



İlk Yayın: 5 Ocak 2017
Sürüm: 2.0
Son Güncelleme: Eylül 2026
Onaylayan Organ: Genel Kurul
Gözden Geçirme: Her yıl Kasım

Veri ve Dijital Güvenlik Politikası

1. Politika Beyanı

Özürlüler Vakfı; faaliyetleri sırasında oluşturduğu, elde ettiği, kullandığı, paylaştığı ve sakladığı bilgi, belge, kayıt ve kişisel verilerin korunmasını; kişilerin temel hak ve özgürlüklerine saygının, kurumsal güvenin, şeffaflığın ve hesap verebilirliğin ayrılmaz bir parçası olarak kabul eder.

Vakıf, bilgi ve veriyi yalnızca korunması gereken bir kurumsal varlık olarak değil, doğru ve sorumlu biçimde yönetilmesi gereken bir emanet olarak ele alır. Kişisel verilerin ve özellikle sağlık bilgileri ile diğer özel nitelikli kişisel verilerin işlenmesinde insan onuru, mahremiyet, bireysel irade ve kişilerin kendi bilgileri üzerindeki hakları gözetilir.

Kişisel veriler hukuka ve dürüstlük kurallarına uygun, belirli, açık ve meşru amaçlarla; işlendikleri amaçla bağlantılı, sınırlı ve ölçülü biçimde işlenir. Bir faaliyetin yürütülmesi için gerekli olmayan kişisel verilerin toplanmaması, kişisel verilerin ileride kullanılabileceği düşüncesiyle gereğinden fazla tutulmaması ve işleme amacı sona erdiğinde mevzuata ve kurumsal saklama esaslarına uygun biçimde silinmesi, yok edilmesi veya anonim hâle getirilmesi esastır.

Vakıftan destek veya hizmet talep edilmesi, bir programa ya da faaliyete katılınması veya Vakıfla başka bir ilişki kurulması; kişinin bilgilerinin sınırsız biçimde toplanmasına, kullanılmasına, açıklanmasına, yayımlanmasına veya üçüncü kişilerle paylaşılmasına izin verdiği anlamına gelmez. Sağlanan destek ve hizmetler, hukuken veya hizmetin niteliği gereği zorunlu olmayan kişisel verilerin verilmesine ya da kişinin fotoğrafının, görüntüsünün, sesinin veya hikâyesinin iletişim amacıyla kullanılmasına bağlanamaz.

Bilgi güvenliği yalnızca bilgisayar sistemlerinin korunmasından ibaret değildir. Fiziki dosyalar, sözleşmeler, yazışmalar, başvuru formları, sağlık raporları, bağışçı ve gönüllü kayıtları, çalışan kayıtları, hukuki ve mali belgeler, fotoğraf, video ve ses kayıtları, e-postalar, veri tabanları, çevrim içi formlar, taşınabilir cihazlar, bulut hizmetleri, yedekler ve Vakıf faaliyetleri kapsamında oluşturulan veya edinilen diğer kayıtlar bu Politika'nın koruma yaklaşımının parçasıdır.

Vakıf, bilgi ve kayıtların gizliliğini, bütünlüğünü, doğruluğunu, erişilebilirliğini ve izlenebilirliğini korumayı; yetkisiz erişim, kayıp, değiştirme, tahrif, açıklama, imha ve kötüye kullanım risklerini azaltmayı esas alır. Bu amaçla bilginin niteliği, işlenen verilerin hassasiyeti, kullanılan sistemler ve ortaya çıkabilecek risklerle orantılı idari, fiziki ve teknik tedbirler alınır.

Bilgi ve veri güvenliğinin yalnızca teknik bir görev olmadığı kabul edilir. Yönetim organlarından çalışanlara, gönüllülerden danışman ve hizmet sağlayıcılara kadar Vakıf adına bilgiye veya verilere erişen herkes, kendi görev ve yetkisi ölçüsünde bu bilgilerin korunmasından sorumludur.

2. Amaç ve Kapsam

Bu Politika'nın amacı; Özürlüler Vakfı'nın faaliyetleri kapsamında üretilen, edinilen veya işlenen kurumsal bilgi ve belgelerin, kişisel verilerin, özel nitelikli kişisel verilerin, fiziki ve elektronik kayıtların ve dijital sistemlerin oluşturulmasından veya elde edilmesinden güvenli biçimde imha edilmesine kadar bütün yaşam döngüsünü düzenleyen ortak kurumsal esasları belirlemektir.

Politika; bilgi ve verinin toplanması, oluşturulması, kaydedilmesi, sınıflandırılması, kullanılması, güncellenmesi, erişilmesi, paylaşılması, aktarılması, saklanması, arşivlenmesi, yedeklenmesi, geri yüklenmesi, silinmesi, yok edilmesi ve anonim hâle getirilmesine ilişkin süreçleri kapsar.

Bu kapsamda Politika;

Vakfın yönetim ve denetim organlarını, çalışanlarını, gönüllülerini ve stajyerlerini;

Vakıf adına görev yapan veya Vakfı temsil eden kişileri; danışmanları, hizmet sağlayıcıları, tedarikçileri ve yüklenicileri, Vakfın bilgi, belge, kişisel veri veya dijital sistemlerine erişimleri ölçüsünde;

Vakıfla ortak faaliyet yürüten kişi, kurum ve kuruluşları, üstlendikleri görev ve erişim düzeyi ölçüsünde kapsar.

Politika; çalışanlar, gönüllüler, bağışçılar, destek veya hizmet başvurusunda bulunan kişiler, destek alan kişiler, çocuklar, aileler, bakım sorumluluğu üstlenen kişiler, etkinlik ve program katılımcıları, tedarikçiler, iş birliği yapılan kuruluşların temsilcileri ve Vakıfla ilişki kuran diğer gerçek kişilere ait kişisel verilerin işlenmesine uygulanır.

Kurumsal bilgi bakımından ise Vakfın idari, mali, hukuki, yönetsel, proje, saha, bağış, gönüllülük, insan kaynakları, iletişim ve savunuculuk faaliyetleri sonucunda oluşturulan veya dışarıdan edinilen her türlü belge ve kayıt kapsam dâhilindedir.

Politikanın kapsamı yalnızca elektronik ortamdaki bilgilerle sınırlı değildir. Basılı belgeler ve fiziki arşivler ile elektronik dosyalar, e-postalar, veri tabanları, bulut ortamları, mobil cihazlar ve diğer dijital kayıt ortamları aynı bilgi yönetimi ve güvenlik yaklaşımı içinde değerlendirilir.

Vakıf adına hizmet sunan bir üçüncü tarafın bilgi veya kişisel veri işlemesi, Vakfın mevzuattan ve bu Politikadan doğan sorumluluklarını ortadan kaldırmaz. Üçüncü tarafların erişimi, sunulan hizmet için gerekli bilgi ve verilerle sınırlandırılır ve bu taraflardan uygun gizlilik ve güvenlik yükümlülüklerine uymaları beklenir.

3. Hukuki Çerçeve ve Temel İlkeler

Bu Politika başta Türkiye Cumhuriyeti Anayasası ve 6698 sayılı Kişisel Verilerin Korunması Kanunu olmak üzere, Vakfın faaliyetlerine uygulanabilir yürürlükteki ulusal mevzuat ile Kişisel Verileri Koruma Kurulu tarafından yayımlanan düzenleme ve kararlar çerçevesinde uygulanır.

Kişisel verilerin işlenmesi, özel nitelikli kişisel verilerin korunması, aydınlatma yükümlülüğü, ilgili kişinin hakları, veri güvenliği, kişisel verilerin yurt içinde ve yurt dışına aktarılması ile kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi konularında yürürlükte bulunan güncel mevzuat esas alınır.

Uluslararası veri koruma, bilgi güvenliği ve kayıt yönetimi standartları ile sivil toplum alanındaki iyi uygulamalar; Türk hukukunun yerine geçmemek, Vakfın yapısına uygun olmak ve kişilerin haklarının korunmasını güçlendirmek kaydıyla yol gösterici olarak dikkate alınabilir.

Vakıf bilgi ve veri yönetiminde aşağıdaki temel ilkeleri benimser:

Hukuka uygunluk ve dürüstlük: Bilgi ve kişisel veriler hukuka, dürüstlük kurallarına ve bu Politikanın amaçlarına uygun biçimde yönetilir.

Belirli amaç ve amaçla sınırlılık: Kişisel veriler belirli, açık ve meşru amaçlar için işlenir. Bir amaç için elde edilen verinin farklı bir amaçla kullanılması gerektiğinde yeni kullanımın hukuki dayanağı ayrıca değerlendirilir.

Gerektiği kadar veri: Bir faaliyetin yürütülmesi için gerekli olmayan kişisel veri talep edilmez. Formlar ve veri toplama süreçleri, artık ihtiyaç duyulmayan bilgi alanlarının kaldırılması amacıyla belirli aralıklarla gözden geçirilir.

Doğruluk ve güncellik: Kullanım amacı bakımından gerekli olduğu ölçüde bilgi ve kişisel verilerin doğru ve güncel tutulması gözetilir.

Saklama süresiyle sınırlılık: Bilgi ve kişisel veriler, mevzuatın veya meşru kurumsal amacın gerektirdiğinden daha uzun süre tutulmaz. Kurumsal hafıza niteliğindeki kayıtlarla kişisel verilerin saklanması arasındaki farklılıklar ayrıca değerlendirilir.

Gizlilik ve mahremiyet: Bilgiye erişim, kişinin görevi ve yetkisiyle sınırlandırılır. Özellikle sağlık bilgileri, özel nitelikli kişisel veriler, destek başvuruları, koruma kayıtları, hukuki dosyalar ve benzeri hassas kayıtlar bakımından daha yüksek koruma uygulanır.

Bütünlük, özgünlük ve izlenebilirlik: Kurumsal kayıtların yetkisiz biçimde değiştirilmesi, tahrif edilmesi veya yok edilmesi önlenir. Kayıtların kaynağının, tarihinin, ilgili sürecinin ve gerektiğinde sürümünün izlenebilir olması gözetilir.

Görev kadar erişim: Bir kişinin bir sisteme veya dosyaya teknik olarak erişebiliyor olması, o bilgiyi inceleme, kullanma veya paylaşma yetkisine sahip olduğu anlamına gelmez.

Riskle orantılı güvenlik: Alınacak güvenlik tedbirleri; bilginin niteliği, verinin hassasiyeti, erişim biçimi, kullanılan teknoloji ve kişilere doğabilecek zarar dikkate alınarak belirlenir. KVKK'nın 12. maddesi çerçevesinde veri sorumlusunun hukuka aykırı işlemeyi ve erişimi önlemek ve verilerin muhafazasını sağlamak üzere gerekli teknik ve idari tedbirleri alma yükümlülüğü bulunmaktadır.

Hesap verebilirlik: Vakıf, yalnızca kurallar koymayı değil; bu kuralların uygulanmasını, erişimlerin ve risklerin gerektiğinde gözden geçirilmesini, ihlallerin değerlendirilmesini ve gerekli düzeltici tedbirlerin alınmasını da bilgi ve veri yönetiminin parçası kabul eder.

Erişilebilirlik: Kişilerin kendi kişisel verileri hakkında bilgilendirilmesi, haklarını kullanması ve başvuruda bulunması süreçlerinin engelli bireyler bakımından erişilebilir olması gözetilir.

İnsan onuru ve zarar vermeme: Bilgi ve verinin kullanılması kişinin damgalanmasına, gereksiz biçimde teşhir edilmesine, ayrımcılığa uğramasına veya haklarına erişiminin engellenmesine yol açacak biçimde gerçekleştirilemez.

Bu ilkeler, kişisel verilerin yanı sıra Vakfın kurumsal bilgi ve kayıtlarının yönetiminde de bilginin niteliğine uygun olduğu ölçüde uygulanır.

4. Bilgi, Belge ve Kayıt Yönetimi

Özürlüler Vakfı; faaliyetleri kapsamında oluşturulan veya edinilen bilgi, belge ve kayıtları kurumsal hafızanın, hukuki güvencenin, şeffaflığın ve hesap verebilirliğin temel unsurları olarak kabul eder. Kurumsal kayıtlar, oluşturuldukları veya Vakfa ulaştıkları andan saklama sürelerinin sona ermesine ve gerektiğinde güvenli biçimde imha edilmelerine kadar bütün yaşam döngüsü boyunca düzenli, güvenilir, erişilebilir ve güvenli biçimde yönetilir.

Bu kapsam; yazışmaları, sözleşmeleri, kararları, toplantı ve Genel Kurul kayıtlarını, mali ve hukuki belgeleri, proje ve faaliyet kayıtlarını, destek başvurularını, bağışçı ve gönüllü kayıtlarını, çalışanlara ilişkin belgeleri, raporları, araştırmaları, fotoğraf, video ve ses kayıtlarını, e-postaları, veri tabanlarını ve Vakfın faaliyetleri sonucunda oluşan diğer fiziki veya dijital kayıtları kapsar.

4.1. Kurumsal kayıt ve kurumsal hafıza

Vakıf adına veya Vakıf faaliyetleri kapsamında oluşturulan ve kurumsal nitelik taşıyan kayıtlar, ilgili mevzuat ve sözleşme hükümleri saklı kalmak kaydıyla Vakfın kurumsal kayıt sisteminin parçasıdır.

Kurumsal kayıtların yalnızca bir çalışanın, gönüllünün veya yöneticinin kişisel cihazında, şahsi e-posta hesabında veya Vakıf tarafından onaylanmamış bir depolama alanında kalıcı olarak tutulmaması esastır. Faaliyetin yürütülmesi sırasında bu tür ortamlarda geçici olarak oluşturulması zorunlu olan kurumsal kayıtlar, gerekli güvenlik önlemleri alınarak mümkün olan en kısa sürede Vakfın onaylı kurumsal sistemine aktarılır.

Görev değişikliği veya Vakıfla ilişkin sona ermesi hâlinde, kişinin sorumluluğunda bulunan kurumsal bilgi ve kayıtların eksiksiz biçimde devredilmesi ve artık gerekli olmayan erişim yetkilerinin kaldırılması sağlanır.

4.2. Özgünlük, bütünlük ve izlenebilirlik

Kurumsal bilgi ve belgelerin özgünlüğü, bütünlüğü ve güvenilirliği korunur. Kayıtların yetkisiz biçimde değiştirilmesi, tahrif edilmesi, gizlenmesi veya yok edilmesi kabul edilmez.

Belgenin niteliğinin gerektirdiği durumlarda kaynağı, oluşturulma veya alınma tarihi, ilgili faaliyet veya işlem, güncel sürümü ve yapılan önemli değişiklikler izlenebilir olmalıdır. Aynı belgenin farklı ve kontrolsüz sürümlerinin kullanılmasından doğabilecek riskleri azaltacak kurumsal dosyalama ve sürüm yönetimi yöntemleri uygulanır.

Resmî, hukuki, mali veya kurumsal karar niteliğindeki kayıtların bütünlüğünü ve gerektiğinde doğrulanabilirliğini sağlayacak uygun kayıt düzeni oluşturulur.

4.3. Bilginin sınıflandırılması

Bilgi ve belgeler, içerdikleri bilginin niteliği, açıklanmasının doğurabileceği risk, kişisel veri içerip içermediği ve erişim ihtiyacı dikkate alınarak uygun erişim ve güvenlik düzeyleriyle yönetilir.

Bu kapsamda kayıtlar genel olarak kamuya açık, kurum içi, gizli ve hassas/özel koruma gerektiren kayıtlar olarak değerlendirilebilir.

Faaliyet raporları, kamuoyu duyuruları, yayımlanmış araştırmalar ve internet sitesinde yayımlanması onaylanmış içerikler kamuya açık olabilir. Kurum içi çalışma belgeleri ve henüz yayımlanmamış kurumsal içerikler yalnızca görev amacıyla kullanılabilir.

Sözleşmeler, ayrıntılı mali kayıtlar, çalışan ve gönüllü özlük bilgileri, bağışçı kayıtları, hukuki dosyalar ve benzeri bilgiler yetkisiz kişilerle paylaşılmaz.

Sağlık verileri, sağlık raporları, engellilik durumuna ilişkin sağlık bilgileri, koruma ve hak ihlali bildirimleri, çocuklara ilişkin hassas kayıtlar ve diğer özel nitelikli kişisel veriler ise taşıdıkları riskle orantılı olarak daha yüksek erişim ve güvenlik tedbirlerine tabi tutulur.

Bilginin “gizli” veya “hassas” olarak sınıflandırılması, ona hiç kimsenin erişemeyeceği anlamına gelmez; erişimin yalnızca görevi gereği bu bilgiye ihtiyaç duyan kişilerle ve gerekli kapsamla sınırlandırılması anlamına gelir.

4.4. Fiziki ve dijital kayıtların yönetimi

Fiziki kayıtlar kayıp, zarar, yangın, su, nem, hırsızlık ve yetkisiz erişim riskleri dikkate alınarak uygun ortamlarda saklanır. Özellikle kişisel veri, özel nitelikli kişisel veri veya gizli kurumsal bilgi içeren dosyaların erişimi sınırlandırılır.

Fiziki arşivden çıkarılan önemli veya hassas belgelerin kim tarafından ve hangi amaçla alındığının gerektiğinde izlenebilmesini sağlayacak kayıt yöntemleri kullanılabilir.

Dijital kayıtlar, Vakfın onayladığı kurumsal sistemlerde, sunucularda veya bulut hizmetlerinde tutulur. Dosya yapıları, adlandırma yöntemleri ve erişim yetkileri; kayıtların bulunabilirliğini, doğru sürümün kullanılmasını ve kurumsal hafızanın korunmasını sağlayacak biçimde düzenlenir.

Kurumsal kayıtların kişisel mesajlaşma uygulamaları, kişisel e-posta hesapları veya onaylanmamış dosya paylaşım hizmetleri üzerinden sürekli ve kontrolsüz biçimde saklanmaması esastır.

5. Kişisel Verilerin İşlenmesi ve Korunması

Özürlüler Vakfı, faaliyetlerini yürütürken kişisel verileri yalnızca yürürlükteki mevzuatta öngörülen hukuki şartlardan birinin bulunması ve belirli bir kurumsal amacın gerektirmesi hâlinde işler.

Her veri işleme faaliyetinde; hangi kişisel verinin neden gerekli olduğu, hangi amaçla kullanılacağı, hangi hukuki işleme şartına dayanıldığı, kimlerin erişimine açık olacağı, gerekli olup olmadığı, ne kadar süre saklanacağı ve gerektiğinde kimlerle paylaşılabilceği değerlendirilir.

Kişisel verilerin hukuka uygun biçimde elde edilmiş olması, bu verilerin Vakıf içinde sınırsız kullanılabileceği veya üçüncü kişilerle serbestçe paylaşılabilceği anlamına gelmez.

5.1. Veri minimizasyonu ve amaçla sınırlılık

Vakıf, faaliyet için gerekli olan kişisel verilerle yetinir. “İleride gerekebilir” düşüncesi tek başına kişisel veri toplamak veya mevcut veriyi süresiz saklamak için yeterli kabul edilmez.

Destek, bağış, gönüllülük, çalışan, etkinlik, araştırma ve diğer başvuru formlarında talep edilen kişisel veriler, yürütülen faaliyetin gerçek ihtiyacıyla sınırlı olmalıdır.

Formlar ve veri toplama yöntemleri belirli aralıklarla gözden geçirilir; artık gerekli olmayan veri alanları kaldırılır.

Bir amaç için elde edilen kişisel verinin farklı bir amaçla kullanılmasının planlanması hâlinde, yeni kullanımın hukuki dayanağı ve ilgili kişiye yapılması gereken bilgilendirme ayrıca değerlendirilir.

Örneğin bir kişinin destek başvurusu kapsamında Vakfa verdiği sağlık veya iletişim bilgilerinin bulunması, bu bilgilerin kendiliğinden bağış kampanyası, tanıtım, kamuoyu iletişimi veya farklı bir proje amacıyla kullanılabileceği anlamına gelmez.

5.2. Kişisel verilerin doğruluğu ve güncelliği

Kişisel verilerin kullanım amacı bakımından doğru ve gerektiğinde güncel olması gözetilir. Yanlış veya güncelliğini yitirmiş bir bilginin kişi bakımından hak kaybına, yanlış değerlendirmeye veya hizmete erişimde soruna yol açabileceği durumlarda gerekli düzeltmeler öncelikle ele alınır.

İlgili kişinin verisinin düzeltilmesi veya güncellenmesi yönündeki talepleri, yürürlükteki mevzuat ve Vakfın ilgili süreçleri doğrultusunda değerlendirilir.

5.3. Açık rızanın veri işlemenin genel şartı olarak kullanılmaması

Açık rıza, kişisel veri işlemenin tek ve genel hukuki dayanağı değildir. Kanunda başka bir kişisel veri işleme şartının bulunduğu durumlarda açık rıza, gereksiz veya zorunlu bir izin yöntemi olarak kullanılmaz.

Açık rızanın hukuken gerekli olduğu durumlarda rızanın belirli bir konuya ilişkin, yeterli bilgilendirmeye dayanan ve kişinin özgür iradesiyle açıklanan bir irade beyanı olması gerekir.

Bir kişinin Vakıftan destek alması, bir programa katılması veya bir hizmetten yararlanması, hizmetin sunulması için gerekli olmayan kişisel verilerin işlenmesine rıza göstermesine bağlanamaz.

6. Özel Nitelikli Veriler, Sağlık, Engellilik ve Destek Kayıtları

Özürlüler Vakfının faaliyet alanı nedeniyle sağlık bilgileri, sağlık raporları, engellilik durumuna ilişkin sağlık verileri, rehabilitasyon ihtiyaçları, kullanılan yardımcı cihazlara ilişkin bilgiler ve kişilerin destek ihtiyaçlarını ortaya koyabilecek diğer kayıtlar işlenebilir.

Bu bilgilerin kişilerin mahremiyeti, ayrımcılığa uğrama riski ve haklara erişimi bakımından taşıdığı hassasiyet dikkate alınarak, gerekli olduğu ölçüde daha yüksek koruma uygulanır.

6.1. Özel nitelikli kişisel veriler

6698 sayılı Kanunda özel nitelikli kişisel veri olarak belirlenen veriler yalnızca Kanunun güncel hükümlerinde öngörülen şartlardan birinin bulunması hâlinde işlenir ve bu verilerin korunmasında mevzuatın gerektirdiği ek tedbirler alınır.

Özel nitelikli verilere erişim, görevin gerektirdiği kişiler ve gerekli bilgiyle sınırlandırılır.

6.2. Engellilik ve sağlık bilgileri

Engelliliğe ilişkin her bilgi kendiliğinden sağlık verisi veya özel nitelikli kişisel veri olarak değerlendirilmez. Ancak kişinin teşhisini, sağlık durumunu, tedavisini, sağlık raporunu veya sağlık durumuna ilişkin başka bir bilgiyi ortaya koyan engellilik verileri, sağlık verisi niteliği taşıdığı ölçüde özel nitelikli kişisel verilere ilişkin hükümlere tabidir.

Bir kişinin engelli olduğunun bilinmesi, onun sağlık geçmişine, raporlarına, teşhisine, kullandığı ilaçlara veya diğer kişisel bilgilerine sınırsız erişim hakkı doğurmaz.

Sağlık raporu, teşhis veya tedavi bilgisi yalnızca ilgili faaliyetin gerçekten gerektirdiği ölçüde talep edilir. Bir desteğin değerlendirilmesi için raporun tamamına ihtiyaç bulunmuyorsa gereksiz sağlık bilgilerinin toplanmasından kaçınılır.

6.3. Destek başvuruları

Vakıftan sağlık, rehabilitasyon, mobilite, temel ihtiyaç veya başka bir alanda destek isteyen kişilerden yalnızca başvurunun değerlendirilmesi, desteğin sağlanması, yasal yükümlülüklerin yerine getirilmesi ve gerekli kayıtların tutulması için ihtiyaç duyulan bilgiler alınır.

Kişinin ihtiyaç sahibi olması veya Vakıftan destek talep etmesi, mahremiyet hakkını azaltmaz.

Başvuru sırasında edinilen sağlık, ekonomik durum, aile yapısı, engellilik veya diğer kişisel bilgiler; hukuki dayanak bulunmaksızın kişinin kamuya açık biçimde tanıtılması, bağış kampanyasında kullanılması veya hikâyesinin paylaşılması amacıyla kullanılamaz.

6.4. Çocuklara ve koruma kapsamındaki kişilere ait veriler

Çocuklara ve Koruma Politikası kapsamında özel dikkat gerektiren kişilere ilişkin kişisel verilerin işlenmesinde, verinin açıklanmasının veya yanlış kullanılmasının kişiye verebileceği zarar özellikle değerlendirilir.

Bu kişilere ait sağlık kayıtları, koruma bildirimleri, fotoğraflar, görüntüler, iletişim bilgileri ve diğer hassas kayıtlar yalnızca görevi gereği erişmesi gereken kişiler tarafından ve gerekli ölçüde kullanılabilir.

Veri koruma gerekçesi kişinin iradesini yok saymak için kullanılamayacağı gibi, engellilik de kişinin kendi bilgileri hakkında bilgilendirilmemesi veya mümkün olduğu ölçüde sürece katılmaması için tek başına gerekçe oluşturmaz.

7. Aydınlatma, Açık Rıza ve İlgili Kişinin Hakları

Özürlüler Vakfı, kişisel verilerin işlenmesinde şeffaflığı esas alır. Kişisel verilerin elde edilmesi sırasında ilgili kişiler, 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında gerekli hususlarda açık ve anlaşılır biçimde bilgilendirilir.

Aydınlatma yükümlülüğü; kişisel verilerin hangi amaçlarla işlendiği, hangi hukuki sebeplere dayandığı, kimlere ve hangi amaçlarla aktarılabileceği, veri toplamanın yöntemi ve ilgili kişinin hakları konusunda gerekli bilgilerin verilmesini kapsar.

Bilgilendirmenin yalnızca hukuki bir metnin sunulmasından ibaret olmadığı kabul edilir. Bilginin ilgili kişi tarafından mümkün olduğu ölçüde anlaşılabilir ve erişilebilir olması gözetilir.

7.1. Aydınlatma ve açık rızanın ayrılığı

Aydınlatma yükümlülüğü ile açık rıza birbirinden ayrı süreçlerdir. İlgili kişinin bilgilendirilmesi, ondan her durumda açık rıza alınması gerektiği anlamına gelmez.

Açık rıza ancak kişisel veri işleme faaliyetinin hukuken açık rızaya dayanması gereken durumlarda kullanılır. Kanunda başka bir işleme şartının bulunduğu durumlarda açık rıza, veri işlemenin genel veya zorunlu şartı hâline getirilmez.

Açık rızaya dayanan hâllerde rıza belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan bir irade beyanı olmalıdır.

7.2. İlgili kişinin hakları

Kişisel verisi Vakıf tarafından işlenen kişiler, 6698 sayılı Kanun ve ilgili mevzuat kapsamında kendilerine tanınan hakları kullanabilir.

Bu kapsamda ilgili kişi; kişisel verisinin işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgi talep etme, işlenme amacını ve amacına uygun kullanılıp kullanılmadığını öğrenme, verinin aktarıldığı üçüncü kişileri bilme, eksik veya yanlış işlenmiş verilerin düzeltilmesini isteme ve Kanunda öngörülen şartların oluşması hâlinde kişisel verilerin silinmesini veya yok edilmesini talep etme haklarına sahiptir.

Kanunda öngörülen diğer haklar da ilgili kişilerin kullanımına açıktır. Başvurular yürürlükteki mevzuatta belirlenen usul ve süreler çerçevesinde değerlendirilir.

7.3. Hakların erişilebilir biçimde kullanılabilmesi

Vakıf, kişisel verilerin korunmasına ilişkin bilgilendirme ve başvuru yollarının engelli bireyler tarafından kullanılabilir olmasını gözetir.

Kişinin iletişim veya erişim ihtiyacının bulunması, veri koruma haklarını kullanmasını engellememelidir. Gerektiğinde erişilebilir iletişim yöntemleri ve makul düzenlemeler sağlanır.

Engellilik, kişinin kendi kişisel verileri hakkında bilgilendirilmemesi veya karar süreçlerinden otomatik olarak dışlanması için gerekçe oluşturmaz.

8. Erişim, Yetkilendirme, Gizlilik ve Bilgi Paylaşımı

Vakıf bünyesindeki kişisel verilere, kurumsal bilgilere ve dijital sistemlere erişim görevin gerektirdiği ölçüyle sınırlandırılır. Bir kişinin bilgiye teknik olarak erişebiliyor olması, o bilgiyi inceleme, kullanma, kopyalama, indirme, değiştirme veya paylaşma yetkisine sahip olduğu anlamına gelmez.

8.1. Erişim ve yetkilendirme

Kullanıcı hesapları ve erişim yetkileri kişiye ve göreve özgü olarak belirlenir. Parolalar ve diğer kimlik doğrulama bilgileri başkalarıyla paylaşılmaz.

Sağlık verileri, özel nitelikli kişisel veriler, destek dosyaları, çalışan kayıtları, koruma bildirimleri, hukuki dosyalar ve benzeri hassas bilgilere daha sınırlı erişim uygulanır.

Görev veya sorumluluğun değişmesi hâlinde erişim yetkileri yeniden değerlendirilir. Çalışma, gönüllülük, danışmanlık veya hizmet ilişkisi sona eren kişilerin artık ihtiyaç duyulmayan sistem ve dosya erişimleri gecikmeksizin kaldırılır.

8.2. Gizlilik yükümlülüğü

Vakıf adına kişisel verilere veya gizli kurumsal bilgilere erişen kişiler, bu bilgileri yalnızca görevlerinin gerektirdiği amaçlarla kullanabilir.

Bilgilerin merak, kişisel ilişki, özel çıkar veya görev dışı başka bir amaçla incelenmesi veya kullanılması kabul edilmez.

Gizlilik yükümlülüğü kişinin Vakıftaki görevinin veya Vakıfla ilişkisinin sona ermesiyle ortadan kalkmaz.

8.3. Kurum içi bilgi paylaşımı

Vakıf içinde bilgi paylaşımı da ihtiyaçla sınırlıdır. Bir çalışanın veya yönetim organı üyesinin Vakıf bünyesinde bulunması, tüm kurumsal bilgilere veya kişisel verilere erişebileceği anlamına gelmez.

Bilgi, ilgili görevin yerine getirilmesi için gerçekten ihtiyaç duyan kişilerle ve gerekli kapsamda paylaşılır.

9. Veri Paylaşımı, Hizmet Sağlayıcılar ve Yurt Dışına Aktarım

Kişisel verilerin Vakıf tarafından hukuka uygun biçimde elde edilmiş olması, bunların başka kişi veya kuruluşlara serbestçe aktarılabilmesi anlamına gelmez.

Her veri aktarımında aktarımın amacı, alıcısı, kapsamı, hukuki dayanağı, aktarılabilecek veri miktarı ve doğurabileceği riskler değerlendirilir. Paylaşım, amacın gerektirdiği bilgiyle sınırlandırılır.

9.1. Yurt içinde veri paylaşımı

Kişisel verilerin üçüncü kişilere aktarılması yürürlükteki mevzuatta öngörülen şartlara uygun olarak gerçekleştirilir.

Kamu kurumları, sağlık kuruluşları, bankalar, mali müşavirler, hukuk danışmanları, proje ortakları, tedarikçiler veya diğer kuruluşlarla bilgi paylaşılması gerektiğinde yalnızca ilgili işlem için gerekli veriler paylaşılır.

Kanundan doğan bir yükümlülük veya yetkili makamın hukuka uygun talebi bulunması hâlinde yapılacak paylaşımlar ilgili mevzuat çerçevesinde gerçekleştirilir.

9.2. Hizmet sağlayıcılar ve veri işleyenler

Vakıf; bilgi teknolojileri, barındırma, bulut depolama, e-posta, yazılım, muhasebe, iletişim, araştırma veya benzeri hizmetler için üçüncü taraflardan hizmet alabilir.

Bir hizmet sağlayıcının Vakıf adına kişisel veri işlemesi veya kurumsal bilgilere erişmesi hâlinde, erişim sunulan hizmet için gerekli kapsamla sınırlandırılır.

Hizmet sağlayıcı seçiminde, işlenen bilginin niteliğine uygun güvenlik sağlayabilme kapasitesi dikkate alınır. Gerekli durumlarda sözleşmelerde veri güvenliği, gizlilik, erişim sınırları, verilerin yalnızca belirlenen amaçlarla kullanılması, alt hizmet sağlayıcılar, veri ihlallerinin bildirilmesi ve hizmet ilişkisinin sona ermesinden sonra verilerin iadesi veya güvenli biçimde silinmesine ilişkin yükümlülükler yer verilir.

Hizmetin üçüncü bir kuruluştan alınması, Vakfın kişisel verilerin korunmasına ilişkin kendi sorumluluklarını ortadan kaldırmaz.

9.3. Bulut, e-posta ve çevrim içi hizmetler

Bir verinin Vakıf merkezindeki bir bilgisayardan başka bir ülkeye fiziksel olarak gönderilmemesi, o verinin mutlaka Türkiye'de tutulduğu anlamına gelmez.

Bulut depolama, kurumsal e-posta, çevrim içi toplantı, dosya paylaşımı, internet sitesi altyapısı, form hizmetleri, yazılım uygulamaları ve benzeri dijital hizmetlerin kullanılması sırasında verilerin hangi ülkelerde işlendiği veya saklandığı gerektiğinde değerlendirilir.

Bu nedenle yeni bir dijital hizmet veya yazılım kullanıma alınırken, kişisel verilerin veya hassas kurumsal bilgilerin nerede ve hangi taraflarca işleneceği bilgi güvenliği ve veri koruma bakımından dikkate alınır.

9.4. Kişisel verilerin yurt dışına aktarılması

Kişisel verilerin yurt dışına aktarılmasında 6698 sayılı Kanunun 9. maddesinin yürürlükte bulunan güncel hükümleri uygulanır.

Yurt dışı aktarımının gerekli olduğu durumlarda aktarım; yeterlilik kararı, Kanunda öngörülen uygun güvenceler veya yalnızca Kanunun izin verdiği hâllerde uygulanabilecek istisnai aktarım şartları bakımından değerlendirilir.

Yurt dışına aktarım değerlendirmesi yalnızca doğrudan dosya gönderimini değil; yurt dışında barındırılan bulut, e-posta, yazılım, dosya paylaşımı ve benzeri hizmetlerin kullanımını da kapsar.

10. Arşiv, Dijital Sistemler ve Bilgi Güvenliği

Özürölüler Vakfı, bilgi güvenliğini yalnızca siber güvenlik veya teknik altyapı konusu olarak değerlendirmez. Fiziki kayıtların korunması, kullanıcı davranışları, erişim yetkileri, kullanılan cihazlar, yazılımlar, hizmet sağlayıcılar, yedekler ve çalışanların bilgi güvenliği farkındalığı aynı güvenlik yapısının parçalarıdır.

10.1. Fiziki arşiv güvenliği

Fiziki arşivler ve hassas belgeler; yetkisiz erişim, kayıp, çalınma, yangın, su, nem ve diğer öngörülebilir risklere karşı uygun biçimde korunur.

Özel nitelikli kişisel veri veya gizli kurumsal bilgi içeren belgeler, açık çalışma alanlarında veya yetkisiz kişilerin kolaylıkla erişebileceği ortamlarda bırakılmaz.

Arşivden alınan önemli belgelerin gerektiğinde kim tarafından, ne zaman ve hangi amaçla alındığının izlenebilmesini sağlayacak yöntemler uygulanır.

Fiziki arşivden çıkarılan önemli ve hassas belgelerin hareketlerinin izlenebilir olması sağlanır.

10.2. Dijital sistemlerin güvenliği

Vakıf, kullandığı sistemlerin niteliğine, işlenen bilgilerin hassasiyetine ve mevcut risklere uygun teknik ve idari güvenlik tedbirleri alır.

Bu tedbirler, ihtiyaç ve risk düzeyine göre; erişim kontrollerini, güçlü kimlik doğrulamayı, güncel yazılım kullanımını, zararlı yazılımlara karşı korumayı, güvenli bağlantıları, uygun yedeklemeyi, erişim ve olay kayıtlarının tutulmasını ve sistem güvenliğinin belirli aralıklarla gözden geçirilmesini içerebilir.

Güvenlik tedbirleri sabit bir teknik kontrol listesi olarak değerlendirilmez. Kullanılan teknolojinin ve risklerin değişmesi hâlinde alınan tedbirler de gözden geçirilir.

10.3. Cihazlar ve uzaktan erişim

Vakıf bilgilerine erişmek için kullanılan bilgisayar, telefon, tablet, taşınabilir bellek ve diğer cihazların kullanımında bilginin niteliğine uygun güvenlik tedbirleri uygulanır.

Hassas kişisel veya kurumsal bilgilerin yetkisiz kişilerin erişebileceği cihazlarda veya ortamlarda korunmasız biçimde saklanmaması esastır.

Uzaktan çalışma veya saha faaliyetleri, bilgi güvenliği yükümlülüklerini ortadan kaldırmaz.

10.4. Fotoğraf, video, ses ve kişisel hikâyeler

Fotoğraf, video, ses kaydı ve kişisel hikâyeler de içeriğine ve ilgili kişinin belirlenebilirliğine göre kişisel veri niteliği taşıyabilir.

Bu içeriklerin oluşturulması, saklanması, seçilmesi, paylaşılması ve yayımlanmasında kişinin mahremiyeti, onuru, güvenliği ve veri koruma hakları gözetilir.

Bir kişinin Vakıftan destek veya hizmet alması; fotoğrafının çekilmesini, görüntüsünün yayımlanmasını veya kişisel hikâyesinin kamuoyuyla paylaşılmasını kabul ettiği anlamına gelmez.

Özellikle sağlık durumu, engellilik, ekonomik koşullar, çocuklar veya koruma kapsamındaki hassas durumları ortaya çıkarabilecek içeriklerde açıklanacak bilgi miktarı ayrıca değerlendirilir.

Bu hükümler, Vakfın Medya Etiği Politikası ile birlikte uygulanır.

11. Saklama, Yedekleme ve Güvenli İmha

Özürölüler Vakfı; kişisel verileri, kurumsal bilgi ve belgeleri süresiz olarak saklamayı esas almaz. Bilgi ve kayıtların saklama süresi; ilgili mevzuat, hukuki yükümlülükler, sözleşmesel gereklilikler, işleme amacı, kurumsal hafıza değeri ve doğabilecek hukuki veya idari ihtiyaçlar dikkate alınarak belirlenir.

Kayıtların yalnızca “ileride gerekebilir” düşüncesiyle süresiz biçimde tutulmasından kaçınılır. Bununla birlikte, kişisel verilerin gereğinden uzun saklanmaması ilkesi ile Vakfın kurumsal hafızasının ve hukuki kayıtlarının korunması gerekliliği birlikte değerlendirilir.

11.1. Saklama süreleri

Belge ve veri kategorilerinin saklama süreleri, uygulanabilir mevzuat ve kurumsal ihtiyaçlar doğrultusunda hazırlanacak Saklama ve İmha Planı ile belirlenir.

Mali ve muhasebe kayıtları, çalışan kayıtları, sözleşmeler, Genel Kurul ve yönetim kayıtları, bağış ve proje belgeleri, destek başvuruları, sağlık belgeleri, hukuki dosyalar, kişisel veri içeren kayıtlar ve diğer kurumsal belgeler aynı süre boyunca saklanmak zorunda değildir.

Saklama süresinin belirlenmesinde ilgili kaydın hukuki niteliği, işleme amacı ve kurumsal değeri ayrı ayrı değerlendirilir.

Bir kişisel verinin saklanmasını gerektiren hukuki veya kurumsal neden ortadan kalktığında, verinin yalnızca teknik olarak sistemde bulunabiliyor olması saklamaya devam etmek için yeterli gerekçe oluşturmaz.

11.2. Yedekleme ve geri yükleme

Kurumsal bilgi ve dijital kayıtların kayıp, sistem arızası, insan hatası, zararlı yazılım, siber olay veya diğer öngörülebilir riskler nedeniyle geri döndürülemez biçimde kaybolmasını önlemek amacıyla uygun yedekleme yöntemleri uygulanır.

Yedeklerin kendileri de bilgi güvenliği ve kişisel veri koruma kurallarına tabidir. Yedekleme, artık saklanmaması gereken kişisel verilerin belirsiz süreyle tutulması için gerekçe olarak kullanılamaz.

Yedekleme sistemlerinin yalnızca oluşturulması değil, ihtiyaç hâlinde kayıtların geri yüklenebilmesini sağlayacak biçimde işler durumda tutulması ve uygun aralıklarla test edilmesi de gözetilir.

11.3. Silme, yok etme ve anonim hâle getirme

Kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması ve verinin saklanmasını gerektiren başka bir hukuki yükümlülüğün bulunmaması hâlinde kişisel veriler yürürlükteki mevzuata uygun olarak silinir, yok edilir veya anonim hâle getirilir.

Uygulanacak yöntem; verinin bulunduğu ortam, niteliği, hassasiyeti ve yeniden elde edilme riski dikkate alınarak belirlenir.

Fiziki belgeler, içerdikleri bilgilerin yetkisiz kişiler tarafından yeniden elde edilmesini önleyecek yöntemlerle imha edilir. Dijital kayıtların silinmesinde ise yalnızca görünür dosyanın kaldırılması değil, sistemin niteliği ve uygulanabilir teknik imkânlar dikkate alınır.

Anonim hâle getirilen verinin, başka bilgilerle birleştirilmesi yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilememesi gerekir.

11.4. Kurumsal arşiv değeri bulunan kayıtlar

Saklama süresinin sona ermesi, her kurumsal belgenin otomatik olarak imha edilmesi anlamına gelmez.

Vakfın kuruluşu, yönetimi, Genel Kurul kararları, önemli projeleri, araştırmaları, savunuculuk faaliyetleri, kurumsal gelişimi ve tarihsel hafızası bakımından kalıcı değer taşıyan kayıtların arşiv niteliği ayrıca değerlendirilir.

Ancak bir belgenin tarihsel veya kurumsal değer taşıması, içinde bulunan bütün kişisel verilerin sınırsız süreyle ve sınırsız erişimle tutulmasını kendiliğinden haklı kılmaz. Arşivleme amacı ile kişilerin mahremiyetinin korunması birlikte değerlendirilir.

12. Bilgi ve Veri Güvenliği İhlalleri, Görev ve Sorumluluklar

Özürlüler Vakfı, bilgi ve veri güvenliği ihlallerinin yalnızca teknik sistemlere yönelik siber saldırılardan ibaret olmadığını kabul eder.

Kişisel veya kurumsal bir belgenin kaybolması, yanlış kişiye e-posta gönderilmesi, bir dosyanın yetkisiz kişilerle paylaşılması, bir cihazın kaybolması veya çalınması, yetkisiz erişim, kayıtların değiştirilmesi veya silinmesi, parola veya erişim bilgilerinin açığa çıkması, kişisel verilerin yanlışlıkla yayımlanması veya benzeri olaylar bilgi veya veri güvenliği ihlali oluşturabilir.

12.1. İhlallerin bildirilmesi

Bilgi veya veri güvenliği ihlalinin ya da ciddi bir ihlal şüphesini fark eden kişi, durumu gecikmeksizin Vakfın belirlediği sorumlu kişiye veya uygun bildirim kanalına iletir.

Bildirimde bulunan kişinin olayın teknik veya hukuki niteliğini kesin olarak belirlemesi beklenmez. Şüpheli bir durumun zamanında bildirilmesi, olayın büyümesinin ve kişilere veya Vakfa daha fazla zarar vermesinin önlenmesi açısından önemlidir.

Bir ihlalin gizlenmesi, ilgili kayıtların yetkisiz biçimde değiştirilmesi veya silinmesi kabul edilmez.

12.2. İlk değerlendirme ve müdahale

Bir ihlal veya ihlal şüphesi öğrenildiğinde öncelikle olayın devam edip etmediği, hangi bilgi veya sistemlerin etkilendiği, kişisel veri içerip içermediği, etkilenen kişilerin kimler olduğu, verinin niteliği ve olayın doğurabileceği riskler değerlendirilir.

Mümkün olan durumlarda yetkisiz erişimin durdurulması, hatalı paylaşımın geri çekilmesi, erişim bilgilerinin değiştirilmesi, kayıp cihaz veya hesabın güvenliğinin sağlanması, etkilenen sistemlerin korunması ve benzeri acil tedbirler alınır.

Olayın nedeni, kapsamı, alınan tedbirler ve gerekli takip işlemleri uygun biçimde kayıt altına alınır.

12.3. Kişisel veri ihlalleri

Olay kişisel verilerin hukuka aykırı biçimde elde edilmesine, açıklanmasına, kaybedilmesine veya güvenliğinin başka biçimde tehlikeye girmesine yol açmışsa, olay ayrıca kişisel veri güvenliği ihlali olarak değerlendirilir.

Mevzuatın gerektirdiği durumlarda Kişisel Verileri Koruma Kuruluna ve etkilenen ilgili kişilere yapılması gereken bildirimler, yürürlükteki süre ve usullere uygun biçimde gerçekleştirilir.

12.4. Olaylardan öğrenme

Bilgi ve veri güvenliği ihlalleri yalnızca tekil olaylar olarak değerlendirilmez. Olayın nedeni ve tekrarını önlemek için gerekli olabilecek değişiklikler incelenir.

Gerekli görülmesi hâlinde erişim yetkileri, veri toplama yöntemleri, kullanılan sistemler, hizmet sağlayıcılar, saklama yöntemleri, eğitimler veya ilgili kurumsal süreçler gözden geçirilir.

Ihlallerden elde edilen kurumsal öğrenme, kişilerin mahremiyetini ve soruşturma veya değerlendirme süreçlerinin gizliliğini ihlal etmeyecek biçimde güvenlik uygulamalarının geliştirilmesinde kullanılabilir.

12.5. Yönetim Kurulu

Yönetim Kurulu, bu Politikanın kurumsal düzeyde uygulanmasının gözetilmesinden sorumludur.

Politikanın uygulanması için gerekli kurumsal düzenlemelerin yapılmasını, ciddi bilgi ve veri güvenliği risklerinin gerektiğinde değerlendirilmesini ve gerekli iyileştirmelerin gerçekleştirilmesini gözetir.

12.6. Çalışanlar, gönüllüler ve Vakıf adına görev yapan kişiler

Vakıf adına bilgi, belge, kişisel veri veya dijital sisteme erişen herkes;

yalnızca görevi için gerekli bilgilere erişmek,

bilgileri yalnızca yetkili amaçlarla kullanmak,

erişim bilgilerini korumak,

gizlilik ve mahremiyet kurallarına uymak,

kurumsal kayıtları uygun sistemlerde tutmak,

fark ettiği bilgi veya veri güvenliği ihlallerini gecikmeksizin bildirmek

konusunda kendi görev ve yetkisi ölçüsünde sorumludur.

Bu yükümlülüklerin bir kısmı, özellikle gizli bilgilerin yetkisiz açıklanmaması yükümlülüğü, kişinin Vakıfla ilişkisinin sona ermesinden sonra da devam eder.

12.7. Hizmet sağlayıcılar

Vakıf adına bilgi veya kişisel veri işleyen hizmet sağlayıcıların erişimleri sundukları hizmetle sınırlandırılır.

Hizmet sağlayıcılardan, eriştikleri bilgilerin niteliğine uygun güvenlik ve gizlilik tedbirleri almaları, bilgileri yetkisiz amaçlarla kullanmamaları ve Vakfı etkileyen önemli bir veri veya güvenlik ihlalini gecikmeksizin bildirmeleri beklenir.

13. Eğitim, İzleme ve Gözden Geçirme

Bu Politikanın etkili biçimde uygulanabilmesi için yalnızca yayımlanması yeterli kabul edilmez.

Kişisel verilere, hassas kurumsal bilgilere veya dijital sistemlere erişen çalışanlar, gönüllüler ve görevleri bakımından gerekli diğer kişiler; görevlerinin niteliğine uygun olarak veri koruma, gizlilik, bilgi güvenliği ve güvenli kayıt yönetimi konularında bilgilendirilir.

Özellikle sağlık ve engellilik verileri, destek dosyaları, çocuklara ilişkin kayıtlar, özel nitelikli kişisel veriler veya yüksek miktarda kişisel veri işleyen görevlerde bulunan kişilerin sorumluluklarına ilişkin bilgilendirmeye önem verilir.

Politikanın uygulanması; meydana gelen ihlaller, ortaya çıkan yeni riskler, kullanılan teknolojiler, hizmet sağlayıcı değişiklikleri, mevzuat ve Kişisel Verileri Koruma Kurulu düzenlemelerindeki gelişmeler dikkate alınarak izlenir.

Bu Politika her yıl Kasım ayında gözden geçirilir. Mevzuatta önemli bir değişiklik, ciddi bir veri güvenliği olayı veya Vakfın bilgi işleme faaliyetlerinde önemli bir değişiklik meydana gelmesi hâlinde yıllık gözden geçirme dönemi beklenmeden de değerlendirme yapılabilir.

14. Hukuki, Ulusal ve Uluslararası Dayanaklar

Bu Politika;

Türkiye Cumhuriyeti Anayasası,

6698 sayılı Kişisel Verilerin Korunması Kanunu,

kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin yürürlükteki düzenlemeler,

veri sorumlusuna başvuru usul ve esaslarına ilişkin yürürlükteki düzenlemeler,

özel nitelikli kişisel verilerin işlenmesine ve korunmasına ilişkin yürürlükteki düzenlemeler ve Kişisel Verileri Koruma Kurulu kararları,

kişisel verilerin yurt dışına aktarılmasına ilişkin yürürlükteki mevzuat ve Kurul düzenlemeleri,

Vakfın faaliyetleri bakımından uygulanabilir diğer ulusal mevzuat

çerçevesinde uygulanır.

Uluslararası insan hakları, kişisel verilerin korunması, bilgi güvenliği ve kayıt yönetimi alanındaki kabul görmüş ilkeler ve iyi uygulamalar, Türkiye'de yürürlükte bulunan mevzuatın yerine geçmemek kaydıyla, Vakfın bilgi ve veri yönetimi yaklaşımının geliştirilmesinde yol gösterici olarak dikkate alınabilir.

15. Yürürlük ve Gözden Geçirme

Bu Politika, Özürlüler Vakfı Genel Kurulu tarafından 15 Kasım 2016 tarihinde onaylanmış ve 5 Ocak 2017 tarihinde yayımlanarak yürürlüğe girmiştir.

Politikanın ikinci güncellemesi Şubat 2026 tarihinde yapılmış, yapılan son gözden geçirme ve düzenlemelerle Eylül 2026 tarihinde yeniden güncellenmiştir.

Politika her yıl Kasım ayında gözden geçirilir. Mevzuatta, Vakfın kurumsal yapısında veya uygulama ihtiyaçlarında önemli bir değişiklik meydana gelmesi hâlinde olağan gözden geçirme dönemi beklenmeden yeniden değerlendirilebilir.

Politikanın uygulanmasından Özürlüler Vakfı Yönetim Kurulu sorumludur. Politika, Vakfın internet sitesinde yayımlanır ve kapsamındaki kişilerin erişimine sunulur.

Politikada yapılacak değişiklikler Genel Kurulun onayıyla yürürlüğe girer.