HUKUKİ UYUM REHBERİ

KVKK UYUM REHBERİ

Ruh Sağlığı Hizmetlerinde Kişisel Verilerin Korunması

Bu rehber; psikiyatristler, klinik psikologlar, psikolojik danışmanlar ve ruh sağlığı merkezleri için 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamındaki hukuki yükümlülükleri, uyum süreçlerini ve pratik araçları kapsamlı biçimde ele almaktadır.

Av. Yavuz Fırat — Ankara Barosu · Sicil No: 38499 · yavuzfirat.com

1. Baskı · Mayıs 2026

Bu Rehberde Neler Bulacaksınız?

Bu rehber, ruh sağlığı alanında çalışan meslek mensuplarının KVKK kapsamındaki yükümlülüklerini pratik ve uygulanabilir bir çerçevede ele almaktadır. Her bölüm, gerçek hukuki senaryolar ve örnek uygulamalar içermektedir.

01

Bölüm I: Temel Kavramlar ve Hukuki Çerçeve

KVKK'nın temel ilkeleri, tanımlar ve ruh sağlığı hizmetlerine özgü hukuki zemin

02

Bölüm II: Meslek Gruplarının Hukuki Konumu

Psikiyatrist, psikolog ve danışmanların veri sorumlusu/işleyeni sıfatları

03

Bölüm III: Kişisel Verilerin İşlenme Şartları

Açık rıza, hukuki yükümlülük ve meşru menfaat koşulları

04

Bölüm IV: Danışan Dosyaları ve Kayıt Yönetimi

Seans notları, ses/video kayıtları ve saklama süreleri

05

Bölüm V: Yapay Zekâ ve Dijital Araçlar

Çevrim içi terapi, yapay zekâ uygulamaları ve veri güvenliği

06

Bölüm VI: Çocuk Danışanlar ve Hassas Gruplar

Velayet uyuşmazlıkları, ergen gizliliği ve özel durumlar

07

Bölüm VII: Veri İhlalleri ve Hukuki Sonuçları

Bildirim yükümlülükleri, idari para cezaları ve tazminat

08

Sonuç ve Ekler

Kontrol listeleri, aydınlatma metni şablonları ve pratik araçlar

Bölüm I – Temel Kavramlar ve Hukuki Çerçeve

1. Kişisel Verilerin Korunması Hakkının Önemi

Dijitalleşmenin hız kazanmasıyla birlikte sağlık verileri, kişisel veri kategorileri içinde en yüksek risk grubunu oluşturan bilgiler hâline gelmiştir. Özellikle ruh sağlığı hizmetlerinde işlenen tanı bilgileri, ilaç kullanımı, seans içerikleri, psikometrik test sonuçları, intihar riski değerlendirmeleri, travma öyküleri ve aile içi çatışmalara ilişkin kayıtlar; yanlış kişi, kurum veya platformların eline geçtiğinde bireyin yalnızca mahremiyetini değil, iş hayatını, aile ilişkilerini, sosyal çevresini ve hatta güvenlik algısını da kalıcı biçimde zedeleyebilir.

Bu nedenle KVKK, sağlık verilerini **özel nitelikli kişisel veri** olarak ayrı ve daha sıkı bir koruma rejimine tabi tutar. Ruh sağlığı alanında veri güvenliği, yalnızca teknik bir uyum meselesi değil; danışanın hekime, psikoloğa veya danışmana duyduğu güvenin ve tedavi ilişkisinin sürdürülebilirliğinin temel şartıdır.

> KVKK, sağlık verilerini özel nitelikli kişisel veri olarak ayrı ve daha sıkı bir koruma rejimine tabi tutar.

---

2. Temel Tanımlar

Aşağıdaki tanımlar, ruh sağlığı uygulamalarında KVKK değerlendirmesinin başlangıç noktasını oluşturur:

Kişisel Veri

Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir. Ruh sağlığı pratiğinde ad, T.C. kimlik numarası, telefon, e-posta, IP adresi, seans tarihleri ve randevu kayıtları bu kapsama girer.

Özel Nitelikli Kişisel Veri

Irk, etnik köken, siyasi düşünce, din, sağlık ve cinsel hayata ilişkin verileri kapsar. Ruh sağlığı tanıları, ilaç bilgileri, terapi notları ve seans içerikleri bu kapsamda değerlendirilir.

Veri Sorumlusu

Verilerin işleme amaç ve yöntemlerini belirleyen kişi veya kuruluştur. Muayenehane sahibi psikiyatrist, klinik direktörü veya merkezi veri yönetimini elinde tutan kuruluş bu sıfatı taşıyabilir.

Veri İşleyen

Veri sorumlusunun adına kişisel veri işleyen kişidir. Muhasebeci, yazılım şirketi, bulut hizmet sağlayıcısı ve süpervizyon platformu bu kategoriye girebilir.

İlgili Kişi

Kişisel verisi işlenen gerçek kişidir. Ruh sağlığı hizmetlerinde danışan veya hasta, ilgili kişi sıfatını taşır.

---

3. KVKK'nın Temel İlkeleri (Madde 4)

6698 sayılı Kanun'un 4. maddesi, kişisel veri işleme faaliyetlerinin dayandığı yedi temel ilkeyi düzenler. Ruh sağlığı hizmetlerinde bu ilkeler, terapötik ilişkinin gizliliği ile hukuka uygun veri yönetimi arasında denge kurar:

Hukuka ve dürüstlük kurallarına uygunluk:
Veri işleme süreci açık, öngörülebilir ve danışanı yanıltmayacak şekilde yürütülmelidir.

Doğru ve güncel olma:
Danışan bilgilerinin periyodik olarak güncellenmesi; yanlış adres, iletişim bilgisi veya acil durum irtibatı gibi hataların düzeltilmesi gerekir.

Belirli, açık ve meşru amaç:
Seans notları yalnızca tedavi, izlem ve mesleki kayıt amacıyla tutulmalı; sonradan farklı ve belirsiz amaçlarla kullanılmamalıdır.

İşlemeyle bağlantılı, sınırlı ve ölçülü olma:
Gereksiz veri toplanmamalı; örneğin terapi için zorunlu olmayan fazla ayrıntılar sistematik biçimde istenmemelidir.

Saklama süresiyle sınırlı olma:
Veriler, ilgili mevzuatta öngörülen süre kadar saklanmalı; amaç ortadan kalktığında silinmeli, yok edilmeli veya anonim hâle getirilmelidir. Uygulamada sağlık kayıtları bakımından 10 yıllık saklama yükümlülüğü sıkça gündeme gelir.

Gizlilik ve erişim kontrolü:
Kayıtlara yalnızca yetkili personel erişmeli; erişim logları, rol bazlı yetkilendirme ve parola güvenliği sağlanmalıdır.

Veri güvenliği tedbirleri:
Fiziksel dosya güvenliği, şifreleme, yedekleme, iki aşamalı doğrulama ve tedarikçi denetimi gibi teknik ve idari tedbirler alınmalıdır.

---

4. İlgili Mevzuat

Ruh sağlığı alanında kişisel verilerin korunmasına ilişkin hukuki değerlendirme, tek başına KVKK ile sınırlı değildir. Uygulama alanını belirleyen başlıca düzenlemeler şunlardır:

- **6698 sayılı Kişisel Verilerin Korunması Kanunu (2016):** Kişisel veri işleme şartlarını, veri sorumlusu yükümlülüklerini, özel nitelikli verilerin işlenme rejimini ve ilgili kişinin haklarını düzenler.
- **3359 sayılı Sağlık Hizmetleri Temel Kanunu:** Sağlık hizmetlerinin genel çerçevesini çizer; sağlık kurum ve kuruluşlarının kayıt ve hizmet sunumuna ilişkin temel dayanaklardan biridir.
- **Kişisel Sağlık Verileri Hakkında Yönetmelik (2019):** Sağlık verilerinin işlenmesi, saklanması, erişimi ve paylaşımına ilişkin usul ve esasları belirler.
- **Türk Tabipleri Birliği Etik Kuralları:** Hekim-hasta gizliliği, mesleki sır, özen yükümlülüğü ve mesleki bağımsızlık bakımından önemli etik çerçeve sunar.
- **Psikolojik Danışmanlık ve Rehberlik Kanunu Taslağı:** Mesleğin yasal statüsü, mesleki sınırlar ve veri gizliliği bakımından normatif beklentileri ortaya koyan taslak metin niteliğindedir.

> Bu mevzuat birlikte değerlendirildiğinde, ruh sağlığı hizmetlerinde veri işleme faaliyetinin yalnızca "rıza alınmış olması" ile meşrulaşmayacağı; hukuki dayanak, amaç sınırlılığı, güvenlik tedbirleri ve saklama süresi boyutlarının da ayrıca incelenmesi gerektiği görülür.

Bölüm II – Meslek Gruplarının Hukuki Konumu ve Veri İşleme Faaliyetleri

5. Genel Olarak

Ruh sağlığı alanında faaliyet gösteren meslek mensupları, mesleklerini icra ederken bireylere ait son derece hassas kişisel verileri işlemektedir. Bu verilerin büyük bölümü 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") kapsamında **özel nitelikli kişisel veri** sayılmakta olup, bu verilerin işlenmesi için Kanun'da öngörülen daha sıkı hukuki şartların ve ek güvenlik tedbirlerinin sağlanması gerekmektedir. Özellikle sağlık verileri, ruh sağlığı hizmetlerinde yalnızca teşhis ve tedavi süreci bakımından değil, bireyin sosyal çevresi, aile ilişkileri ve mesleki yaşamı üzerinde doğurabileceği etkiler nedeniyle de yüksek koruma ihtiyacı taşır.

Bu nedenle ruh sağlığı profesyonellerinin veri işleme faaliyetleri değerlendirilirken yalnızca mesleki unvanlarına bakılması yeterli değildir; mesleğin icra edildiği ortam, veri üzerindeki tasarruf yetkisi, amaç ve vasıta belirleme serbestisi ile kurumsal yapılanma birlikte incelenmelidir. Nitekim aynı veri, bağımsız çalışan bir uzman bakımından veri sorumluluğu doğurabilirken, bir hastane, okul ya da klinik bünyesinde çalışan uzman bakımından veri işleyen konumunu gündeme getirebilir.

> Aynı veri, bağımsız çalışan bir uzman bakımından veri sorumluluğu doğurabilirken, bir hastane, okul ya da klinik bünyesinde çalışan uzman bakımından veri işleyen konumunu gündeme getirebilir.

---

6. Psikiyatristlerin Hukuki Konumu

Psikiyatristler, tıp fakültesi mezunu ve ruh sağlığı ve hastalıkları alanında uzmanlık eğitimini tamamlamış hekimlerdir. Türk Tabipleri Birliği'ne kayıtlı hekimler olarak hem 3359 sayılı Sağlık Hizmetleri Temel Kanunu hem de KVKK kapsamında faaliyet göstermektedirler. Psikiyatristlerin sunduğu hizmet, sağlık hizmeti niteliğinde olduğundan; hasta kayıtlarının tutulması, tedavi planlarının oluşturulması, reçete düzenlenmesi, sevk ve yatış işlemlerinin yürütülmesi sırasında işlenen veriler sağlık mevzuatına uygun biçimde korunmalıdır.

Muayenehane sahibi bir psikiyatrist, veri işleme amaç ve vasıtalarını belirlediği ölçüde **veri sorumlusu** sıfatını taşır. Bu durumda, işleme faaliyetlerinin hukuki dayanağını belirlemek, ilgili kişileri aydınlatmak, gerekli açık rıza ve diğer işleme şartlarını değerlendirmek, veri güvenliğini sağlamak ve saklama-imha politikalarını uygulamak doğrudan kendisinin yükümlülüğündedir. Ayrıca muayenehanenin niteliğine ve çalışan sayısına göre **VERBİS** kaydı da gündeme gelebilir.

Buna karşılık bir hastane, klinik ya da tıp merkezi bünyesinde görev yapan psikiyatrist, çoğu durumda kurumsal veri sorumluluğu altında hareket eder. Bu durumda hekimin konumu, kurumun belirlediği amaç ve araçlar çerçevesinde veri işleyen niteliğine yaklaşabilir. İşlenen veriler arasında **DSM-5/ICD-11 tanıları**, ilaç reçeteleri, psikometrik test sonuçları, yatış kayıtları ve intihar riski değerlendirmeleri yer alır. Bu verilerin niteliği gereği erişim yetkileri sıkı biçimde sınırlandırılmalı, log kayıtları tutulmalı ve üçüncü kişilerle paylaşım ancak hukuki dayanak varsa gerçekleştirilmelidir.

---

7. Klinik Psikologların Hukuki Konumu

Klinik psikologlar, psikolojik değerlendirme, psikoterapi, test uygulamaları ve psikolojik destek hizmetleri yürüten uzmanlardır. Klinik psikologların hukuki statüsü, hizmeti bağımsız olarak mı yoksa bir kurum çatısı altında mı sunduklarına göre değişmektedir. Bağımsız muayenehane veya danışmanlık ofisi işleten klinik psikolog, veri işleme amaç ve yöntemlerini bizzat belirlediği için **veri sorumlusu** sayılacaktır. Buna karşılık hastane, rehabilitasyon merkezi, klinik veya benzeri bir kuruluş bünyesinde çalışan klinik psikolog, kurumun belirlediği veri işleme sistemi içinde hareket ettiği ölçüde **veri işleyen** konumunda değerlendirilebilir.

Önemli bir husus, klinik psikologların Türkiye'de hâlen bağımsız ve kapsamlı bir meslek kanununa sahip olmamasıdır. Bu durum, özellikle mesleki yetki sınırları, sır saklama yükümlülüğünün kapsamı, tanıklıktan çekinme hakkı ve bazı veri işleme faaliyetlerinin hukuki dayanağı bakımından uygulamada yorum farklılıklarına yol açabilmektedir. Bu nedenle klinik psikologların veri işleme faaliyetleri değerlendirilirken yalnızca KVKK değil, ilgili yönetmelikler, kurum içi düzenlemeler ve somut olayın özellikleri birlikte ele alınmalıdır.

İşlenen veriler arasında **psikolojik değerlendirme raporları**, WAIS/MMPI gibi psikometrik test sonuçları, seans notları ve danışanın aile öyküsüne ilişkin kayıtlar bulunmaktadır. Bu veriler, çoğu zaman doğrudan bireyin ruh sağlığına, bilişsel kapasitesine, kişilik yapısına ve yaşam öyküsüne ilişkin olduğundan, yüksek derecede gizlilik gerektirir.

---

8. Psikolojik Danışmanların Hukuki Konumu

Psikolojik danışmanlar (PDR mezunları), ağırlıklı olarak eğitim, rehberlik ve danışmanlık hizmetleri sunmaktadır. Psikolojik danışmanlar okul psikolojik danışmanı olarak Millî Eğitim Bakanlığı (MEB) bünyesinde görev yapıyorsa, veri işleme faaliyetleri bakımından kurumun veri işleme politikaları doğrultusunda hareket ederler ve çoğu durumda **veri işleyen** sıfatı ile değerlendirilirler. Buna karşılık özel danışmanlık ofisi, özel etüt merkezi, danışmanlık şirketi veya bağımsız rehberlik hizmeti yürütülmesi hâlinde veri işleme amaç ve araçları bizzat belirlendiğinden **veri sorumlusu** konumu doğar.

Okul ortamında işlenen öğrenci verileri yalnızca KVKK'ya değil, aynı zamanda **MEB mevzuatına**, rehberlik hizmetlerine ilişkin düzenlemelere ve kurum içi veri güvenliği politikalarına tabidir. Bu nedenle öğrenci gelişim dosyaları, aile görüşme notları ve davranış değerlendirmeleri gibi kayıtların hem hukuka uygunluk hem de ölçülülük ilkeleri çerçevesinde işlenmesi gerekir. Öğrencinin üstün yararı ile veri minimizasyonu arasında denge kurulmalı; gereksiz, aşırı veya amaçla ilgisiz veri toplanmamalıdır.

Psikolojik danışmanlık faaliyetlerinde sık karşılaşılan veri türleri arasında **öğrenci gelişim dosyaları**, aile görüşme notları, kariyer envanterleri ve davranış değerlendirme formları yer alır. Bu kayıtların özellikle ergenler ve çocuklar bakımından daha da hassas sonuçlar doğurabileceği gözetilmeli; erişim yalnızca yetkili kişilerle sınırlandırılmalıdır.

---

9. Ruh Sağlığı Merkezleri ve Kliniklerin Durumu

Birden fazla uzmanın çalıştığı ruh sağlığı merkezleri, klinikler ve çok disiplinli uygulama alanlarında veri sorumluluğu çoğunlukla kuruma aittir. Bu tür yapılarda veri işleme amaçlarını, saklama sürelerini, erişim yetkilerini ve teknik-idari tedbirleri belirleyen taraf kurum olduğundan, çalışan uzmanlar genellikle **veri işleyen** konumunda değerlendirilir. Ancak somut organizasyon yapısına göre ortak veri sorumluluğu ihtimali de ayrıca incelenmelidir.

Bu merkezlerde KVKK uyumu bakımından yalnızca bireysel mesleki sorumluluk yeterli değildir; kurumsal düzeyde yazılı politikaların oluşturulması zorunludur. Özellikle tüm çalışanlarla **veri işleme sözleşmesi (DPA)** imzalanması, iç veri politikalarının hazırlanması, erişim yetki matrisi oluşturulması, saklama-imha sürecinin belirlenmesi ve **VERBİS** kaydının tamamlanması gerekir. Ayrıca merkez içinde çalışanın görevine göre değişen rol bazlı erişim, gizlilik taahhüdü, yedekleme ve olay müdahale prosedürleri uygulanmalıdır.

---

10. VERBİS Kayıt Yükümlülüğü

6698 sayılı KVKK'nın 16. maddesi uyarınca kişisel veri işleyen gerçek ve tüzel kişi veri sorumlularının Veri Sorumluları Siciline (VERBİS) kayıt ve bildirim yükümlülüğünü yerine getirmeleri için belirlenen son tarih **31.12.2021** olarak uygulanmıştır. Bu tarihten sonra yükümlü hâline gelen veri sorumlularının ise Veri Sorumluları Sicili Hakkında Yönetmelik'in 8. maddesinin ikinci fıkrası uyarınca, yükümlülük altına girmelerini müteakip **30 gün içinde** Sicile kayıt ve bildirimlerini tamamlamaları gerekmektedir.

2025 Yılı Mali Bilanço Eşikleri ve Yeni Yükümlüler

Kişisel Verileri Koruma Kurulu'nun 04.09.2025 tarihli ve 2025/1572 sayılı Kararı ile değişik 2018/87 sayılı Kararı uyarınca VERBİS kaydı yükümlülüğünden muafiyet, çalışan sayısı ve mali bilanço toplamı kriterlerinin kümülatif olarak değerlendirilmesine bağlıdır. Her iki eşiğin birlikte aşılması hâlinde kayıt yükümlülüğü doğar; yalnızca birinin aşılması muafiyeti sona erdirmez. Eşik sonradan aşılırsa, yükümlülüğün doğduğu tarihten itibaren 30 gün içinde Sicile kayıt yapılmalıdır. Mali bilanço eşiğinin aşılması genellikle ilgili yıla ait kurumlar vergisi beyannamesinin verilmesi ve bilançonun kesinleşmesiyle gerçekleşir; 30 günlük süre bu tarihi izleyerek başlar.

Yükümlülük doğuran eşikler şu şekilde belirlenmiştir:

- **Ana faaliyet konusu özel nitelikli kişisel veri işleme olan tüzel kişi veri sorumluları (ruh sağlığı merkezleri, klinikler):** Muafiyet için yıllık çalışan sayısının 10'dan az VE yıllık mali bilanço toplamının 10 milyon TL'den az olması gerekir. Her iki eşiğin birlikte aşılması hâlinde VERBİS kaydı zorunlu hâle gelir.
- **Ana faaliyet konusu özel nitelikli kişisel veri işleme olmayan tüzel kişi veri sorumluları:** Muafiyet için yıllık çalışan sayısının 50'den az VE yıllık mali bilanço toplamının 100 milyon TL'den az olması gerekir. Her iki eşiğin birlikte aşılması hâlinde VERBİS kaydı zorunlu hâle gelir.
- **Bilanço esasına göre defter tutan veri sorumlularında** her iki kriter (çalışan sayısı ve mali bilanço) kümülatif olarak değerlendirilir. Buna karşılık işletme hesabı veya serbest meslek defteri tutan veri sorumlularında mali bilanço bilgisi bulunmadığından yalnızca çalışan sayısı kriteri esas alınır.

Ruh Sağlığı Hizmetleri Açısından Değerlendirme

Ruh sağlığı merkezleri ve klinikler, ana faaliyet konusu itibarıyla özel nitelikli kişisel veri (sağlık verisi) işleyen kuruluşlar olarak değerlendirilmektedir. Bu nedenle söz konusu kuruluşlar için çalışan sayısı ve 10 milyon TL mali bilanço eşikleri kümülatif biçimde uygulanır; her iki eşiğin birlikte aşılması hâlinde VERBİS kaydı zorunlu hâle gelir. Bireysel muayenehane sahibi psikiyatrist veya klinik psikologlar ise çoğunlukla bu eşiklerin altında kalmaktadır. Ancak bu durum, KVKK'nın diğer yükümlülüklerini (aydınlatma, güvenlik tedbirleri, ilgili kişi hakları, saklama ve imha) ortadan kaldırmaz. VERBİS kaydı zorunlu olmasa dahi temel uyum yükümlülükleri eksiksiz yerine getirilmelidir.

Veri Sorumlusu Türü	Kümülatif Eşik	VERBİS Kayıt Yükümlülüğü
Ana faaliyet konusu özel nitelikli veri işleme olan tüzel kişi (ruh sağlığı merkezi, klinik)	Çalışan sayısı 10+ VE mali bilanço 10 milyon TL+	Her iki eşiğin birlikte aşılması hâlinde evet; yükümlülüğün doğmasını izleyen 30 gün içinde
Ana faaliyet konusu özel nitelikli veri işleme olmayan tüzel kişi	Çalışan sayısı 50+ VE mali bilanço 100 milyon TL+	Her iki eşiğin birlikte aşılması hâlinde evet; yükümlülüğün doğmasını izleyen 30 gün içinde
Bireysel muayenehane (gerçek kişi veri sorumlusu)	Kurul kararıyla belirlenen eşikler	Eşik aşılırsa evet; aksi hâlde diğer yükümlülükler geçerli

Bölüm III – Kişisel Verilerin İşlenme Şartları

11. Genel Olarak

6698 sayılı Kişisel Verilerin Korunması Kanunu (“KVKK”), kişisel verilerin işlenmesini kural olarak ilgili kişinin iradesine bağlı bir faaliyet olarak kabul etmektedir. Bununla birlikte Kanun, kişisel verilerin açık rıza olmaksızın da işlenebileceği sınırlı sayıda hukuki dayanak öngörmektedir. Ruh sağlığı hizmetlerinde hangi hukuki dayanağın uygulanacağı, somut veri işleme faaliyetinin niteliğine, amacına ve tarafların konumuna göre belirlenir.

---

12. Açık Rıza (Madde 5/1 ve 6/2)

Açık rıza; belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan onay beyanıdır. Ruh sağlığı pratiğinde açık rıza alınırken aşağıdaki hususlara dikkat edilmelidir:

- Rıza, hizmet sunumunun ön koşulu olarak dayatılamaz; koşullu rıza yasağına aykırı davranılamaz.
- Rıza, mutlaka aydınlatma yükümlülüğü yerine getirildikten sonra alınmalıdır.
- Sözlü rıza ispat güçlüğü yaratır; bu nedenle yazılı veya elektronik rıza tercih edilmelidir.
- Danışan rızasını her zaman geri alabilir; geri alma, önceki işlemlerin hukuka aykırılığını doğurmaz.
- Seans kaydı alınacaksa ses veya video kaydı için ayrı ve açık bir rıza alınmalıdır.

Bu kapsamda açık rıza, genel ve soyut bir onay şeklinde değil; işlenecek veri kategorisi, amaç, aktarım yapılan kişiler ve saklama süresi bakımından somutlaştırılmış olmalıdır.

---

13. Hukuki Yükümlülük (Madde 5/2-a)

Veri işlemenin kanunlarda açıkça öngörülmesi hâlinde açık rızaya gerek yoktur. Bu hukuki sebep, ruh sağlığı alanında özellikle kamusal yükümlülüklerin yerine getirilmesi bakımından önem taşır. Örneğin:

- Adli makamların talebi üzerine tanı ve tedavi bilgilerinin paylaşılması.
- Zorunlu bildirim yükümlülükleri kapsamında bulaşıcı hastalık bildirimi yapılması.
- Çocuk istismarı şüphesinin yetkili mercilere bildirilmesi.
- Sigorta şirketlerine veya SGK süreçlerine ilişkin fatura ve işlem bilgilerinin iletilmesi.

Bu tür durumlarda veri sorumlusu, işlemenin kanuni dayanağını ayrıca değerlendirmeli; talebin kapsamını aşan veri paylaşımından kaçınmalı ve sadece zorunlu olan bilgilerle yetinmelidir.

---

14. Sözleşmenin Kurulması veya İfası (Madde 5/2-c)

Danışanla kurulan terapi sözleşmesinin kurulması veya ifası için zorunlu olan veriler bu kapsamda işlenebilir. Örneğin randevu bilgileri, ödeme kayıtları, faturalama bilgileri ve iletişim bilgileri bu hukuki dayanağa dayandırılabilir. Ancak bu dayanak sınırsız değildir; sözleşmenin ifası için zorunlu olmayan veriler için ayrıca başka bir hukuki sebep bulunmalıdır.

Özellikle seans içeriği ve tanı bilgileri bakımından sözleşmenin ifası dayanağı çoğu durumda yeterli görülmez. Bu veriler, niteliği itibarıyla sağlık verisi olduğundan, ayrıca KVKK’nın 6. maddesi çerçevesinde değerlendirilmelidir. Dolayısıyla veri sorumlusu, hangi verinin sözleşmenin ifası için gerçekten zorunlu olduğunu ayrı ayrı tespit etmelidir.

---

15. Meşru Menfaat (Madde 5/2-f)

Veri sorumlusunun meşru menfaati, ilgili kişinin temel hak ve özgürlüklerine zarar vermemesi koşuluyla kişisel verilerin işlenmesine imkân tanıyabilir. Ancak ruh sağlığı pratiğinde bu hukuki dayanak dikkatli kullanılmalıdır. Çünkü danışanlara ait veriler çoğu zaman hassas nitelikte olup mahremiyet riski yüksektir.

Meşru menfaat değerlendirmesinde denge testi yapılmalı; veri sorumlusunun menfaati ile ilgili kişinin gizlilik ve mahremiyet beklentisi karşılaştırılmalıdır.

⚠ Danışanın hassas verileri söz konusu olduğunda meşru menfaat dayanağı çoğu zaman yeterli olmayacak; daha güçlü bir hukuki sebep aranacaktır.

---

16. Özel Nitelikli Kişisel Verilerin İşlenmesi (Madde 6)

Sağlık verileri, KVKK bakımından özel nitelikli kişisel veri niteliğindedir. Bu veriler için iki temel hukuki dayanak geçerlidir:

- Açık rıza (Madde 6/2)
- Sağlık hizmetinin sunulması amacıyla, sır saklama yükümlülüğü altındaki kişiler tarafından işlenmesi (Madde 6/3)

Madde 6/3 istisnası, ruh sağlığı alanında özellikle psikiyatristler ve klinik psikologlar bakımından kritik öneme sahiptir. Zira sağlık hizmetinin sunulması amacıyla ve mesleki sır saklama yükümlülüğü çerçevesinde işlenen veriler, açık rıza aranmaksızın işlenebilir. Bununla birlikte bu istisna, sınırsız bir yetki vermez; veri işleme mutlaka sağlık hizmetinin sunulması amacıyla bağlantılı olmalı ve ölçülülük ilkesine uygun yürütülmelidir.

Özel nitelikli verilerin işlenmesinde ayrıca uygun güvenlik tedbirlerinin alınması, erişim yetkilerinin sınırlandırılması ve gereksiz paylaşım yapılmaması gerekir.

---

17. Pratik Senaryo Tablosu

Ruh sağlığı pratiğinde hangi veri işleme faaliyetinin hangi hukuki dayanağa oturtulacağı somut olaya göre belirlenmelidir. Aşağıdaki tablo, uygulamada sık karşılaşılan örnekleri göstermektedir:

Veri İşleme Faaliyeti	Hukuki Dayanak	Dikkat Edilmesi Gereken Husus
Seans notları tutulması	Madde 6/3 (sağlık hizmeti)	Yalnızca tedavi amacıyla sınırlı tutulmalı
Ses/video kaydı	Açık rıza	Ayrı, özel rıza formu gerekli
Adli makama bilgi verme	Hukuki yükümlülük	Talep yazılı olmalı, kayıt tutulmalı
Sigorta/SGK faturası	Hukuki yükümlülük	Yalnızca zorunlu bilgiler iletilmeli
Süpervizyon paylaşımı	Açık rıza veya anonimleştirme	Kimlik bilgileri çıkarılmalı
Araştırma/yayın	Açık rıza + etik kurul onayı	Anonimleştirme tercih edilmeli

Bölüm IV – Danışan Dosyaları, Seans Notları ve Kayıtların Yönetimi

18. Genel Olarak

Ruh sağlığı hizmetlerinin sunulması sırasında çok sayıda kişisel veri ve özel nitelikli kişisel veri üretilmektedir. Bu veriler yalnızca danışanın kimlik ve iletişim bilgilerinden ibaret değildir; seans notları, psikometrik test sonuçları, ses/video kayıtları, aile öyküleri, travma anlatıları ve intihar riski değerlendirmeleri de bu kapsamda yer almaktadır. Söz konusu verilerin nasıl oluşturulacağı, saklanacağı, paylaşılacağı ve imha edileceği, hem KVKK hem de sağlık mevzuatı açısından titizlikle yönetilmelidir.

---

19. Seans Notlarının Hukuki Niteliği

Seans notları, danışanın ruh sağlığına ilişkin özel nitelikli kişisel veri içerdiğinden KVKK'nın en sıkı koruma rejimine tabidir. Bu nedenle notlar yalnızca tedavi amacıyla tutulmalı; gereksiz ayrıntı, üçüncü kişilere ilişkin bilgi ve kişisel yorum içermemelidir. Özellikle danışanın beyanları ile klinik değerlendirme birbirinden ayrılmalı, notların amacı tıbbi/psikolojik bakımın sürdürülmesiyle sınırlı kalmalıdır.

Notların içeriği bakımından aşağıdaki ilkeler uygulanmalıdır:

- **Klinik gözlem ve değerlendirme odaklı olmalı**
- **Danışanın ifadelerini doğrudan aktarmaktan kaçınılmalı** (özellikle üçüncü kişiler hakkında)
- **Notlar, danışanın talebi hâlinde erişime açık olabileceği için dikkatli kaleme alınmalı**
- **Kâğıt notlar kilitli dolapta; dijital notlar şifreli sistemlerde saklanmalıdır**

Seans notlarının, ileride doğabilecek uyuşmazlıklarda delil niteliği taşıyabileceği de gözetilmeli; bu kayıtların subjektif, küçültücü veya gereksiz ayrıntı içeren bir dil yerine profesyonel, ölçülü ve doğrulanabilir bir dille tutulması gerekir.

---

20. Ses ve Video Kayıtları

Seans ses veya video kaydı için danışandan ayrı ve açık rıza alınması zorunludur. Bu rıza, genel aydınlatma metninin içinde örtülü biçimde alınamaz; her kayıt faaliyeti bakımından somut, bilgilendirmeye dayalı ve özgür iradeyle verilmiş olmalıdır. Ayrıca rıza metni, kayıt işleminin kapsamını ve sınırlarını açıkça göstermelidir.

Rızanın özellikle şu unsurları içermesi gerekir:

- Kaydın amacı (süpervizyon, eğitim, araştırma, kişisel arşiv)
- Kaydın kimlerle paylaşılacağı
- Saklama süresi
- Rızanın geri alınabilir olduğu

Kayıtlar şifreli ortamda saklanmalı; süpervizyon amaçlı paylaşımda kimlik bilgileri mümkünse anonimleştirilmelidir. Kayıtların ihtiyaçtan uzun süre tutulması veri minimizasyonu ilkesine aykırılık oluşturabilir. Bu nedenle ses ve video kayıtları bakımından saklama süresi, kayıt amacının sürmesiyle sınırlı olmalı; amaç sona erdiğinde kayıtlar gecikmeksizin imha edilmelidir.

---

21. Saklama Süreleri

Sağlık kayıtları için saklama süresi belirlenirken hem özel mevzuat hem de uyuşmazlık ihtimali birlikte değerlendirilmelidir. Uygulamada aşağıdaki süreler esas alınabilir:

- **Yetişkin danışanlar:** Son işlem tarihinden itibaren 10 yıl
- **Çocuk danışanlar:** Reşit olma tarihinden itibaren 10 yıl
- **Adli nitelik taşıyan kayıtlar:** Dava zamanaşımı süresince
- **Ses/video kayıtları:** Amaca göre belirlenmeli; amaç ortadan kalkınca imha edilmelidir

Saklama süresi belirlenirken, dosyanın yalnızca idari ihtiyaçlar için değil, olası bir denetim, şikâyet, tazminat veya ceza soruşturması sürecinde de gerekli olabileceği dikkate alınmalıdır. Buna karşılık, süresi dolan kayıtların süresiz biçimde muhafaza edilmesi KVKK'nın amaçla bağlantılı, sınırlı ve ölçülü olma ilkeleriyle bağdaşmaz.

---

22. Fiziksel ve Dijital Güvenlik Tedbirleri

Danışan dosyalarının hem fiziksel hem de dijital ortamda korunması zorunludur. Güvenlik tedbirleri, verinin niteliğine ve erişim riskine göre kademeli biçimde uygulanmalıdır. Aşağıdaki karşılaştırma, temel tedbirleri göstermektedir:

Fiziksel Güvenlik

- Kilitli dosya dolabı, yalnızca yetkili erişim
- Kâğıt formların imhası: çapraz kesim imha makinesi
- Ziyaretçi erişiminin kısıtlanması
- Ofis güvenliği (alarm, kamera — danışan alanları hariç)

Dijital Güvenlik

- Güçlü parola + iki faktörlü kimlik doğrulama
- Şifreli bulut depolama (tercihen Türkiye sunucusu)
- Düzenli yedekleme ve yedek şifreleme
- Antivirüs, güvenlik duvarı, güncel yazılım
- Erişim log kaydı tutulması

Fiziksel güvenlik bakımından, yalnızca yetkili personelin erişebileceği kilitli alanlar oluşturulmalı; belgelerin masada açık bırakılması, ortak alanlarda unutulması veya danışanların görebileceği yerlerde saklanması önlenmelidir. Dijital ortamda ise sistem güvenliği yalnızca teknik yazılımlarla değil, kullanıcı yetkilendirmesi, log takibi ve düzenli güvenlik denetimleriyle desteklenmelidir.

---

23. İmha ve Silme Prosedürü

Saklama süresi dolan veriler için periyodik bir imha takvimi oluşturulmalıdır. İmha yöntemi verinin niteliğine göre belirlenmeli; kâğıt belgeler çapraz kesim imha makinesiyle, dijital veriler ise güvenli silme yazılımıyla yok edilmelidir. Basit silme işlemleri, verinin teknik olarak geri getirilebilir olması nedeniyle yeterli kabul edilmemelidir.

İmha sürecinde aşağıdaki hususlara uyulmalıdır:

- İmha işlemi önceden belirlenmiş takvime göre yürütülmelidir
- İmha edilen veri türü ve kapsamı kayıt altına alınmalıdır
- İmha tutanağı düzenlenmeli ve saklanmalıdır
- İmha işlemi, sonradan ispatlanabilir olmalıdır

Böylece hem veri güvenliği sağlanır hem de gereksiz veri saklama riskleri azaltılır. İmha yükümlülüğünün sistematik şekilde yürütülmesi, ruh sağlığı hizmeti sunanların hem KVKK hem de mesleki özen yükümlülükleri bakımından temel sorumluluklarından biridir.

Bölüm V – Yapay Zekâ ve Dijital Araçlar

24. Dijitalleşme ve Ruh Sağlığı Hizmetleri

Son yıllarda dijital teknolojilerde yaşanan gelişmeler, ruh sağlığı hizmetlerinin sunuluş biçimini önemli ölçüde değiştirmiştir. Elektronik danışan dosyaları, çevrim içi terapi uygulamaları, yapay zekâ destekli değerlendirme araçları ve dijital ruh sağlığı platformları artık günlük pratiğin bir parçası hâline gelmiştir. Bu dönüşüm, hizmet erişimini kolaylaştırırken veri güvenliği, gizlilik ve hukuki uyum açısından yeni riskler de doğurmaktadır.

---

25. Çevrim İçi Terapi ve Telepsikiyatri

Video görüşme platformları aracılığıyla yürütülen terapi ve psikiyatri hizmetleri, KVKK kapsamında özel değerlendirme gerektirmektedir. Bu hizmetlerde kullanılan altyapının yalnızca teknik yeterliliği değil, aynı zamanda sağlık verisi işleme bakımından hukuka uygunluğu da aranmalıdır. Özellikle platform seçimi, veri işleme ilişkisi, kayıt uygulamaları ve bağlantı güvenliği bakımından aşağıdaki asgari standartlara uyulmalıdır.

- **Platform seçimi:** Yalnızca sağlık verisi işlemeye uygun, şifreli ve KVKK uyumlu platformlar kullanılmalıdır; WhatsApp ve Zoom ücretsiz sürüm gibi tüketici uygulamaları uygun değildir.
- **Veri işleme sözleşmesi:** Platform sağlayıcısıyla yazılı veri işleme sözleşmesi (DPA) imzalanmalıdır.
- **Sunucu konumu:** Türkiye'de veya yeterli koruma düzeyine sahip ülkede veri depolama tercih edilmelidir.
- **Kayıt yasağı:** Danışanın açık rızası olmaksızın görüşme kaydedilemez.
- **Güvenli bağlantı:** Şifreli (end-to-end) bağlantı zorunludur.

Çevrim içi terapi hizmetlerinde, görüşmenin yapıldığı ortamın gizliliği kadar iletim altyapısının güvenliği de önem taşır. Meslek mensubu, kullandığı sistemin üçüncü kişilerin erişimine kapalı olduğundan, verilerin açık aktarılmadığından ve görüşme içeriklerinin hizmet sağlayıcının ticari amaçları için işlenmediğinden emin olmalıdır.

---

26. Yapay Zekâ Araçlarının Kullanımı

Ruh sağlığı pratiğinde yapay zekâ araçlarının kullanımı ciddi KVKK riskleri taşımaktadır. ChatGPT benzeri büyük dil modelleri, otomatik transkripsiyon yazılımları ve klinik karar destek sistemleri, danışan verisini doğrudan veya dolaylı olarak işleyebildiğinden, her kullanım senaryosu ayrıca hukuki değerlendirme gerektirir. Danışan verisinin bu sistemlere girilmesi çoğu durumda veri aktarımı niteliği taşıyabilir ve uygun hukuki dayanak olmaksızın gerçekleştirilemez.

Risk Alanı	Hukuki Değerlendirme	Uygulamada Dikkat Edilecek Nokta
ChatGPT / LLM kullanımı	Danışan bilgilerini yapay zekâya girmek veri aktarımı sayılır; açık rıza ve DPA olmaksızın yapılamaz.	Kimlik belirleyici unsurlar çıkarılmalı, mümkünse paylaşım yapılmamalıdır.
Otomatik transkripsiyon	Seans ses kaydının yapay zekâ ile metne dönüştürülmesi için ayrı rıza gerekir.	Ses kaydı, işleme amacı ve saklama süresi önceden belirlenmelidir.
Klinik karar destek	Tanı önerisi sunan sistemler, veri işleyen sıfatıyla DPA kapsamına girebilir.	Nihai karar yalnızca meslek mensubu tarafından verilmelidir.
Yapay zekâ ile not tutma	Danışan kimliğini içeren notların yapay zekâya aktarılması hukuki dayanak gerektirir.	Asgari veri kullanımı ve anonimleştirme ilkeleri uygulanmalıdır.

⚠ Danışan verisinin yapay zekâ sistemlerine girilmesi çoğu durumda veri aktarımı niteliği taşıyabilir ve uygun hukuki dayanak olmaksızın gerçekleştirilemez.

Yapay zekâ sistemlerinin sağladığı hız ve kolaylık, mesleki özen yükümlülüğünü ortadan kaldırmaz. Aksine, sağlık verisinin işlenmesi bakımından daha sıkı bir denetim ve kayıt disiplini gerektirir. Bu nedenle her kullanım öncesinde sistemin veri akışı, saklama politikası ve sağlayıcının rolü açıkça değerlendirilmelidir.

---

27. Pratik Kural: Yapay Zekâ Kullanımında Asgari Standartlar

Yapay zekâ kullanımında riskleri azaltmak için aşağıdaki asgari kurallara uyulmalıdır:

- Danışan verisi içeren hiçbir bilgi, DPA imzalanmamış yapay zekâ platformuna girilmemelidir.
- Yapay zekâ kullanımı aydınlatma metninde açıkça belirtilmelidir.
- Danışan adı, T.C. kimlik no ve doğrudan tanımlayıcılar yapay zekâya aktarılmamalıdır.
- Anonimleştirilmiş vaka özetleri kullanılabilir; ancak yeniden tanımlanabilirlik riski değerlendirilmelidir.
- Yapay zekâ sağlayıcısının sunucu konumu ve veri saklama politikası incelenmelidir.

ⓘ Bu kurallar, yapay zekâ araçlarının tamamen dışlanması gerektiği anlamına gelmez. Ancak ruh sağlığı alanında, teknoloji kullanımı ancak veri minimizasyonu, amaçla sınırlılık ve açık hukuki dayanak ilkeleriyle birlikte kabul edilebilir.

---

28. Dijital Ruh Sağlığı Uygulamaları (Mobil Uygulamalar)

Danışanlara önerilebilecek meditasyon, ruh hâli takibi veya terapi destek uygulamaları da KVKK kapsamında değerlendirilmelidir. Uzman, danışanına bir uygulama önerirken o uygulamanın veri politikasını incelemeli; özellikle veri aktarımı, sunucu konumu ve üçüncü taraf paylaşımı konularında danışanı bilgilendirmelidir. Uygulamanın reklam amaçlı veri toplaması, sağlık dışı profilleme yapması veya üçüncü kişilerle paylaşımda bulunması hâlinde ek risk oluşabileceği unutulmamalıdır.

---

29. Bulut Depolama ve Elektronik Dosya Sistemleri

Danışan dosyalarının bulut ortamında saklanması için teknik ve hukuki güvence birlikte sağlanmalıdır. Bulut sistemleri, erişim kolaylığı ve yedekleme avantajı sunsa da, verinin nerede tutulduğu ve kimler tarafından işlendiği açıkça belirlenmeden kullanılmamalıdır. Sağlayıcı ile kurulan ilişki, veri işleme faaliyeti bakımından yazılı şekilde düzenlenmelidir.

Bulut depolama ve elektronik dosya sistemlerinde aşağıdaki şartlar aranmalıdır:

- Türkiye'de sunucu barındıran veya yeterli koruma düzeyine sahip ülkede hizmet veren sağlayıcı seçilmeli
- Sağlayıcıyla veri işleme sözleşmesi imzalanmalı
- Erişim yetkileri rol bazlı tanımlanmalı
- Şifreleme hem aktarımda hem depolamada sağlanmalı
- Yedekleme ve felaket kurtarma planı oluşturulmalı

Elektronik dosya sistemlerinde yalnızca teknik güvenlik yeterli değildir; kullanıcı yetkilendirmesi, erişim kayıtları ve periyodik denetim de sistemin bir parçası olmalıdır. Özellikle sağlık verilerinin işlendiği ortamlarda, yanlış yapılandırılmış bir bulut hizmeti ciddi veri ihlallerine yol açabilir.

Bölüm VI – Çocuk Danışanlar ve Hassas Gruplar

30. Genel Olarak

Ruh sağlığı hizmetlerinde bazı danışan grupları ve bazı yaşam olayları, kişisel verilerin korunması bakımından özel değerlendirme gerektirmektedir. Özellikle; çocuklar, ergenler, boşanmış ebeveynlerin çocukları, intihar riski taşıyan bireyler, aile içi şiddet mağdurları, bağımlılık sorunu yaşayan kişiler gibi hassas gruplar bakımından veri işleme faaliyetleri yalnızca KVKK perspektifinden değil, bireyin üstün yararı ve temel haklarının korunması perspektifinden de değerlendirilmelidir.

---

31. Çocuklara İlişkin Kişisel Veriler

Çocuklara ait kişisel veriler, veri koruma hukukunda özel önem verilen veri kategorileri arasında yer almaktadır. Bunun temel nedeni çocukların hukuki ve fiili açıdan yetişkinlere göre daha korunmasız olmalarıdır. Ruh sağlığı hizmetlerinde işlenen çocuk verileri çoğu zaman yalnızca sağlık verilerini değil; aile ilişkilerini, eğitim hayatını, gelişimsel özellikleri, davranışsal gözlemleri, sosyal çevreyi de içermektedir. Bu nedenle çocuklara ilişkin verilerin korunması konusunda yüksek hassasiyet gösterilmelidir.

---

32. Çocuğun Üstün Yararı İlkesi

Çocuklara ilişkin her türlü değerlendirmede temel hareket noktası çocuğun üstün yararı ilkesidir. Bu ilke hem uluslararası insan hakları belgelerinde hem de Türk hukukunda kabul edilmektedir. Veri paylaşımı, kayıt saklama veya üçüncü kişilere bilgi verilmesi gibi işlemler değerlendirilirken yalnızca ebeveynlerin talepleri değil, çocuğun menfaatleri de dikkate alınmalıdır. Bazı durumlarda ebeveynin bilgi talebi ile çocuğun mahremiyetinin korunması arasında hassas bir denge kurulması gerekebilir.

---

33. Boşanmış Ebeveynler ve Bilgi Talepleri

Uygulamada en sık karşılaşılan sorunlardan biri boşanmış ebeveynlerin danışan kayıtlarına erişim talepleridir. Boşanmış olma durumu tek başına ebeveynlik sıfatını ortadan kaldırmaz. Ancak her somut olayda; velayet durumu, mahkeme kararları, ebeveynlerin temsil yetkileri, çocuğun üstün yararı birlikte değerlendirilmelidir. Bu nedenle bilgi taleplerinin otomatik biçimde kabul edilmesi veya reddedilmesi doğru değildir. Her talep kendi hukuki çerçevesi içerisinde incelenmelidir.

> Anayasa Mahkemesi Kararı. Anayasa Mahkemesi, boşanma sürecinde eşlerden birinin diğer eşe ait sağlık kayıtlarını ve psikiyatrik tedavi bilgilerini elde ederek mahkemeye sunmasına ilişkin olayda, sağlık verilerinin özel korumaya tabi kişisel veri niteliğinde olduğunu vurgulamıştır. Mahkeme ayrıca eş olmanın sağlık kayıtlarına erişim hakkı vermeyeceğini belirterek kişisel verilerin korunmasını isteme hakkının ihlal edildiğine karar vermiştir (H.Ö. Başvurusu, B. No: 2019/20473, 03.02.2022). Aynı yöndeki AİHM içtihadı da tıbbi belgelerin medeni yargılamada, başka yolla ulaşılabilecekken kullanılmasını ihlal saymıştır (L.L. v. Fransa, B. No: 7508/02, 10.10.2006). Buna karşılık, sağlık durumunu bizzat dava konusu yapan kişinin kayıtlarının sınırlı biçimde sunulması orantılı bulunabilir (M.S. v. İsveç, B. No: 20837/92, 27.08.1997). Bu iki karar birlikte, ifşanın yasak olmadığını ama yalnızca gereklilik ve ölçülülük ölçütleri çerçevesinde mümkün olduğunu göstermektedir.

---

34. Aile Üyelerinin Bilgi Talepleri

Meslek mensupları sıklıkla; eşlerden, anne ve babalardan, kardeşlerden, diğer yakın akrabalardan bilgi talepleri alabilmektedir. Bu talepler çoğu zaman iyi niyetli gerekçelere dayanıyor olsa da kişisel verilerin korunmasına ilişkin yükümlülükleri ortadan kaldırmaz. Bir kişinin aile üyesi olması, danışana ait tüm bilgileri öğrenme hakkı bulunduğu anlamına gelmez. Bu nedenle aile üyelerinden gelen talepler değerlendirilirken hukuki dayanak ayrıca incelenmelidir.

---

35. Acil Durumlar ve Hayatın Korunması

Bazı durumlarda bireyin yaşamı veya beden bütünlüğü bakımından ciddi riskler ortaya çıkabilir. Örneğin; intihar girişimi riski, ağır kendine zarar verme eğilimi, ciddi psikiyatrik krizler, üçüncü kişilere yönelik yakın ve ciddi tehlike gibi durumlarda veri işleme faaliyetlerinin hukuki değerlendirmesi olağan vakalardan farklılık gösterebilir. Bu tür durumlarda yalnızca gizlilik ilkesi değil, yaşam hakkı ve beden bütünlüğünün korunmasına ilişkin yükümlülükler de dikkate alınmalıdır. Her olay kendi özellikleri içerisinde değerlendirilmelidir.

---

36. İntihar Riski Taşıyan Danışanlar

İntihar düşüncelerinin paylaşılması ruh sağlığı hizmetlerinde karşılaşılabilecek en hassas durumlardan biridir. Bu tür vakalarda meslek mensupları bir yandan danışanın mahremiyetini korumakla yükümlü iken, diğer yandan ortaya çıkabilecek hayati riskleri de değerlendirmek zorundadır. Bu nedenle risk değerlendirmesinin dikkatli şekilde yapılması ve alınan kararların kayıt altına alınması önem taşımaktadır. Özellikle yakın ve ciddi bir tehlikenin varlığı değerlendiriliyorsa, yalnızca veri koruma perspektifiyle değil, temel hakların korunması perspektifiyle de hareket edilmelidir.

---

37. Aile İçi Şiddet ve İstismar İddiaları

Aile içi şiddet ve istismar vakaları, hem kişisel verilerin korunması hem de bireyin güvenliğinin sağlanması bakımından özel önem taşımaktadır. Bu tür vakalarda elde edilen bilgiler çoğu zaman son derece hassas niteliktedir. Meslek mensupları; mağdurun güvenliği, veri güvenliği, hukuki yükümlülükler, ilgili mevzuat hükümleri arasındaki dengeyi gözetmelidir. Özellikle çocukların taraf olduğu vakalarda durum daha da hassas hâle gelebilmektedir.

---

38. Üçüncü Kişiler Hakkındaki Bilgiler

Terapi ve danışmanlık süreçlerinde yalnızca danışana ilişkin bilgiler değil, üçüncü kişiler hakkında bilgiler de paylaşılabilmektedir. Örneğin danışan; eşi, ailesi, iş arkadaşları, arkadaş çevresi hakkında ayrıntılı açıklamalarda bulunabilir. Bu bilgiler de veri koruma hukuku bakımından önem taşımaktadır. Meslek mensuplarının kayıt oluştururken ve veri paylaşımı yaparken bu hususu dikkate almaları gerekir.

---

39. Sosyal Medya ve Danışan Mahremiyeti

Günümüzde sosyal medya kullanımı yeni hukuki sorunları beraberinde getirmektedir. Meslek mensuplarının danışanlara ilişkin bilgileri doğrudan veya dolaylı biçimde sosyal medya ortamlarında paylaşmaları ciddi mahremiyet ihlallerine yol açabilir. Kişinin ismi belirtilmese bile; olay örgüsü, meslek bilgisi, yaşadığı şehir, aile yapısı gibi detaylar danışanın belirlenmesine neden olabilir. Bu nedenle sosyal medya kullanımı sırasında mahremiyet risklerinin ayrıca değerlendirilmesi gerekir.

---

40. Ara Değerlendirme

Çocuklar, hassas gruplar ve kriz vakaları bakımından veri koruma hukukunun uygulanması çoğu zaman standart vakalara göre daha karmaşık bir görünüm arz etmektedir. Bu nedenle ruh sağlığı alanında faaliyet gösteren meslek mensuplarının yalnızca mevzuat hükümlerini değil; insan hakları, çocuk hakları, yaşam hakkı ve bireyin üstün yararı gibi temel ilkeleri de dikkate alarak hareket etmeleri gerekmektedir. Her somut olay kendi koşulları içerisinde değerlendirilmeli; özellikle bireyin güvenliği ile mahremiyet hakkı arasında ortaya çıkabilecek çatışmalarda dikkatli ve ölçülü bir yaklaşım benimsenmelidir.

Bölüm VII – Veri İhlalleri ve Hukuki Sonuçları

41. Veri İhlali Kavramı

Kişisel verilerin korunması hukukunda veri ihlali, kişisel verilerin hukuka aykırı şekilde; elde edilmesi, açıklanması, değiştirilmesi, silinmesi, kaybedilmesi, erişilemez hâle gelmesi, yetkisiz kişiler tarafından görüntülenmesi sonuçlarını doğuran güvenlik olaylarını ifade etmektedir. Veri ihlali yalnızca dışarıdan gerçekleştirilen siber saldırılar sonucunda ortaya çıkmaz. İnsan hataları, organizasyon eksiklikleri ve teknik yetersizlikler de veri ihlaline neden olabilir.

---

42. Ruh Sağlığı Alanında Veri İhlallerinin Özelliği

Ruh sağlığı alanında meydana gelen veri ihlallerinin etkisi birçok sektöre göre daha ağır olabilir. Çünkü ihlale konu olan veriler çoğu zaman; psikiyatrik teşhisleri, terapi süreçlerini, travmatik yaşantıları, bağımlılık geçmişini, aile ilişkilerini, cinsel yaşamı içermektedir. Bu tür bilgilerin ifşası bireylerin sosyal hayatlarında, aile ilişkilerinde ve mesleki yaşamlarında ciddi sonuçlar doğurabilir. Bu nedenle ruh sağlığı alanında veri güvenliği yalnızca teknik bir mesele olarak görülmemelidir.

---

43. Veri İhlalinin Kaynakları

Uygulamada veri ihlalleri farklı nedenlerle ortaya çıkabilmektedir. En sık karşılaşılan sebepler şunlardır:

İnsan Kaynaklı Hatalar

- yanlış kişiye e-posta gönderilmesi,
- yanlış dosyanın paylaşılması,
- danışan bilgilerinin açık bırakılması,
- erişim yetkilerinin hatalı tanımlanması.

Teknik Sorunlar

- sistem arızaları,
- yedekleme eksiklikleri,
- güvenlik açıkları,
- yazılım hataları.

Siber Saldırılar

- fidye yazılımları,
- kimlik avı saldırıları,
- yetkisiz erişim girişimleri,
- veri sızıntıları.

---

44. Veri İhlali Tespit Edildiğinde İlk Yapılması Gerekenler

Bir veri ihlali fark edildiğinde panik yerine sistematik hareket edilmelidir. Öncelikle; ihlalin devam edip etmediği, hangi verilerin etkilendiği, kaç kişinin etkilendiği, risk seviyesinin ne olduğu tespit edilmeye çalışılmalıdır. Olayın mümkün olduğunca erken kayıt altına alınması önemlidir.

---

45. Olayın Belgelendirilmesi

Veri ihlali sonrasında yapılan en önemli işlemlerden biri olayın kayıt altına alınmasıdır. Bu kapsamda; olayın tarihi, tespit zamanı, etkilenen veri kategorileri, alınan tedbirler, yapılan değerlendirmeler belgelenmelidir. Belgelendirme hem kurumsal hafıza hem de olası hukuki süreçler bakımından önem taşımaktadır.

---

46. Risk Değerlendirmesi

Her veri ihlali aynı düzeyde risk oluşturmaz. Bu nedenle ihlalin etkileri ayrıca değerlendirilmelidir. Örneğin yalnızca randevu bilgilerinin ifşası ile terapi notlarının ifşası aynı risk düzeyine sahip değildir. Özellikle sağlık verilerinin etkilenmesi durumunda daha dikkatli değerlendirme yapılması gerekir.

---

47. İlgili Kişiler Açısından Olası Sonuçlar

Veri ihlallerinin bireyler üzerinde doğurabileceği sonuçlar farklılık gösterebilir. Bunlar arasında; ayrımcılık, damgalanma, psikolojik zarar, ekonomik zarar, itibar kaybı, sosyal dışlanma gibi sonuçlar yer alabilir. Ruh sağlığı alanında işlenen veriler bakımından bu riskler daha yüksek düzeyde ortaya çıkabilmektedir.

---

48. İdari Para Cezaları

KVKK kapsamında veri sorumluları çeşitli idari yaptırımlarla karşılaşabilir. İhlalin niteliğine göre; aydınlatma yükümlülüğünün ihlali, veri güvenliği yükümlülüklerinin ihlali, Kurul kararlarının yerine getirilmemesi, sicil yükümlülüklerine aykırılık gibi nedenlerle idari yaptırımlar uygulanabilir. İdari yaptırımların miktarı mevzuattaki güncellemeler doğrultusunda zaman içerisinde değişebilmektedir. Bu nedenle güncel tutarların ayrıca kontrol edilmesi gerekir.

---

49. Tazminat Sorumluluğu

Veri ihlalleri yalnızca idari yaptırımlara neden olmaz. Bazı durumlarda ilgili kişiler maddi veya manevi zararlarının giderilmesini talep edebilirler. Özellikle sağlık verilerinin ifşası sonucunda ortaya çıkan zararlar bakımından tazminat talepleri gündeme gelebilmektedir. Bu nedenle veri ihlali süreçlerinin dikkatli şekilde yönetilmesi önem taşımaktadır.

---

50. Ceza Hukuku Boyutu

Bazı veri ihlalleri aynı zamanda ceza hukuku bakımından da sonuç doğurabilir. Türk Ceza Kanunu'nda; kişisel verilerin hukuka aykırı kaydedilmesi, kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi, verilerin yok edilmemesi gibi fiiller suç olarak düzenlenmiştir. Bu nedenle veri ihlalleri yalnızca KVKK perspektifiyle değil, ceza hukuku bakımından da değerlendirilmelidir.

---

51. Norveç Veri Koruma Otoritesi'nin Takip Pikseli (Tracking Pixel) Kararları

2025 yılında Norveç Veri Koruma Otoritesi (Datatilsynet), internet sitelerinde kullanılan takip piksellerine ilişkin kapsamlı bir denetim gerçekleştirmiştir. Denetim kapsamında incelenen altı farklı internet sitesinin tamamında, ziyaretçilere ait kişisel verilerin üçüncü taraflara hukuka aykırı biçimde aktarıldığı tespit edilmiştir. İncelenen internet siteleri arasında; çevrim içi sağlık hizmeti sunan platformlar, sağlık bilgileri paylaşan internet siteleri, çevrim içi eczane hizmetleri, çocuklara yönelik destek hatları, hassas sosyal gruplara hizmet veren platformlar yer almaktadır.

Denetim sonucunda, internet sitelerinde kullanılan takip piksellerinin ziyaretçilere ilişkin çeşitli bilgileri otomatik olarak üçüncü taraf şirketlere aktardığı belirlenmiştir. Otorite, bazı durumlarda aktarılan bilgilerin kişilerin sağlık durumları, dini inançları, özel yaşamları veya hassas sosyal durumları hakkında dolaylı çıkarım yapılmasına imkân sağlayabilecek nitelikte olduğunu değerlendirmiştir. Özellikle çocuklara ve kırılgan gruplara ilişkin verilerin üçüncü taraflara aktarılması ağır bir ihlal olarak kabul edilmiştir.

Kararlarda dikkat çeken hususlardan biri, veri sorumlularının önemli bir bölümünün kullanılan teknolojinin nasıl çalıştığını tam olarak bilmediklerini ileri sürmelerine rağmen sorumluluktan kurtulamamış olmalarıdır. Otorite, veri sorumlularının kullandıkları teknolojik araçların kişisel veri işleme süreçleri üzerindeki etkilerini anlamak ve gerekli hukuki değerlendirmeleri yapmakla yükümlü olduklarını vurgulamıştır.

Bu kararlar, ruh sağlığı alanında faaliyet gösteren meslek mensupları açısından da önem taşımaktadır. Günümüzde birçok internet sitesi ve çevrim içi danışmanlık platformunda; Meta Pixel, Google Analytics, reklam teknolojileri, üçüncü taraf analiz araçları, çevrim içi randevu sistemleri kullanılmaktadır. Bu sistemlerin bazıları, kullanıcıların internet sitesi üzerindeki davranışlarını üçüncü taraf hizmet sağlayıcılara aktarabilmektedir. Özellikle psikolojik danışmanlık, psikoterapi veya ruh sağlığı hizmeti sunan internet sitelerinde, ziyaret edilen sayfalar veya gerçekleştirilen işlemler tek başına dahi kişinin sağlık durumu hakkında çıkarım yapılmasına imkân verebilir. Bu nedenle veri güvenliği değerlendirmeleri yalnızca danışan dosyaları veya terapi kayıtları bakımından değil; internet siteleri, çevrim içi randevu sistemleri ve dijital pazarlama araçları bakımından da yapılmalıdır.

---

52. Vastaamo Vakası: Veri Güvenliğinin Önemi

Ruh sağlığı alanında yaşanan en dikkat çekici veri ihlallerinden biri Finlandiya'da faaliyet gösteren Vastaamo psikoterapi merkezine ilişkin olaydır. Bu olayda çok sayıda danışana ait son derece hassas terapi kayıtlarının yetkisiz kişiler tarafından ele geçirildiği ve bazı danışanların şantaja maruz bırakıldığı kamuoyuna yansımıştır. Vaka, ruh sağlığı hizmetlerinde veri güvenliğinin yalnızca hukuki bir formalite olmadığını açık biçimde göstermiştir. Bir kez ifşa edilen terapi kayıtlarının geri alınması çoğu zaman mümkün değildir. Bu nedenle veri güvenliğinin temel amacı yalnızca yaptırımlardan kaçınmak değil, danışanların mahremiyetini korumaktır.

---

53. Kurumsal Hazırlık ve Kriz Yönetimi

Her kurumun veri ihlali yaşanabileceği varsayımıyla hareket etmesi gerekir. Bu nedenle önceden; kriz planları, iletişim prosedürleri, teknik müdahale süreçleri, sorumluluk dağılımları oluşturulmalıdır. Kriz anında alınacak kararların önceden planlanmış olması, olası zararların azaltılmasına katkı sağlayacaktır.

Sonuç ve Ekler – Pratik Araçlar ve Kontrol Listeleri

Sonuç

Ruh sağlığı hizmetleri, bireylerin en mahrem bilgilerinin işlendiği faaliyet alanlarından biridir. Psikiyatristler, klinik psikologlar ve psikolojik danışmanlar tarafından işlenen veriler çoğu zaman bireyin yalnızca sağlık durumuna değil; yaşam öyküsüne, aile ilişkilerine, travmalarına, düşünce dünyasına ve kişisel tercihlerine ilişkin son derece hassas bilgiler içermektedir.

Bu nedenle kişisel verilerin korunması, yalnızca yasal yükümlülüklerin yerine getirilmesinden ibaret değildir. Veri koruma hukuku, danışan ile meslek mensubu arasındaki güven ilişkisinin korunmasının da temel araçlarından biridir. Teknolojik gelişmeler, çevrim içi hizmetler, yapay zekâ uygulamaları ve dijital kayıt sistemleri veri işleme faaliyetlerini kolaylaştırmakta; ancak aynı zamanda yeni hukuki riskler de ortaya çıkarmaktadır. Bu nedenle ruh sağlığı alanında faaliyet gösteren tüm meslek mensuplarının; güncel mevzuatı takip etmeleri, veri güvenliği tedbirlerini sürekli geliştirmeleri, kurumsal farkındalığı artırmaları, danışan mahremiyetini merkeze alan bir yaklaşım benimsemeleri gerekmektedir.

Kişisel verilerin korunmasına ilişkin yükümlülükler yalnızca hukuki bir zorunluluk değil; aynı zamanda insan onuruna, özel hayatın gizliliğine ve mesleki etik ilkelere duyulan saygının da bir yansımasıdır.

Ekler – Pratik Araçlar ve Kontrol Listeleri

Aşağıdaki kontrol listeleri ve risk testleri, yukarıda açıklanan hukuki çerçeveyi uygulamaya dökmek için hazırlanmış pratik araçlardır. Sorulardan herhangi birine "Hayır" cevabı veriliyorsa, ilgili alanda veri koruma riski oluşabilir.

Ek 1 – Danışan Mahremiyeti Hızlı Risk Testi

Şeffaflık

- ☐ Danışanlara güncel bir aydınlatma metni sunuluyor mu?
- ☐ Çevrim içi görüşmelerde ayrıca bilgilendirme yapılıyor mu?
- ☐ Danışanlar hangi verilerinin işlendiğini anlayabiliyor mu?
- ☐ Veri işleme amaçları açık ve anlaşılır şekilde açıklanıyor mu?

Veri Minimizasyonu

- ☐ Yalnızca gerekli veriler toplanıyor mu?
- ☐ Formlarda yer alan her veri kategorisinin somut bir amacı bulunuyor mu?
- ☐ "İleride kullanılabilir" düşüncesiyle veri toplanmasından kaçınılıyor mu?

Güvenlik

- ☐ Danışan dosyalarına yalnızca yetkili kişiler erişebiliyor mu?
- ☐ Erişim yetkileri düzenli olarak gözden geçiriliyor mu?
- ☐ İşten ayrılan personelin erişimleri kaldırılıyor mu?
- ☐ Elektronik kayıtlar uygun güvenlik tedbirleri ile korunuyor mu?

Ek 2 – Seans Notları Risk Değerlendirmesi

Seans notları, ruh sağlığı hizmetlerinde en yüksek risk taşıyan veri kategorilerinden biridir. Aşağıdaki sorular düzenli olarak değerlendirilmelidir:

- ☐ Seans notlarının tutulma amacı belirli mi?
- ☐ Tutulan her bilgi terapi süreci bakımından gerekli mi?
- ☐ Notlara erişim yetkileri sınırlandırılmış mı?
- ☐ Notlar güvenli biçimde saklanıyor mu?
- ☐ Notların paylaşılmasına ilişkin kurallar belirlenmiş mi?
- ☐ Kayıtlar gerektiğinde hukuki olarak açıklanabilecek nitelikte mi?

Ek 3 – Yapay Zekâ Kullanımı Risk Testi

Yapay zekâ sistemleri kullanılmadan önce aşağıdaki hususlar değerlendirilmelidir.

Danışan Verilerinin Korunması

- ☐ Danışanın adı ve kimlik bilgileri çıkarılıyor mu?
- ☐ İletişim bilgileri sisteme aktarılmıyor mu?
- ☐ Aile bireylerinin kimliklerini ortaya çıkarabilecek bilgiler temizleniyor mu?
- ☐ Veri minimizasyonu ilkesi uygulanıyor mu?

Anonimleştirme

- ☐ Kişinin tanınmasına yol açabilecek olay örgüleri gözden geçiriliyor mu?
- ☐ Yaş, meslek, şehir ve benzeri bilgiler değerlendiriliyor mu?
- ☐ Yeniden kimliklendirme riski dikkate alınıyor mu?

İnsan Denetimi

- ☐ Yapay zekâ çıktıları insan tarafından kontrol ediliyor mu?
- ☐ Nihai karar meslek mensubu tarafından veriliyor mu?
- ☐ Yapay zekâ sistemleri profesyonel değerlendirme yerine kullanılmıyor mu?

⚠ Uyarı. Bir danışanın adının kaldırılması tek başına anonimleştirme anlamına gelmez. Bazı durumlarda yaş, meslek, şehir, aile yapısı ve olay örgüsü birlikte değerlendirildiğinde kişinin yeniden belirlenmesi mümkün olabilir.

Ek 4 – Web Sitesi ve Dijital Hizmetler Kontrol Listesi

Çerezler ve Takip Teknolojileri

- ☐ Çerez politikası mevcut mu?
- ☐ Çerez tercih mekanizması bulunuyor mu?
- ☐ Kullanılan takip teknolojileri tespit edilmiş mi?
- ☐ Üçüncü taraf hizmet sağlayıcılar belirlenmiş mi?

Analiz ve Reklam Araçları

- ☐ Google Analytics kullanılıyor mu?
- ☐ Meta Pixel kullanılıyor mu?
- ☐ Reklam veya analiz araçlarının hangi verileri topladığı biliniyor mu?
- ☐ Bu araçların veri aktarım süreçleri değerlendirilmiş mi?

Çevrim İçi Hizmetler

- ☐ Çevrim içi randevu sistemi kullanılıyor mu?
- ☐ İletişim formlarında sağlık verisi toplanıyor mu?
- ☐ Aktarılan verilerin kapsamı değerlendirilmiş mi?
- ☐ Yurt dışına veri aktarımı ihtimali incelenmiş mi?

⚠ Uyarı. Veri ihlalleri yalnızca siber saldırılar sonucunda ortaya çıkmaz. Takip pikselleri, analiz araçları ve üçüncü taraf hizmetler aracılığıyla da kişisel verilerin hukuka aykırı şekilde aktarılması mümkündür.

Ek 5 – Çocuk Danışanlar İçin Kırmızı Bayraklar

Çocuklara ilişkin veri işleme faaliyetlerinde aşağıdaki hususlar ayrıca değerlendirilmelidir.

- ☐ Velayet durumu incelendi mi?
- ☐ Temsil yetkisi bulunan kişiler belirlendi mi?
- ☐ Bilgi talebinde bulunan kişinin yetkisi doğrulandı mı?
- ☐ Çocuğun üstün yararı değerlendirildi mi?
- ☐ Çocuğun mahremiyet hakkı dikkate alındı mı?
- ☐ Paylaşılması istenen bilgi gerçekten gerekli mi?
- ☐ Mahkeme kararları ve diğer hukuki belgeler incelendi mi?

⊗ Kırmızı Bayrak. Velayet uyuşmazlığı bulunan durumlarda bilgi paylaşımı yapılmadan önce ayrıca hukuki değerlendirme yapılması gerekir.

Ek 6 – Veri Paylaşımı Öncesi Son Kontrol

Her veri paylaşımı öncesinde aşağıdaki beş temel soru sorulmalıdır.

01

Neden?

Bu veriyi neden paylaşıyorum?

02

Hukuki dayanak nedir?

Paylaşımın hukuki dayanağı mevcut mu?

03

Gerekli mi?

Aynı amaca daha az veri paylaşarak ulaşılabilir mi?

04

Güvenli mi?

Paylaşım güvenli bir yöntemle gerçekleştiriliyor mu?

05

Açıklanabilir mi?

Bu paylaşım daha sonra denetlendiğinde gerekçelendirilebilir mi?

Kural. Paylaşılması zorunlu olmayan hiçbir veri paylaşılmamalıdır.

Ek 7 – Personel ve Sekreterya Kontrol Listesi

- ☐ Personelin erişim yetkileri yazılı olarak belirlenmiş mi?
- ☐ Gizlilik yükümlülükleri personele açıklanmış mı?
- ☐ Gizlilik taahhütnameleri imzalanmış mı?
- ☐ Sekreterlerin erişimi görev alanları ile sınırlandırılmış mı?
- ☐ Stajyerlerin erişim yetkileri ayrıca belirlenmiş mi?
- ☐ İşten ayrılan personelin erişimleri kaldırılıyor mu?
- ☐ Düzenli KVKK farkındalık eğitimleri veriliyor mu?

Ek 8 – Veri İhlali Acil Durum Kartı

İlk 60 Dakika

- ☐ İhlalin devam edip etmediği tespit edildi mi?
- ☐ Yetkisiz erişim sonlandırıldı mı?
- ☐ Etkilenen sistemler izole edildi mi?
- ☐ İlk olay kaydı oluşturuldu mu?

İlk 24 Saat

- ☐ Etkilenen veri kategorileri belirlendi mi?
- ☐ Risk değerlendirmesi yapıldı mı?
- ☐ Teknik inceleme başlatıldı mı?
- ☐ Hukuki değerlendirme yapıldı mı?
- ☐ Sorumlu kişiler bilgilendirildi mi?

İlk 72 Saat

- ☐ Bildirim yükümlülükleri değerlendirildi mi?
- ☐ İlgili kişiler üzerindeki etkiler analiz edildi mi?
- ☐ Düzeltici önlemler planlandı mı?
- ☐ Olay raporu hazırlandı mı?

Ek 9 – Yıllık KVKK Uyum Denetimi

Her kurum yılda en az bir kez aşağıdaki hususları gözden geçirmelidir.

- ☐ Aydınlatma metinleri güncel mi?
- ☐ Açık rıza süreçleri gözden geçirildi mi?
- ☐ Saklama süreleri kontrol edildi mi?
- ☐ Süresi dolan kayıtlar imha edildi mi?
- ☐ Veri güvenliği tedbirleri güncellendi mi?
- ☐ Personel eğitimleri tekrarlandı mı?
- ☐ Veri işleyenlerle yapılan sözleşmeler gözden geçirildi mi?
- ☐ Yapay zekâ ve dijital sistemler yeniden değerlendirildi mi?
- ☐ Web sitesi ve takip teknolojileri kontrol edildi mi?
- ☐ Veri ihlali müdahale planı güncellendi mi?

Ek 10 – Beş Temel Yönetici Sorusu

Her veri sorumlusu aşağıdaki sorulara açık ve net cevap verebilmelidir:

1. **Hangi verileri işliyorum?**
2. **Bu verileri neden işliyorum?**
3. **Kimler bu verilere erişebiliyor?**
4. **Verileri ne kadar süre saklıyorum?**
5. **Veri ihlali yaşanırsa ne yapacağım?**

Bu soruların cevaplandırılamadığı durumlarda veri koruma uyum süreçlerinin yeniden değerlendirilmesi gerekir. Başarılı bir veri koruma programı yalnızca hukuki bilgiye değil; teknik güvenlik önlemlerine, kurumsal disipline, çalışan farkındalığına ve düzenli denetime dayanır. Ruh sağlığı alanında faaliyet gösteren meslek mensupları bakımından kişisel verilerin korunması, yalnızca yasal bir yükümlülük değil; danışan güveninin ve mesleki itibarın korunmasının da temel unsurlarından biridir.