait olduğunu gösteren liste **ayrı olarak ve güvenli bir şekilde** saklanır.

Bu durumda veri hâlâ kişisel veri sayılır, çünkü geri dönüştürülebilir. Ancak **veri işleme daha güvenli hale gelir.**

DSGVO Madde 4 No. 5'e göre, pseudonimleştirme:

- Ek verilerle birlikte ayrı tutulmalı
- Teknik ve organizasyonel önlemlerle korunmalıdır

Avantajı:
Verilerin tamamen silinmesi gerekmediği durumlarda, **pseudonimleştirme** hem veri güvenliği sağlar hem de belirli analizlerin yapılmasına olanak tanır.

Anonimleştirme nedir?

Anonimleştirme, verilerin artık **hiçbir şekilde** belirli bir kişiye atfedilemeyecek şekilde işlenmesidir – **geri dönüşü yoktur.**

Örnek:

- Bir anket çalışmasında katılımcıların isimleri ve tüm tanımlayıcı bilgiler kalıcı olarak silinir.
- Anket sonuçları yalnızca sayısal veriler olarak saklanır (örneğin yaş grupları, genel eğilimler).

Anonim veri, **DSGVO'nun kapsamına girmez** – çünkü artık kişisel veri değildir.

Hukuki farklar:

Özellik	Pseudonimleştirme	Anonimleştirme
Geri dönüş mümkün mü?	Evet, ek bilgilerle mümkündür	Hayır, geri dönüş imkansızdır
DSGVO'ya tabi mi?	Evet	Hayır
Kullanım amacı	Risk azaltma, analiz	İstatistik, araştırma, raporlama
Teknik koruma gerekli mi?	Evet	Hayır, çünkü kişisel veri değildir

Pseudonimleştirmenin teşvik edilmesi:

DSGVO, pseudonimleştirmeyi teşvik eder:

- **Madde 6 (4):** Veri işleme amacı değiştirildiğinde, pseudonimleştirme **meşrulaştırıcı bir unsur** olabilir
- **Madde 25:** "Tasarım yoluyla gizlilik (privacy by design)" ilkesi gereği, pseudonimleştirme **önleyici veri koruma önlemi** olarak kabul edilir
- **Madde 32:** Teknik-organizasyona ilişkin güvenlik önlemleri kapsamında uygun görülebilir

4. Hukuka Uygunluk – Kişisel Veri İşlemenin Yasal Dayanakları

4.1 İşlemenin Genel Hukuki Dayanağı – DSGVO Madde 6

Yasal dayanak: DSGVO Madde 6

Kişisel verilerin işlenebilmesi için mutlaka bir **hukuki dayanak** gereklidir. Bu, veri koruma hukukunun temel ilkesidir:
"Yasak – izinle serbestlik ilkesi" (Verbot mit Erlaubnisvorbehalt). Yani: Veri işleme **kural olarak yasaktır**, ancak **açıkça izin verildiği durumlarda hukuka uygun** hâle gelir.

DSGVO Madde 6 – Yasal dayanaklar nelerdir?

Bir veri işleme faaliyeti, aşağıdaki **altı gerekçeden** en az birine dayanmak zorundadır:

1. Rıza (Madde 6 (1) a)

İlgili kişi, kişisel verilerinin belirli bir amaçla işlenmesine **açık ve özgür iradesiyle** onay vermiştir.

Koşullar:

- Rıza açık olmalıdır (örtülü olmamalı)
- Belirli bir amaç için verilmiş olmalıdır
- Her zaman geri çekilebilir (bkz. Madde 7)

Not: Rıza geçerli olsa bile, diğer yasal dayanaklara göre **daha az güvenli** olabilir. Özellikle çalışanlar açısından "özgürlük" tartışmalı olabilir.

2. Sözleşmenin ifası (Madde 6 (1) b)

Veri işlemesi, **sözleşmenin kurulması veya ifası** için gereklidir.

Örnekler:

- Online siparişte teslimat adresinin alınması
- Müşteri hesabı oluşturulması

- Sözleşme öncesi teklif gönderimi

3. Hukuki yükümlülüğün yerine getirilmesi (Madde 6 (1) c)

Veri sorumlusu, **yasal bir yükümlülük** gereği veri işliyordur.

Örnekler:

- Vergi hukuku gereği fatura bilgilerinin saklanması
- Kamu kurumu olarak kanunen öngörülen bildirimler

4. Hayati çıkarların korunması (Madde 6 (1) d)

İlgili kişinin veya başka birinin **hayati çıkarlarını** korumak için veri işlemesi gereklidir.

Örnekler:

- Acil tıbbi müdahalede kimlik ve sağlık verilerinin işlenmesi
- Kazazedeye ait iletişim bilgilerinin paylaşılması

5. Kamu yararı veya kamu yetkisi (Madde 6 (1) e)

Veri işlemesi, kamu yararına yürütülen bir görev için veya kamu yetkisi çerçevesinde gereklidir.

Özellikle kamu kurumları bu maddeye dayanarak işlem yapar.

Not: Bu gerekçeye dayanmak için **ulusal veya AB hukukunda açık düzenleme** bulunmalıdır.

6. Meşru menfaat (Madde 6 (1) f)

Veri işlemesi, veri sorumlusunun veya üçüncü bir kişinin **meşru menfaatleri** için gereklidir ve bu menfaatler, ilgili kişinin temel hak ve özgürlüklerinden ağır basmaktadır.

Örnekler:

- Dolandırıcılığa karşı sistem güvenliği sağlamak
- Müşteri ilişkilerini geliştirmek
- Reklam/analiz amaçlı veri değerlendirmesi (sınırlı ölçüde)

Ancak: Bu maddeye dayanıldığında her zaman **çıkar dengesi** analizi yapılmalıdır.

4.2 Rıza Beyanına İlişkin Gereklilikler – DSGVO Madde 7

Yasal dayanak: DSGVO Madde 7

Kişisel verilerin işlenmesinde rıza (onay) önemli bir yasal dayanak olabilir. Ancak bu rıza ancak belirli **şartlar** altında geçerlidir. DSGVO'nun 7. maddesi, **rıza beyanının geçerliliği** ve **geri çekilmesi** ile ilgili kuralları düzenler.

Rıza beyanı geçerli sayılabilmesi için aşağıdaki kriterleri karşılamalıdır:

1. **Açık ve özgür iradeye dayalı olmalıdır**
   – Kişi baskı altında olmamalıdır
   – Rızanın verilmesi bir koşula bağlanmamalıdır ("rıza ya da hizmet yok" gibi)
2. **Belirli bir amaç için verilmiş olmalıdır**
   – Genel ve belirsiz rızalar geçersizdir
3. **Açık ve anlaşılır bir şekilde bilgilendirme yapılmalıdır**
   – Kişi, neye onay verdiğini açıkça anlamalıdır
   – Bilgilendirme açık, sade ve anlaşılır bir dille yapılmalıdır (Madde 12)
4. **Rıza ispat edilebilir olmalıdır**
   – Veri sorumlusu, rızanın gerçekten verildiğini ispat etmekle yükümlüdür
   – Bu nedenle rıza mümkünse yazılı veya dijital kayda alınmalıdır

Rızanın geri çekilmesi (Madde 7 (3))

- Rıza, **her zaman ve gerekçesiz olarak geri çekilebilir**
- Geri çekme, rızaya dayalı işlemeyi **geleceğe dönük olarak** geçersiz kılar
- Veri sahibi, geri çekme hakkında **rıza verilmeden önce bilgilendirilmelidir**
- Geri çekme işlemi **kolay ve zahmetsiz** olmalıdır (örneğin: tek tıkla e-posta listesi aboneliğinden çıkış)

Uygulamada dikkat edilmesi gerekenler:

- **Formlar, kutucuklar, butonlar**: Rıza için kullanılan yöntemler açık ve ayrılabilir olmalı
  – "Tüm şartları ve veri işlemeye onay veriyorum" gibi toplu kutular **geçerli değildir**
- **Önceden işaretli kutular**: Geçersizdir – kullanıcı aktif olarak seçim yapmalıdır
- **Çocuklardan alınan rıza**: 16 yaş altı bireyler için, **ebeveyn onayı gereklidir** (DSGVO Madde 8, Almanya'da 16 yaş sınırı geçerlidir)

4.3 Meşru Menfaat Dengesi – DSGVO Madde 6 (1) f

Yasal dayanak: DSGVO Madde 6 (1) f

DSGVO Madde 6 (1) f, kişisel verilerin işlenmesine şu durumda izin verir:

"İşlemenin, veri sorumlusunun veya üçüncü bir kişinin meşru menfaatleri için gerekli olması ve ilgili kişinin temel hak ve özgürlüklerinin bu menfaate ağır basmaması."

Bu, DSGVO'daki en **esnek** ancak aynı zamanda **en dikkatli değerlendirme gerektiren** yasal dayanaklardan biridir.

1. Meşru menfaat nedir?

Bu terim, geniş yorumlanabilir ve sadece ekonomik çıkarları değil, aynı zamanda güvenlik, dolandırıcılığın önlenmesi veya hizmet iyileştirmesi gibi **haklı çıkarları** da kapsar.

Örnekler:

- BT sistemlerinin güvenliğinin sağlanması
- Müşteri sadakat programlarının yürütülmesi
- Doğrudan pazarlama faaliyetleri
- Yasa dışı eylemlerin tespiti ve önlenmesi
- İş yerinde sınırlı kamera gözetimi

2. Denge testi nasıl yapılır?

Veri sorumlusu, işleme faaliyetinin meşru menfaate dayanıp dayanmadığını belirlemek için **üç aşamalı bir denge testi** yapmak zorundadır:

A. Meşru bir menfaat var mı?

İşlemenin arkasındaki amaç **meşru ve haklı** olmalıdır. Rastgele veya keyfi gerekçeler kabul edilemez.

B. İşleme gerekli mi?

Amaç, bu şekilde veri işlenmeden **başka yollarla** sağlanabilir mi?
– Eğer daha hafif bir yöntem varsa, tercih edilmelidir.

C. İlgili kişinin hakları daha ağır mı basıyor?

Veri sahibinin temel hak ve özgürlükleri, işlemeye engel teşkil ediyor mu?

Değerlendirme kıstasları:

- Kişisel verilerin türü (örneğin hassas mı?)
- İşlemenin şeffaflığı
- İlgili kişinin makul beklentileri
- Veri işleme süresi
- İtiraz hakkı sağlanıyor mu?
- Güvenlik önlemleri yeterli mi?

3. Belgelendirme ve şeffaflık zorunluluğu

- Denge testinin **belgelendirilmesi önerilir** (örneğin dahili risk değerlendirme belgesi)
- Veri sahibi, gizlilik beyanı aracılığıyla bu işlemeden **haberdar edilmelidir**
- Madde 21 kapsamında, kişi işleme faaliyetlerine **itiraz etme hakkına** sahiptir

4. Doğrudan pazarlamada özel durum

Doğrudan reklamcılık amacıyla veri işleme, genellikle meşru menfaat olarak kabul edilir (bkz. Gerekçe 47). Ancak:

- Veri sahibine açıkça **itiraz hakkı** tanınmalı
- İtiraz gelirse, işleme **derhal durdurulmalıdır**

E-posta ile pazarlama için ayrıca Almanya'da **UWG (Haksız Rekabet Yasası)** hükümleri de dikkate alınmalıdır.

4.4 Hassas Verilerin İşlenmesi – DSGVO Madde 9

Yasal dayanak: DSGVO Madde 9

DSGVO Madde 9, bazı kişisel veri türlerinin işlenmesini **özellikle hassas (korunmaya değer)** olarak sınıflandırır ve bu verilerin işlenmesini **genel olarak yasaklar**. Ancak belirli istisnai durumlarda, bu tür verilerin işlenmesine **açıkça izin verilir**.

Hangi veriler hassas (özel nitelikli) sayılır?

Madde 9 (1) uyarınca aşağıdaki veriler özel koruma altındadır:

- Irk veya etnik köken
- Politik görüş
- Dini veya felsefi inançlar
- Sendika üyeliği
- Genetik veriler
- Biyometrik veriler (kimlik tespiti amacıyla)
- Sağlık verileri
- Cinsel yaşam veya cinsel yönelim verileri

Bu verilerin işlenmesi, temel hak ve özgürlükler açısından yüksek risk taşıdığı için **özel yasal düzenlemelere tabidir.**

Ne zaman işlenebilirler? – İstisnalar (Madde 9 (2))

Bu veriler, aşağıdaki istisnai durumlardan biri söz konusuysa işlenebilir:

1. **Açık rıza verilmişse** (Madde 9 (2) a)
   – İlgili kişi, verisinin işlenmesine **özgür iradesiyle ve açıkça** rıza göstermelidir.
   – Rıza verilmemişse veya geri çekilirse, işleme hukuka aykırı olur.
2. **İş hukuku, sosyal güvenlik veya sosyal koruma hukuku çerçevesinde zorunluysa** (Madde 9 (2) b)
   – Örneğin: iş göremezlik raporlarının işverence saklanması
3. **Hayati çıkarların korunması için gerekli ise** (Madde 9 (2) c)
   – Örneğin: baygınlık geçiren bir kişiye müdahale için sağlık bilgisine ulaşılması
4. **Üyelikle bağlantılı olarak, siyasi, dini veya sendikal kuruluşlar tarafından işleniyorsa** (Madde 9 (2) d)
   – Örneğin: bir kilise cemaati üyelik kaydı

5. **Kamuya açık bir şekilde açıklanmışsa** (Madde 9 (2) e)
   – Örneğin: kişi dini inancını sosyal medyada paylaşmışsa
6. **Bir hak talebi veya yasal savunma için gerekiyorsa** (Madde 9 (2) f)
   – Örneğin: bir dava sürecinde sağlık raporlarının sunulması
7. **Önemli kamu yararı gerekçesi varsa** (Madde 9 (2) g)
   – Ulusal veya AB hukuku açık şekilde bu işleme izni vermelidir
8. **Halk sağlığının korunması için işleniyorsa** (Madde 9 (2) i)
   – Örneğin: bulaşıcı hastalıkların takibi
9. **İstatistiksel, bilimsel veya tarihi araştırma amaçlıysa** (Madde 9 (2) j)
   – Ancak bu tür işlemlerde ek güvenlik önlemleri alınmalıdır (örneğin pseudonimleştirme)

Ek güvenlik önlemleri

Hassas verilerin işlenmesinde aşağıdaki ilkelere **özellikle dikkat edilmelidir**:

- **Veri minimizasyonu**: Yalnızca gerçekten gerekli olan veriler işlenmeli
- **Erişim kontrolü**: Bu verilere erişim sadece yetkili kişilerle sınırlandırılmalı
- **Şifreleme ve pseudonimleştirme**: Uygun teknik önlemler alınmalı
- **Silme politikası**: Veri artık gerekli değilse silinmeli
- **Rıza belgeleri açık ve anlaşılır olmalı**

4.5 Sağlık Verileri – DSGVO ve BDSG Uygulaması

Yasal dayanaklar: DSGVO Madde 4 No. 15, Madde 9 (1), Madde 9 (2) h, Madde 9 (3); BDSG § 22

Sağlık verileri, DSGVO kapsamında **özel olarak korunması gereken kişisel verilerdir**. Bu veriler, bireylerin fiziksel veya ruhsal sağlığı hakkında bilgiler içerir ve doğrudan veya dolaylı olarak kişisel sağlık durumunun anlaşılmasına imkân tanır.

1. Sağlık verisi nedir?

DSGVO Madde 4 No. 15'e göre:

"Sağlık verisi, bir gerçek kişinin fiziksel ya da ruhsal sağlığına ilişkin ve bu kişinin sağlık durumu hakkında bilgi veren kişisel verilerdir."

Örnekler:

- Hastalık teşhisleri
- Laboratuvar sonuçları
- Röntgen görüntüleri
- Reçeteler
- Engellilik bilgileri
- Aşı durumu
- Psikolojik durumla ilgili bilgiler

2. Genel ilke: İşleme yasağı

DSGVO Madde 9 (1) uyarınca, sağlık verilerinin işlenmesi kural olarak **yasaktır.** Ancak belirli istisnalar altında bu yasağın kalkmasına izin verilir.

3. Sağlık verilerinin işlenmesine ne zaman izin verilir?

DSGVO Madde 9 (2) h uyarınca:

Sağlık verileri şu durumlarda işlenebilir:

- Sağlık veya sosyal hizmetlerin sunulması
- Sağlık hizmetlerinin yönetimi (örneğin hasta kayıtları)
- Tıbbi teşhis
- Tedavi veya bakım hizmetleri
- Sağlık sistemlerinin/kurumlarının işleyişi

Ancak şu koşullar gereklidir:

- İşleme, bir sağlık mesleği mensubu tarafından yapılmalı veya onun sorumluluğunda yürütülmeli
- Bu kişi mesleki gizliliğe tabi olmalıdır (örneğin hekim, hemşire, psikolog)

Alternatif olarak:

- İlgili kişinin **açık rızası** varsa (Madde 9 (2) a)
- İşleme, **hayati çıkarları** korumak için gerekiyorsa (Madde 9 (2) c)
- **Kamu sağlığına ilişkin nedenlerle** işleniyorsa (Madde 9 (2) i)

4. BDSG § 22'ye göre uygulama

BDSG § 22, sağlık verileri dâhil olmak üzere özel nitelikli verilerin işlenmesini daha ayrıntılı düzenler. Buna göre:

- İşleme yalnızca **özel koruma önlemleri** ile mümkündür
- Uygun teknik ve organizasyonel önlemler alınmalıdır
- Özellikle **erişim sınırlamaları**, **şifreleme**, **eğitimli personel** ve **veri minimizasyonu** gibi önlemler şarttır

5. Sağlık verilerinin üçüncü taraflara aktarılması

Sağlık verileri, yalnızca şu durumlarda üçüncü kişilere aktarılabilir:

- İlgili kişi **açık rıza vermişse**
- **Yasal bir zorunluluk** varsa (örneğin bulaşıcı hastalık bildirimi)
- Hayati çıkarların korunması gerekiyorsa

Aksi hâlde aktarım hukuka aykırıdır.

6. Özellikle dikkat edilmesi gereken alanlar:

- **İşyerinde sağlık verileri** → yalnızca sınırlı koşullarda işlenebilir
- **Sigorta şirketleri** → açık rıza ya da yasal zorunluluk olmadan veri işleyemez
- **Okullar veya kreşler** → yalnızca enfeksiyon koruma yasaları kapsamında sınırlı veri işleyebilir
- **Psikolojik veriler** → ek hassasiyet gerektirir, mutlaka gizlilik kurallarına uyulmalıdır

4.6 Ceza Hukuku Kapsamındaki Veriler – DSGVO Madde 10 ve BDSG § 46

Yasal dayanaklar: DSGVO Madde 10, BDSG § 46

Ceza hukuku kapsamındaki kişisel veriler, DSGVO ve BDSG uyarınca **özel koruma gerektiren başka bir veri kategorisini** oluşturur. Bu verilerin işlenmesi yalnızca **sıkı koşullar altında** mümkündür.

1. Hangi veriler ceza hukuku kapsamına girer?

DSGVO Madde 10'da belirtilen veriler şunlardır:

- Ceza mahkûmiyetleri
- Suçlar ve kabahatler
- Önleyici güvenlik tedbirleri
- Ceza davalarıyla ilgili bilgiler
- Kolluk kuvvetlerinin veya adli makamların değerlendirme ve sınıflandırmaları

Örnekler:

- Sabıka kaydı
- Devam eden bir ceza soruşturmasına ilişkin bilgiler
- Güvenlik riski değerlendirmeleri (örneğin havalimanı kontrollerinde)

2. DSGVO Madde 10'un içeriği

Bu maddeye göre:

"Ceza mahkûmiyetlerine ve suçlara ilişkin kişisel verilerin işlenmesi, yalnızca ulusal hukukun izin verdiği ölçüde ve uygun güvencelerle yapılabilir. Bu tür veriler, yalnızca yetkili makamların gözetiminde işlenmelidir veya AB veya üye devlet hukuku, bunun dışında açık bir hüküm içermelidir."

3. BDSG § 46'ya göre düzenleme

Almanya'da ceza verilerinin işlenmesi **BDSG § 46** tarafından ayrıntılı biçimde düzenlenmiştir. Buna göre:

- Bu tür veriler ancak **özel olarak yetkilendirilmiş makamlar** tarafından işlenebilir
- İşleme faaliyeti, **yasal bir dayanağa** sahip olmalıdır
- İşleme sırasında **uygun teknik ve organizasyonel önlemler** alınmalıdır
- Verilerin amacı dışında kullanımı **yasaktır**

4. Kimler bu verileri işleyebilir?

- **Kolluk kuvvetleri** (örneğin polis, gümrük)
- **Yargı makamları**
- **Savcılıklar**
- **Adli sicil kurumları**
- **Belirli kamu kurumları**, eğer görev alanı bunu gerektiriyorsa

5. Özel sektörün durumu

Özel sektör (örneğin işverenler, sigorta şirketleri) ceza hukuku kapsamındaki verileri:

- **Yalnızca istisnai hallerde** ve
- **açık yasal dayanak veya açık rıza** ile işleyebilir

Örnek:

- Bir işveren, sabıka kaydı sunulmasını talep edebilir ancak yalnızca ilgili pozisyon için **zorunlu güvenlik gerekçeleri** varsa (örneğin çocuklarla çalışma)

6. Güvence önlemleri

Ceza hukuku kapsamındaki verilerin işlenmesinde:

- **Yetkisiz erişim engellenmelidir**
- **Erişim kayıtları tutulmalıdır**
- Verilere yalnızca **yetkili personel** erişebilmelidir
- İşleme amacı açıkça tanımlanmalı ve yalnızca bu amaçla sınırlı kalınmalıdır
- Gereksiz veriler silinmeli ya da anonimleştirilmelidir

5. Veri Sahibi Bilgilendirmesi ve Şeffaflık Yükümlülüğü

5.1 Genel Bilgilendirme Yükümlülüğü – DSGVO Madde 12

Yasal dayanak: DSGVO Madde 12

DSGVO'nun temel ilkelerinden biri **şeffaflık** ilkesidir. Veri işleyen kişi ya da kurum, ilgili kişilere kişisel verilerinin işlenmesi hakkında **kolay erişilebilir ve anlaşılır** bilgiler sunmakla yükümlüdür. Bu yükümlülük, özellikle **Madde 12 ile** düzenlenmiştir.

1. Açık, sade ve anlaşılır dil

Veri sahiplerine yapılacak bilgilendirme:

- **Açık ve sade** bir dille yazılmalıdır
- **Anlaşılır olmalı**, teknik terimlerden kaçınılmalıdır
- Gerektiğinde **görsel öğeler** veya örneklerle desteklenebilir
- Özellikle **çocuklara yönelik** bilgiler, çocukların anlayabileceği şekilde hazırlanmalıdır

2. Bilgilendirme araçları

Bilgilendirme:

- Yazılı olarak (örneğin mektupla)
- Elektronik ortamda (örneğin internet sitesi, e-posta)
- Sözlü olarak (örneğin müşteri hizmeti görüşmesi sırasında) sağlanabilir

Veri sahibi talep ederse, bilgilendirme **yazılı** veya **elektronik** olarak sunulmalıdır (örneğin PDF belgesi).

3. Bilgilendirme ne zaman yapılmalı?

- **Veriler ilgili kişiden toplanıyorsa → toplama sırasında** bilgi verilmeli (Madde 13)
- **Veriler üçüncü bir kaynaktan elde ediliyorsa** → en geç **bir ay içinde**, ilk iletişim sırasında veya ilk açıklama anında bilgi verilmeli (Madde 14)

4. Bilgilendirme ücretsizdir

Veri sahibi, bu bilgilere **ücretsiz olarak** erişme hakkına sahiptir.
Sadece **açıkça temelsiz veya aşırı** taleplerde (örneğin tekrar tekrar istenirse) makul bir ücret talep edilebilir.

5. Teknik ve organizasyonel gereklilikler

Veri sorumlusu, bilgilendirme yükümlülüğünü yerine getirebilmek için:

- Şeffaf bir **veri işleme kaydı** tutmalıdır
- Hangi verilerin ne amaçla işlendiğini sistemli şekilde tanımlamalıdır
- **Gizlilik beyanı** (Datenschutzerklärung) hazırlamalıdır
- **Bilgi taleplerine** hızlı ve doğru şekilde yanıt verecek süreçleri kurmalıdır

5.2 Doğrudan Veri Toplama Durumunda Bilgilendirme – DSGVO Madde 13

Yasal dayanak: DSGVO Madde 13

Veri sorumlusu, kişisel verileri **doğrudan ilgili kişiden topluyorsa**, DSGVO Madde 13'e göre, bu kişiye veri toplandığı **anda** aşağıdaki bilgileri sağlamakla yükümlüdür.

1. Bilgilendirme ne zaman yapılmalıdır?

Bilgilendirme:

- **Veri toplandığı anda** veya
- **En geç veri toplama sırasında** yapılmalıdır.

Örnek:

- Bir web formu doldurulуyorsa, formun altında bilgilendirme metni yer almalı
- Bir sözleşme imzalanıyorsa, gizlilik beyanı eklenmiş olmalı

- Telefonla bilgi alınırken, görüşme başında sözlü bilgilendirme yapılmalı

2. Hangi bilgiler verilmelidir? (Madde 13 (1) ve (2))

Veri sahibine aşağıdaki konularda bilgi verilmelidir:

Madde 13 (1):

- **Veri sorumlusunun kimliği ve iletişim bilgileri**
- Varsa, **veri koruma görevlisinin iletişim bilgileri**
- Verilerin işlenme **amaçları** ve **hukuki dayanakları**
- Veri işleme meşru menfaate dayanıyorsa, bu **meşru menfaatin** ne olduğu
- Verilerin alıcıları veya alıcı kategorileri
- Verilerin **üçüncü bir ülkeye** veya **uluslararası kuruluşa** aktarılıp aktarılmadığı (ve varsa güvenlik önlemleri)

Madde 13 (2):

- Verilerin saklanma süresi veya bu sürenin belirlenme kriterleri
- Veri sahibinin hakları:
    - Erişim hakkı
    - Düzeltme hakkı
    - Silme hakkı
    - İşlemenin kısıtlanması hakkı
    - İtiraz hakkı
    - Veri taşınabilirliği hakkı
- Rızaya dayalı işleme varsa: **rıza her zaman geri çekilebilir**
- Şikâyet hakkı: ilgili veri koruma denetim makamına başvuru hakkı
- Yasal ya da sözleşmesel bir yükümlülük gereği verilerin sağlanıp sağlanmadığı ve bu verilerin sağlanmamasının olası sonuçları
- Otomatik karar verme/profil oluşturma olup olmadığı ve varsa mantığı ile beklenen sonuçlar

3. Özel durumlar

Bilgilendirme metni, veri sahibinin **anlayabileceği düzeyde ve uygun biçimde** hazırlanmalıdır:

- **Çocuklar** için özel olarak uyarlanmış açıklamalar
- **Kolay erişim** (örneğin: web sitesinde görünür bağlantı)
- Gerekiyorsa **çok dilli** metinler

4. Belgelendirme ve ispat yükümlülüğü

Veri sorumlusu, bilgilendirme yükümlülüğünü yerine getirdiğini **ispat edebilmelidir**.

Bu nedenle:

- **Gizlilik beyanı** yazılı veya dijital olarak saklanmalı
- Formların üzerine tarih ve imza alınmalı

- Elektronik sistemlerde **log kaydı** tutulmalı

5.3 Dolaylı Veri Toplama Durumunda Bilgilendirme – DSGVO Madde 14

Yasal dayanak: DSGVO Madde 14

Veri sorumlusu, kişisel verileri **doğrudan ilgili kişiden değil**, başka bir kaynaktan (örneğin üçüncü bir kişi, kamu kayıtları, internet) elde ediyorsa, bu durumda da veri sahibine **ayrıntılı bilgi verme yükümlülüğü** vardır. Bu yükümlülük **Madde 14'te** düzenlenmiştir.

1. Bilgilendirme ne zaman yapılmalıdır?

Bilgilendirme, aşağıdaki süreler içinde yapılmalıdır:

- **Veri elde edilmesini takiben en geç bir ay içinde**,
- **Veri sahibiyle ilk iletişim kurulursa**, bu sırada,
- **Veriler başka bir alıcıya ilk kez açıklanıyorsa**, bu açıklama sırasında

2. Hangi bilgiler verilmelidir?

Veri sahibine Madde 14 uyarınca aşağıdaki bilgiler sunulmalıdır:

Madde 14 (1):

- Veri sorumlusunun **kimliği ve iletişim bilgileri**
- Varsa veri koruma görevlisinin iletişim bilgileri
- Veri işleme **amaçları**
- İşlemenin **hukuki dayanağı**
- İşlemenin dayandığı **meşru menfaatler** (varsa)
- **Veri kategorileri** (çünkü kişi kendi verisini vermemiştir)
- **Verilerin kaynağı** ve varsa bu kaynağın kamuya açık olup olmadığı
- Alıcılar veya alıcı kategorileri
- Verilerin üçüncü bir ülkeye aktarılıp aktarılmadığı ve varsa uygun güvenceler

Madde 14 (2):

- Verilerin saklanma süresi veya belirleme kriterleri
- Veri sahibinin hakları (erişim, düzeltme, silme, vs.)
- Rıza varsa, her zaman geri çekilebileceği bilgisi
- Şikâyet hakkı
- Verilerin sağlanmasının yasal ya da sözleşmesel bir zorunluluk olup olmadığı
- Otomatik karar alma / profil oluşturma olup olmadığı ve etkileri

3. Bilgilendirme yapılmayabileceği istisnalar

DSGVO Madde 14 (5) bazı durumlarda bilgilendirmeden **vazgeçilebileceğini** belirtir:

- İlgili kişi zaten gerekli tüm bilgilere sahipse
- Bilgilendirme **imkânsız** ise veya orantısız çaba gerektiriyorsa
  (örneğin: çok sayıda veri sahibi, bilgi iletişimi teknik olarak mümkün değil)

- Bilgilendirme, bir yasal düzenleme nedeniyle açıkça yasaklanmışsa
- Bilgilendirme, yasal amaçların (örneğin suçla mücadele) gerçekleştirilmesini engelliyorsa

Ancak dikkat: Bu istisnalar **sıkı şekilde yorumlanmalı** ve belgelenmelidir.

4. Uygulama örnekleri

Durum	Ne zaman bilgilendirme yapılmalı?
Veri sosyal medyadan toplanmışsa	En geç bir ay içinde
Kredi derecelendirme verileri kullanılıyorsa	En geç ilk karar verme anında
Kişiyle hemen iletişime geçiliyorsa	İletişim sırasında

6. Veri Sahibinin Hakları – Erişim, Düzeltme, Silme, Kısıtlama, İtiraz

6.1 Erişim Hakkı – DSGVO Madde 15

Yasal dayanak: DSGVO Madde 15

Veri sahibi, DSGVO uyarınca **kendi kişisel verilerine ilişkin bilgi talep etme hakkına sahiptir.** Bu hak, veri işlemenin şeffaflığını ve denetlenebilirliğini güvence altına alır.

1. Ne talep edilebilir?

Veri sahibi, veri sorumlusuna başvurarak aşağıdaki bilgileri **ücretsiz** olarak talep edebilir:

- Kendi kişisel verilerinin işlenip işlenmediği
- İşleniyorsa:
    - İşleme amaçları
    - İlgili kişisel veri kategorileri
    - Alıcılar veya alıcı kategorileri (verilerin açıklandığı veya açıklanacağı)
    - Verilerin saklama süresi (veya belirleme kriterleri)
    - Düzeltme, silme, kısıtlama ve itiraz hakları
    - Denetim makamına şikâyet hakkı
    - Verilerin kaynağı (veri doğrudan ilgili kişiden alınmamışsa)
    - Otomatik karar verme/profil oluşturma olup olmadığı ve etkileri

Ayrıca veri sahibi, **işlenen verilerin bir kopyasını** da talep edebilir (Madde 15 (3)).

2. Süre ve biçim

- Bilgilendirme **en geç bir ay içinde** sağlanmalıdır
- Gerektiğinde bu süre **iki aya kadar uzatılabilir**, ancak bu durumda ilgili kişiye gerekçesiyle birlikte bilgi verilmelidir
- Bilgi, **yazılı veya elektronik** olarak sunulabilir
- Talep **kimliği açıkça belli olan** kişiden gelmelidir – kimlik doğrulaması yapılabilir

3. İstisnalar ve sınırlamalar (BDSG § 34)

Aşağıdaki durumlarda bilgi verme **tamamen ya da kısmen reddedilebilir**:

- Devlet güvenliği veya kamu düzeni tehlikeye giriyorsa
- Bilginin açıklanması üçüncü kişilerin haklarını ihlal ediyorsa
- Adli soruşturma, ceza kovuşturması veya idari işlemler engelleniyorsa
- Veri yalnızca istatistiksel veya bilimsel amaçla kullanılıyorsa ve ilgili kişinin hakları ciddi şekilde etkilenmiyorsa

Not: Bilgi verilmediğinde, bu durum veri sahibine gerekçesiyle birlikte **yazılı olarak açıklanmalıdır.**

6.2 Düzeltme Hakkı – DSGVO Madde 16

Yasal dayanak: DSGVO Madde 16

Veri sahibi, işlenen kişisel verilerinin **eksik veya yanlış olması durumunda**, veri sorumlusundan bu verilerin **derhal düzeltilmesini** talep etme hakkına sahiptir.

1. Hakkın kapsamı

Veri sahibi:

- Yanlış olan kişisel verilerinin **doğrulanmasını**
- Eksik olan verilerin ise, duruma göre **tamamlanmasını** talep edebilir

Örnekler:

- Yanlış yazılmış isim, doğum tarihi, adres
- Eksik iş unvanı veya akademik derece
- Güncel olmayan iletişim bilgileri

Not: Gerekirse, veri sahibi düzeltmeyi destekleyen **kanıt sunmakla yükümlüdür** (örneğin kimlik fotokopisi).

2. Düzeltme süresi

Veri sorumlusu, düzeltme talebini aldıktan sonra **gecikmeden (unverzüglich)** işlem yapmak zorundadır.

Bu, pratikte **birkaç gün ile birkaç hafta** arasında makul bir süreyi ifade eder – konuya göre değişir.

3. Eksik verilerin tamamlanması

Eğer kişisel veriler eksikse, veri sahibi:

- Bunların **ek bir açıklama beyanıyla** (z. B. “Ergänzende Erklärung”) tamamlanmasını da talep edebilir.

Örnek:
İş başvurusu formunda yalnızca soyad girilmişse, kişi “ad” bilgisinin de eklenmesini talep edebilir.

4. Üçüncü kişilere bildirimi

Eğer düzeltme yapılan veriler **önceden üçüncü taraflara iletilmişse**, veri sorumlusu bu **düzeltmeyi de söz konusu alıcılara bildirmekle yükümlüdür** (DSGVO Madde 19).

Veri sahibi, bu alıcıların **kimler olduğunu öğrenme hakkına** da sahiptir.

6.3 Silme Hakkı (“Unutulma Hakkı”) – DSGVO Madde 17

Yasal dayanak: DSGVO Madde 17

Veri sahibi, belirli durumlarda **kişisel verilerinin silinmesini** talep etme hakkına sahiptir. Bu hak, kamuoyunda sıkça "**unutulma hakkı**" olarak da anılmaktadır.

1. Ne zaman silme talep edilebilir?

Veri sahibi, aşağıdaki durumlarda verilerinin **derhal silinmesini** talep edebilir:

1. **Veri işleme amacı sona ermişse**
   – Örn. bir sözleşme sona ermiş ve saklama yükümlülüğü yoksa
2. **İlgili kişi rızasını geri çekmişse**
   – Ve veri işleme başka bir hukuki temele dayanmıyorsa
3. **Veri işleme hukuka aykırıysa**
4. **Veri sahibinin itiraz hakkını kullanması sonucunda**
   – Ve işleme için geçerli daha ağır bir meşru menfaat yoksa
5. **Silme yasal bir yükümlülükse**
   – Örn. belirli verilerin belirli süreden sonra silinmesi gerekiyorsa
6. **Çocuklara ait veriler, bilgi toplumu hizmetleri bağlamında işlenmişse**
   – Örn. sosyal medya profili

2. İstisnalar – Ne zaman silme hakkı yoktur?

DSGVO Madde 17 (3) uyarınca bazı durumlarda veri sorumlusu, silme talebine uymak zorunda değildir:

- **İfade özgürlüğü ve bilgi edinme hakkının kullanımı için** gerekiyorsa
- **Yasal bir zorunluluk** nedeniyle veri saklanıyorsa (örneğin muhasebe veya vergi kanunları gereği)
- **Kamu yararına dayalı arşivleme, bilimsel veya istatistiksel araştırma amaçlarıyla** saklanıyorsa ve silme, bu amaçları ciddi şekilde engelliyorsa
- **Yasal iddiaların ileri sürülmesi, kullanılması veya savunulması** için gerekiyorsa

3. Teknik olarak “unutulma” – arama motorları örneği

Unutulma hakkı, özellikle **arama motorlarında** görünürlüğün kaldırılması ile ilgilidir.

Avrupa Adalet Divanı'nın 2014 tarihli kararı uyarınca:

- Kişi, adının arama motorlarında belli içeriklerle ilişkilendirilmesini **kaldırttırabilir**
- Bu durum, özellikle içerik güncelliğini yitirmişse veya kişi açısından **orantısız bir zarara** yol açıyorsa geçerlidir

4. Üçüncü kişilere bildirimi

Veri sorumlusu, silinen verilerin daha önce açıklandığı **alıcıları** da bu durumdan **haberdar etmekle yükümlüdür** (DSGVO Madde 19).

Ayrıca veri sahibi, bu alıcıların kimler olduğunu **öğrenme hakkına** sahiptir.

6.4 İşlemenin Kısıtlanması Hakkı – DSGVO Madde 18

Yasal dayanak: DSGVO Madde 18

Veri sahibi, belirli koşullar altında kişisel verilerinin işlenmesinin **kısıtlanmasını** talep etme hakkına sahiptir. Bu durumda veriler **yalnızca saklanır**, başka hiçbir işleme tabi tutulamaz.

1. Hangi durumlarda kısıtlama talep edilebilir?

Veri sahibi, aşağıdaki durumlarda veri işleme faaliyetinin kısıtlanmasını talep edebilir:

1. **Verilerin doğruluğuna itiraz etmişse**
   – Doğruluk denetlenene kadar veri işleme kısıtlanır
2. **Veri işleme hukuka aykırıysa**
   – Silme yerine kısıtlama tercih ediliyorsa
3. **Veri sorumlusunun artık veriye ihtiyacı kalmamışsa**, ancak veri sahibi yasal iddialar için veriye ihtiyaç duyuyorsa
   – Örneğin: dava açma veya savunma amacıyla
4. **Veri sahibi, Madde 21 uyarınca işlemeye itiraz etmişse**
   – Bu durumda çıkar dengesi süresince işleme kısıtlanır

2. Kısıtlama ne anlama gelir?

Veri işleme şu şekillerde sınırlandırılır:

- Veriler **sadece saklanır**
- İşleme, yalnızca:
  - **İlgili kişinin rızasıyla**,
  - **Yasal iddiaların ileri sürülmesi veya savunulması amacıyla**,
  - **Diğer kişilerin haklarının korunması için**,
  - **Birlik veya üye devletin önemli kamu yararı** gerekçesiyle yapılabilir

Herhangi bir **aktif kullanım, analiz, aktarım veya silme işlemi yapılamaz.**

3. Kısıtlamanın kaldırılması

Kısıtlama kaldırılacaksa (örneğin doğruluk teyit edildiyse veya itiraz reddedildiyse), veri sahibi bu konuda **önceden bilgilendirilmelidir.**

4. Uygulama örnekleri

Durum	Kısıtlama süresi
Adres verisinin doğruluğu konusunda itiraz	Doğrulama tamamlanana kadar
Rıza geri çekilmiş, ancak dava devam ediyor	Dava sonuçlanana kadar
İtiraz edilmiş ve denge analizi bekleniyor	Analiz süresince

6.5 İtiraz Hakkı – DSGVO Madde 21

Yasal dayanak: DSGVO Madde 21

Veri sahibi, belirli koşullar altında kişisel verilerinin işlenmesine **itiraz etme hakkına** sahiptir. Bu hak, özellikle **meşru menfaate** (Madde 6 (1) f) veya **kamusal görev** (Madde 6 (1) e) gerekçesiyle yürütülen işlemler için geçerlidir.

1. Genel itiraz hakkı – Madde 21 (1)

Veri sahibi, **kendi özel durumu ile ilgili gerekçelerle**, aşağıdaki durumlarda veri işlenmesine **her zaman itiraz edebilir**:

- İşleme faaliyeti, **kamusal görev** kapsamında yürütülüyorsa (Madde 6 (1) e)
- İşleme faaliyeti, **veri sorumlusunun meşru menfaati** gerekçesine dayanıyorsa (Madde 6 (1) f)

Sonuç:
Veri sorumlusu, **zorunlu ve üstün meşru gerekçeler** ortaya koyamazsa, **veri işlemeyi durdurmak zorundadır.**

2. Doğrudan pazarlamaya itiraz – Madde 21 (2) ve (3)

Veri sahibi, kişisel verilerinin **doğrudan ticari iletişim (reklam, kampanya, analiz)** amacıyla işlenmesine **koşulsuz ve gerekçesiz olarak** her zaman **itiraz edebilir.**

Bu itiraz, profil oluşturma (profiling) faaliyetleri için de geçerlidir – eğer bu faaliyet doğrudan pazarlama ile bağlantılıysa.

Sonuç:
Veri sorumlusu, **derhal ve kalıcı olarak** işleme faaliyetini durdurmak zorundadır.

3. İtiraz hakkı nasıl uygulanır?

- İtiraz, **her zaman ve ücretsiz olarak** yapılabilir
- Yazılı, elektronik veya sözlü yapılabilir
- İlgili kişi, bu hakkı **veri toplama anında açıkça öğrenmiş olmalıdır**

DSGVO Madde 21 (4) uyarınca, veri sorumlusu itiraz hakkı konusunda:

- **Açık, anlaşılır ve ayrı bir şekilde** bilgilendirme yapmak zorundadır (örneğin gizlilik politikasında)

4. İtirazdan sonraki süreç

Veri sorumlusu:

- İtirazı derhal değerlendirmeli
- Veri işlemeyi durdurmalı (istisnai gerekçeler yoksa)
- Karar hakkında ilgili kişiye bilgi vermelidir

5. Uygulama örnekleri

Durum	İtiraz hakkı var mı?	Sonuç
Şirket, müşteri verilerini sadakat analizi için kullanıyor	Evet – meşru menfaat	Denge testi sonrası karar
Banka, kampanya e-postası gönderiyor	Evet – doğrudan pazarlama	Derhal durdurulmalı
Belediye, verileri kamu görevleri kapsamında kullanıyor	Evet – özel gerekçeyle itiraz edilebilir	Üstün kamu menfaati varsa işlem sürebilir

6.6 Veri Taşınabilirliği Hakkı – DSGVO Madde 20

Yasal dayanak: DSGVO Madde 20

Veri sahibi, kendisiyle ilgili olarak **veri sorumlusuna sağladığı kişisel verileri**, yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta alma ve bu verileri **başka bir veri sorumlusuna aktarma** hakkına sahiptir.

Bu hak, dijital dünyada **veri üzerindeki bireysel kontrolü güçlendirmek** için getirilmiştir.

1. Hakkın kapsamı nedir?

Veri sahibi aşağıdaki haklara sahiptir:

- Kendi verilerini, makine tarafından okunabilir biçimde alma
- Bu verileri başka bir veri sorumlusuna **teknik olarak mümkünse doğrudan aktarılmasını** talep etme

2. Hangi veriler kapsama girer?

Sadece:

- **Veri sahibinin kendisinin sağladığı** veriler
- İşleme şu hukuki dayanaklardan birine dayanıyorsa:
  - **Rıza (Madde 6 (1) a veya Madde 9 (2) a)**
  - **Sözleşme (Madde 6 (1) b)**
- Ve işleme **otomatik yollarla** yapılıyorsa

3. Hangi veriler dahil değildir?

Aşağıdakiler bu hak kapsamında değildir:

- **Veri sorumlusunun oluşturduğu türev veriler** (örneğin analizler, değerlendirmeler)
- **Veri sahibinin kendisinin sağlamadığı** veriler (örneğin kamu kaynaklı veriler, üçüncü kişi hakkındaki veriler)
- **Kağıt üzerinde tutulan veriler** (eğer otomatik değilse)

4. Teknik gereklilikler

Veriler şu şekilde sunulmalıdır:

- **Yapılandırılmış** (örneğin tablo biçiminde)
- **Yaygın kullanılan** (örneğin CSV, JSON, XML)
- **Makine tarafından okunabilir** formatta

Talep hâlinde, veri doğrudan diğer veri sorumlusuna da **aktarılabilir** – teknik olarak mümkünse.

5. Sınırlar ve istisnalar

Veri taşınabilirliği hakkı:

- Diğer kişilerin haklarını veya özgürlüklerini **olumsuz etkilememelidir**
- Şirketin ticari sırları veya fikri mülkiyet haklarını ihlal etmemelidir
- Kamu görevlerinin yerine getirilmesinde **geçerli değildir** (örneğin kamu kayıtları)

6. Uygulama örnekleri

Durum	Veri taşınabilirliği hakkı var mı?
Müşteri kendi banka işlem verilerini almak istiyor	Evet
Kişi, sosyal medya platformundaki fotoğraflarını başka bir platforma taşımak istiyor	Evet
Vergi dairesinden vergi bilgilerini başka bir kuruma aktarmak istiyor	Hayır – kamu kurumu ve kamu görevi kapsamında

6.7 Otomatik Kararlara ve Profil Oluşturmaya İtiraz – DSGVO Madde 22

Yasal dayanak: DSGVO Madde 22

Veri sahibi, **yalnızca otomatik işlemeye dayalı bir karara** tabi tutulmama hakkına sahiptir – özellikle bu karar, kişi üzerinde **hukuki sonuçlar doğuruyorsa** veya benzer şekilde **önemli bir etkisi** varsa.

1. Otomatik karar verme nedir?

Otomatik karar verme, bir kararın **tamamen bir algoritma veya yazılım tarafından** alınmasıdır; yani **insan müdahalesi olmaksızın**.

Örnekler:

- Online kredi başvurusunun sistem tarafından doğrudan reddedilmesi
- Sigorta priminin otomatik hesaplanması
- Otomatik işe alım elemeleri
- Davranışa dayalı fiyat teklifleri

2. Genel kural: yasaktır

Madde 22 (1) uyarınca, kişi:

"Kendisiyle ilgili hukuki sonuçlar doğuran veya benzer şekilde önemli etkiler yaratan, yalnızca otomatik işlemeye dayalı bir karara tabi tutulmama hakkına sahiptir."

3. İstisnalar – Ne zaman mümkündür?

Otomatik karar verme yalnızca aşağıdaki üç koşuldan biri karşılandığında hukuka uygundur:

1. **Kişiyle yapılan bir sözleşmenin kurulması veya ifası için gerekli ise** (Madde 22 (2) a)
   – Örneğin: hızlı kredi değerlendirmesi
2. **İlgili kişinin açık rızasına dayanıyorsa** (Madde 22 (2) c)
   – Ancak bu rıza her zaman geri çekilebilir
3. **AB veya üye devlet hukuku açıkça izin veriyorsa** (Madde 22 (2) b)
   – Örneğin: dolandırıcılık tespiti sistemleri

Bu durumlarda bile, veri sahibinin **ek hakları** vardır.

4. Veri sahibinin ek hakları (Madde 22 (3))

Veri sahibi, aşağıdaki haklara her durumda sahiptir:

- Kararın arkasında **bir insan müdahalesi** talep etme
- Kendi bakış açısını açıklama
- Karara **itiraz etme**

Bu haklar, adalet ve bireysel değerlendirme açısından önemlidir.

5. Profil oluşturma nedir?

Profil oluşturma (profiling), kişisel verilerin **otomatik olarak analiz edilmesiyle** bireyin:

- belirli yönlerinin değerlendirilmesi (örneğin performans, sağlık, tercih, davranış, konum)

Otomatik karar verme, çoğu zaman profil oluşturmaya dayanır.

6. Örnekler ve değerlendirme

Durum	Otomatik karar verme sayılır mı?	Hukuka uygun mu?
Online kredi başvurusu sistem tarafından reddediliyor	Evet	Ancak yalnızca sözleşme gerekçesi varsa geçerli
E-posta adresine göre reklam önerisi sunuluyor	Hayır – otomatik karar değil	Profil oluşturma olabilir
Sigorta priminin geçmiş hastalık verilerine göre belirlenmesi	Evet	Açık rıza varsa mümkün

7. Veri Güvenliği – Teknik ve Organizasyonel Önlemler (Madde 32 vd.)

7.1 Genel Yükümlülük – DSGVO Madde 32

Yasal dayanak: DSGVO Madde 32

DSGVO, veri sorumlularına ve veri işleyenlere, kişisel verilerin güvenliğini sağlamak üzere **uygun teknik ve organizasyonel önlemleri alma yükümlülüğü** getirir. Bu yükümlülük, **verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini** korumaya yöneliktir.

1. Güvenliğin üç temel ilkesi

1. **Gizlilik (Vertraulichkeit):** Verilere yalnızca yetkili kişilerin erişebilmesi
2. **Bütünlük (Integrität):** Verilerin kasıtlı veya kazara değiştirilmesini veya bozulmasını önlemek
3. **Erişilebilirlik (Verfügbarkeit):** Yetkili kişilerin verilere zamanında erişebilmesi

2. Uygunluk değerlendirmesi – "uygun" ne demektir?

DSGVO Madde 32'ye göre alınacak önlemler, özellikle aşağıdaki unsurlar dikkate alınarak **"uygun" olmalıdır**:

- **Teknik düzey** (güncel teknoloji)
- **Uygulama maliyetleri**
- İşlemenin **niteliği, kapsamı, bağlamı ve amaçları**
- Veri işleme faaliyetinin birey hakları açısından oluşturduğu **risk derecesi**

Yani: Güvenlik önlemleri orantılı olmalı – ne çok az ne de gereksiz derecede fazla.

3. Örnek teknik ve organizasyonel önlemler

- **Şifreleme (Encryption)**
- **Pseudonimleştirme**
- **Erişim kontrol sistemleri**
- **Veri yedekleme** ve **acil durum planları**
- **Güvenlik duvarları**, **antivirüs yazılımları**
- **Çalışan eğitimi**
- **Veri işleme politikaları**
- **Güvenli iletişim yolları** (örn. HTTPS, VPN)

4. Veri işleyenin sorumluluğu

Veri sorumlusu, birlikte çalıştığı **veri işleyenlerin** (örneğin bulut sağlayıcıları, yazılım firmaları) da bu güvenlik önlemlerine **uyduğundan emin olmakla** yükümlüdür (Madde 28).

5. Sürekli değerlendirme ve güncelleme

Güvenlik önlemleri bir kez alındıktan sonra **sabit kalmamalıdır** – düzenli olarak:

- Gözden geçirilmeli
- Güncellenmeli
- Yeni tehdit ve risklere göre **uyarlanmalıdır**

7.2 Özel Teknik Güvenlik Önlemleri ve Örnekler

Yasal dayanak: DSGVO Madde 32 (1) bent a–d

DSGVO Madde 32 (1)'de, veri güvenliğini sağlamak üzere alınabilecek özel teknik ve organizasyonel önlemlere örnekler verilmiştir. Aşağıda bunların açıklamaları ve uygulamadaki anlamları yer almaktadır.

1. Pseudonimleştirme ve şifreleme (Madde 32 (1) a)

- **Pseudonimleştirme:** Kişisel verilerin kimliği doğrudan belirlemeyecek şekilde işlenmesi (örneğin kodlarla)
- **Şifreleme (encryption):** Verilerin yalnızca yetkili kişiler tarafından okunabilir hâle getirilmesi

Örnekler:

- E-posta içeriklerinin TLS veya PGP ile şifrelenmesi
- Sağlık verilerinin ayrı şifreli veri tabanlarında tutulması

2. Sürekli gizlilik, bütünlük, erişilebilirlik ve dayanıklılığın sağlanması (Madde 32 (1) b)

Sistem ve hizmetlerin, sürekli olarak:

- **Yetkisiz erişime karşı korumalı olması**
- **Verilerin bozulmasını veya kaybolmasını önlemesi**

- **Yetkili kişiler tarafından erişilebilir olması**
- **Yüksek yük veya saldırı altında bile çalışmaya devam etmesi** gerekir

Örnekler:

- Sunucu sistemlerinde RAID teknolojisi
- Otomatik yedekleme çözümleri
- DDoS koruma sistemleri
- Yük dengeleme altyapısı

3. Olay durumunda veriye zamanında erişim (Madde 32 (1) c)

Örneğin bir sistem çökmesi, siber saldırı veya doğal afet durumunda:

- Verilerin hızlı şekilde **geri yüklenmesi**
- Sistemin yeniden devreye alınması gerekir

Örnekler:

- Acil durum planları
- Yedek veri merkezleri
- Günlük yedekleme süreçleri
- Felaket kurtarma tatbikatları

4. Güvenliğin düzenli test edilmesi, değerlendirilmesi ve denetlenmesi (Madde 32 (1) d)

Veri güvenliği önlemleri:

- **Periyodik olarak test edilmeli**
- **Etkililiği kontrol edilmeli**
- **İç ve dış denetimlere tabi tutulmalıdır**

Örnekler:

- Penetrasyon testleri
- Log (kayıt) analizleri
- Bilgi güvenliği iç denetimleri
- ISO 27001 gibi standartlara uygunluk kontrolleri

5. Risk odaklı yaklaşım

Tüm teknik ve organizasyonel önlemler, veri işleme faaliyetinden doğabilecek **risk seviyesine uygun olarak** seçilmelidir.

Örnek yaklaşım:

Risk düzeyi	Uygun önlemler
Düşük (örneğin haber bülteni aboneliği)	Basit şifreleme, temel erişim kontrolü
Orta (örneğin çalışan verileri)	Şifreli sunucular, iki faktörlü kimlik doğrulama
Yüksek (örneğin sağlık verileri, finansal bilgiler)	Gelişmiş şifreleme, segmentasyon, kapsamlı acil durum planları

7.3 Veri İhlali Bildirim Yükümlülüğü – DSGVO Madde 33 ve 34

Yasal dayanaklar: DSGVO Madde 33 ve 34

Veri güvenliği her zaman tamamen sağlanamayabilir. Kimi zaman kişisel veriler kazara ya da yetkisiz bir şekilde ifşa olabilir, kaybolabilir veya silinebilir. Bu gibi durumlara **veri ihlali** (Verletzung des Schutzes personenbezogener Daten) denir. DSGVO, bu tür ihlallerin hem **denetim makamına** hem de **ilgili kişilere** bildirilmesini şart koşar.

1. Veri ihlali nedir?

DSGVO Madde 4 No. 12'ye göre veri ihlali şunları kapsar:

- Yetkisiz erişim (örneğin hacklenme)
- Kazara veya kasıtlı silme, kayıp, değişiklik
- Yetkisiz açıklama veya iletim
- Fiziksel veri taşıyıcıların çalınması

2. Denetim makamına bildirim (Madde 33)

Veri sorumlusu, kişisel verilerin korunmasına yönelik bir ihlali:

- **Farkına vardığı andan itibaren 72 saat içinde**
- **Yetkili veri koruma denetim makamına** bildirmekle yükümlüdür

Bildirim şunları içermelidir:

- İhlalin niteliği (veri türleri, etkilenen kişi sayısı)
- Veri koruma görevlisinin iletişim bilgileri
- Olası sonuçlar
- Alınan veya planlanan önlemler

Not: 72 saatlik süre, ihlal tespit edildiği andan itibaren başlar – henüz araştırma tamamlanmamış olsa bile **ön bildirim** yapılmalıdır.

3. İlgili kişiye bildirim (Madde 34)

Veri ihlali, veri sahiplerinin hakları açısından **yüksek risk** doğuruyorsa, veri sorumlusu bu durumu:

- **Gereksiz gecikme olmaksızın**
- **Veri sahibine açık ve anlaşılır şekilde** bildirmek zorundadır

Bildirim içeriği:

- Ne tür veriler etkilendi
- Olası sonuçlar
- Alınan veya planlanan önlemler
- İrtibat kişisi bilgileri

Ancak şu durumlarda bildirim gerekmez:

- Veriler etkili biçimde şifrelenmişse veya pseudonimleştirilmişse
- Risk, artık geçerli değilse
- Bireysel bilgilendirme orantısız çaba gerektiriyorsa ve yerine kamuya açık bir bildirim yapılabiliyorsa

4. Veri işleyenin yükümlülüğü

Veri ihlali, **veri işleyen** (örneğin dış bir hizmet sağlayıcı) tarafından fark edilirse, bu durumu derhal **veri sorumlusuna bildirmekle** yükümlüdür (Madde 33 (2)).

Veri işleyenin kendisinin doğrudan denetim makamına bildirme yükümlülüğü yoktur – bu sorumluluk **veri sorumlusuna aittir.**

5. Örnek uygulamalar

Durum	Bildirim zorunlu mu?
Müşteri listesi yanlış kişiye e-posta ile gönderildi	Evet, yüksek risk varsa
Şifrelenmiş USB bellek kayboldu	Hayır, şifreleme etkiliyse
Web sitesindeki güvenlik açığı üzerinden veri çalındı	Evet, hem denetim makamına hem ilgili kişilere

8. Denetim Makamları ve Yaptırımlar – DSGVO Madde 51 vd.

8.1 Denetim Makamlarının Yetki ve Görevleri – DSGVO Madde 51–59

Yasal dayanaklar: DSGVO Madde 51–59

Avrupa Veri Koruma Tüzüğü (DSGVO), her üye devlette **bağımsız bir veri koruma denetim makamının** oluşturulmasını zorunlu kılar. Almanya'da bu görev, federal düzeyde **Federal Veri Koruma ve Bilgi Özgürlüğü Görevlisi (BfDI)** ile 16 eyaletin her birindeki **eyalet veri koruma görevlileri** tarafından yerine getirilir.

1. Temel ilke: Bağımsızlık

DSGVO Madde 52 uyarınca, denetim makamları:

- **Tam bağımsız** çalışmalıdır
- Hiçbir makamdan **talimat alamazlar**
- Görevlerini kendi takdirleriyle yerine getirirler
- **Personel ve teknik donanım bakımından yeterli kaynaklara** sahip olmalıdırlar

2. Görevleri (Madde 57)

Denetim makamlarının başlıca görevleri şunlardır:

- Veri koruma kurallarının **uygulanmasını izlemek ve denetlemek**
- **Şikâyetleri değerlendirmek ve yanıtlamak**
- Veri sorumluları ve veri işleyenlere **danışmanlık yapmak**
- Toplumun veri koruma bilincini artırmak
- **Yasama organlarına görüş bildirmek**
- **Veri ihlallerini araştırmak**
- Gerekirse **yaptırım uygulamak**

3. Yetkileri (Madde 58)

Denetim makamları, görevlerini yerine getirirken **geniş yetkilere sahiptir**:

Araştırma yetkileri:

- Veri işleme faaliyetleri hakkında bilgi talep etme
- Denetim yapma (önceden haberli veya habersiz)
- Erişim sağlama (örneğin veri merkezlerine)

Düzeltici yetkiler:

- Uyarı ve ihtarda bulunma
- Veri işleme faaliyetlerini geçici veya kalıcı olarak durdurma
- Verilerin silinmesini emretme
- **Para cezası uygulama** (Madde 83)

Onaylayıcı yetkiler:

- Sertifikasyon sistemlerini onaylama
- Veri koruma etki değerlendirmelerine ilişkin görüş bildirme
- Davranış kurallarını onaylama

4. İşbirliği ve tutarlılık (Madde 60–63)

Avrupa düzeyinde tutarlı bir uygulama sağlanması için denetim makamları:

- Birbiriyle **işbirliği içinde çalışır**
- Sınır ötesi işlemlerde birlikte hareket eder

- Uyuşmazlık durumlarında, **Avrupa Veri Koruma Kurulu (EDPB)** devreye girer

8.2 Yaptırımlar ve Para Cezaları – DSGVO Madde 83–84

Yasal dayanaklar: DSGVO Madde 83 ve 84

DSGVO, veri koruma kurallarına uyulmaması hâlinde **ağır yaptırımlar** öngörür. Bu yaptırımlar, **önleyici**, **cezalandırıcı** ve **caydırıcı** etki yaratmayı amaçlar. En bilinen yaptırım türü ise **idari para cezalarıdır**.

1. Para cezalarının amacı

- Veri koruma kurallarına uyumu **teşvik etmek**
- İhlallerin tekrarını **önlemek**
- Avrupa genelinde **uyumlu ve adil** uygulamayı sağlamak

2. Cezaların miktarı – Madde 83 (4) ve (5)

DSGVO iki düzeyde idari para cezası öngörür:

Alt düzey ihlaller (Madde 83 (4)):

En fazla:
10 milyon avro veya şirketin bir önceki yılki global cirosunun %2'si (hangisi yüksekse)

Örnek ihlaller:

- Veri sorumlusunun yükümlülüklerine uymaması
- Veri işleyici ile sözleşme yapılmaması
- Denetim makamlarının işini zorlaştırma
- Veri koruma görevlisi atamama (gerekliyse)

Üst düzey ihlaller (Madde 83 (5)):

En fazla:
20 milyon avro veya şirketin bir önceki yılki global cirosunun %4'ü (hangisi yüksekse)

Örnek ihlaller:

- Hukuka aykırı veri işleme
- Rızasız veri kullanımı
- Veri sahibinin haklarının ihlali
- Yetersiz güvenlik önlemleri
- Bilgilendirme yükümlülüğünün yerine getirilmemesi

3. Cezaların belirlenmesinde dikkate alınan kriterler – Madde 83 (2)

Ceza miktarı belirlenirken aşağıdaki hususlar dikkate alınır:

- İhlalin niteliği, süresi ve tekrarlanma durumu

- Kasıtlı mı yoksa ihmal sonucu mu olduğu
- Etkilenen kişilerin sayısı
- İşbirliği yapılıp yapılmadığı
- Alınan önlemler ve iyileştirici adımlar
- Önceden benzer bir ihlal olup olmadığı
- Veri kategorilerinin hassasiyeti
- Sertifikasyon bulunup bulunmadığı
- İhlalin bildirilip bildirilmediği

4. Diğer yaptırımlar – Madde 84

DSGVO, üye devletlere ayrıca **ceza hukuku kapsamında yaptırımlar** öngörme yetkisi verir.

Örneğin Almanya'da:

- BDSG kapsamında belirli ihlaller **suç** veya **kabahat** olarak değerlendirilebilir
- Örnek: gizli verilerin yetkisiz kişilere açıklanması

5. Uygulama örnekleri

İhlal türü	Ceza miktarı
Rıza alınmadan reklam e-postası gönderilmesi	5.000 € – 50.000 €
Güvenlik ihlali sonrası bildirim yapılmaması	20.000 € – 100.000 €
Sağlık verilerinin izinsiz ifşası	1.000.000 €'ya kadar
Veri koruma görevlisi atamamak	10.000 € – 50.000 €

9. Özel Konular – Örnek Durumlar ve Sektörel Uygulamalar

9.1 İşyeri Ortamında Veri Koruma

Yasal dayanaklar: DSGVO Madde 88, BDSG § 26

Çalışanlara ait kişisel veriler de **DSGVO ve BDSG** kapsamında korunur. Almanya'da bu alandaki özel düzenleme **BDSG § 26** maddesinde yer alır. İşyeri ortamındaki veri koruması, hem çalışanların haklarını hem de işverenin yasal yükümlülüklerini kapsamaktadır.

1. Ne tür veriler işlenebilir?

Yalnızca şu durumlarda çalışan verileri işlenebilir:

- **İş ilişkisinin kurulması**, yürütülmesi veya sonlandırılması için **gerekliyse**
- Örneğin:
    - İş başvuru belgeleri
    - Bordro verileri
    - Vardiya planları
    - Performans değerlendirmeleri

Bu verilerin işlenmesi, ancak **belirli, açık ve meşru amaçlarla** olmalı ve **gerekli olduğu ölçüyle** sınırlı tutulmalıdır.

2. Açık rıza ve hassas veriler

- İş ilişkilerinde rıza, ancak **gerçekten gönüllü** olduğu durumlarda geçerlidir
- **Baskı altındaki rızalar** (örneğin işten çıkarılma tehdidiyle verilen) geçerli sayılmaz
- Hassas veriler (örneğin sağlık bilgileri) yalnızca:
    - Açık rıza varsa
    - Yasal zorunluluk bulunuyorsa
    - Çalışma gücü tespiti gibi özel nedenlerle işlenebilir

3. Kamera, GPS ve benzeri izleme sistemleri

- Kamera gözetimi ancak iş güvenliği veya hırsızlık önleme gibi **haklı nedenlerle** yapılabilir
- Sürekli izleme, **orantısız** kabul edilir
- Çalışanlar açıkça **önceden bilgilendirilmelidir**
- GPS takibi sadece:
    - Araç güvenliği
    - Rota planlaması gibi amaçlarla
    - Gereklilik ve şeffaflık ilkelerine uygun olarak yapılabilir

4. E-posta ve internet kullanımı

- Kişisel kullanım tamamen yasaklanıyorsa, işveren **içerik denetimi yapabilir**
- Kısmi veya tam izin verilmişse, denetim **ancak belirli şartlarla ve orantılı biçimde** mümkündür
- İşveren, kullanım kurallarını açıkça belirlemeli ve çalışanları bilgilendirmelidir

5. İşyeri veri koruma görevlisi

- 20 veya daha fazla çalışan **sürekli olarak** kişisel veri işliyorsa → veri koruma görevlisi atanmalıdır
- Bu kişi çalışanların haklarını gözetmek ve işverenin yükümlülüklerini yerine getirmesine yardımcı olmakla görevlidir

9.2 Sağlık Sektöründe Veri Koruma

Yasal dayanaklar: DSGVO Madde 9, 32, 33; BDSG § 22

Sağlık sektörü, kişisel verilerin işlenmesi bakımından **en hassas alanlardan biridir**. Burada genellikle **sağlık verileri** işlendiğinden, veri koruma gerekleri çok daha sıkıdır. DSGVO Madde 9 bu verileri **özel nitelikli kişisel veriler** olarak tanımlar.

1. Kimler sağlık verisi işler?

- Hekimler ve muayenehaneler
- Hastaneler
- Eczaneler

- Psikologlar, fizyoterapistler
- Laboratuvarlar
- Sağlık sigortaları
- Sağlık uygulamaları / dijital hizmet sağlayıcıları

Bu kurum ve kişiler, verileri işlerken **mesleki gizlilik yükümlülüğü** altındadırlar.

2. İşleme ne zaman hukuka uygundur?

Sağlık verileri ancak şu durumlarda işlenebilir:

- **Tıbbi tanı, tedavi veya bakım amacıyla**,
- **Yasal bir yükümlülük gereği** (örneğin bulaşıcı hastalık bildirimi),
- **Hayati çıkarların korunması için**,
- **Kamu sağlığı gerekçesiyle**,
- **İlgili kişinin açık rızası** varsa

Ek olarak: İşleme, yalnızca **gizlilik yükümlülüğü olan profesyonellerce** veya onların gözetiminde yapılmalıdır.

3. Teknik ve organizasyonel önlemler

Veri güvenliğini sağlamak için aşağıdaki önlemler alınmalıdır:

- Erişim kontrolü (sadece yetkili personel)
- Dosya ve cihazların şifrelenmesi
- Günlük yedekleme sistemleri
- Hasta dosyalarının kilit altında tutulması
- Muayenehane yazılımında oturum açma/kapama sistemleri
- Personelin düzenli veri koruma eğitimi

4. Hasta bilgilendirmesi ve rıza

Hastalar, verilerinin işlenmesi hakkında:

- **Açık, sade ve anlaşılır bir şekilde** bilgilendirilmelidir
- Gerekirse **yazılı rıza** alınmalıdır
- Rıza her zaman **geri çekilebilir**
- Rıza verilmediğinde alternatif yasal dayanaklar varsa bu kullanılabilir (örneğin tedavi için zorunluluk)

5. İhlal durumunda yükümlülükler

Sağlık verilerine ilişkin bir güvenlik ihlali (örneğin veri sızıntısı, yanlış kişiye gönderim):

- **Denetim makamına** 72 saat içinde bildirilmeli
- Eğer yüksek risk varsa, **hasta da bilgilendirilmelidir**
- Güvenlik ihlali belgelenmeli ve süreç kayıt altına alınmalıdır

9.3 Eğitim, İnanç ve Sivil Toplum Kurumlarında Veri Koruma

Yasal dayanaklar: DSGVO Madde 9, 91; BDSG § 22

Okullar, üniversiteler, dini topluluklar ve dernekler gibi kurumlar, çeşitli nedenlerle çok sayıda kişisel veri işler. Bu verilerin bir kısmı **özel nitelikli** olabilir (örneğin inanç, sağlık, çocuk bilgileri), bu nedenle veri koruma açısından dikkatli hareket edilmesi gerekir.

1. Eğitim kurumlarında veri koruma

İşlenen veriler:

- Öğrenci kayıt bilgileri
- Notlar ve performans belgeleri
- Sağlık bilgileri (örneğin alerjiler, özel ihtiyaçlar)
- Veli iletişim bilgileri
- Görüntü ve ses kayıtları (örneğin okul etkinliklerinde)

Önemli ilkeler:

- Öğrenciler ve veliler bilgilendirilmelidir
- Veri minimizasyonu uygulanmalı
- Sınıf listeleri, fotoğraflar gibi bilgiler sadece **gerekliyse ve izin alınmışsa** paylaşılmalı
- Dijital platformlarda (örneğin çevrim içi ders sistemleri) veri güvenliği sağlanmalı

2. Dini topluluklar ve inanç temelli kuruluşlar

DSGVO Madde 91, dini topluluklara **kendi veri koruma kurallarını belirleme** hakkı tanır – ancak bu kurallar **DSGVO'ya denk koruma sağlamalıdır.**

Örnek kurumlar:

- Kiliseler
- Cemaatler
- İslami vakıflar
- Yahudi toplulukları

Veri konuları:

- Üyelik bilgileri
- İbadet katılımı
- Dini inanç beyanı
- Bağış ve ödeme kayıtları

İlke: Dini inanç verileri, DSGVO Madde 9 kapsamında özel korumaya tabidir → işleme ancak **rıza** veya açık yasal dayanakla mümkündür.

3. Sivil toplum kuruluşları ve dernekler

Örnek veriler:

- Üye kayıtları
- Gönüllülerin iletişim bilgileri
- Etkinlik kayıtları (fotoğraf/video)
- Bağışçı listeleri

Veri koruma uygulamaları:

- Üyeler bilgilendirilmeli (örneğin gizlilik politikası ile)
- Duyurular, yalnızca **açık rıza alınan kişilere** gönderilmeli
- Görüntülerin yayımlanması için önceden izin alınmalı
- Gönüllülerin verileri yalnızca görevle ilgili olarak işlenmeli

4. Özet: Sektörel dikkat noktaları

Kurum türü	Özel dikkat edilmesi gereken konular
Okul	Çocuk verileri, veli onayı, sınırlı paylaşım
Dini kurum	İnanç verileri, rıza ve iç düzenlemeler
Dernek	Üyelik ve iletişim verilerinin sınırlı kullanımı