



Bu proje Avrupa Birlięi tarafından finanse edilmektedir.
This project is funded by the European Union.

Sivil Toplum Destek Programı-III PAYDAŞLARLA GÜÇLÜ AĞLAR PROJESİ

STK'LAR İÇİN KVKK REHBERİ

2022



TÜRKİYE EĞİTİM GÖNÜLLÜLERİ VAKFI



“Bu yayın Avrupa Birliđinin maddi desteđi ile hazırlanmıřtır. İerik tamamıyla Trkiye Eđitim Gnllleri Vakfı sorumluluđu altındadır ve Avrupa Birliđinin grřlerini yansıtmak zorunda deđildir”

“This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of Trkiye Eđitim Gnllleri Vakfı and do not necessarily reflect the views of the European Union”

PAYDAŞLARLA GÜÇLÜ AĞLAR PROJESİ

STK'lar için KVKK Rehberi Hakkında

Türkiye'nin dört bir yanındaki binlerce çocuğu nitelikli eğitim ile buluşturmak amacıyla faaliyet gösteren Türkiye Eğitim Gönüllüleri Vakfı (TEGV), paydaşları ile mevcut ilişkisini geliştirmeye yönelik güçlü bir CRM (Bağışçı İlişkileri Yönetim Sistemi) altyapısı kurmak üzere, Sağlık ve Eğitim Vakfı (SEV) ve Koç Üniversitesi Sosyal Etki Forumu (KUSIF) ile birlikte ortak bir proje gerçekleştirdi.

T.C. Dışışleri Bakanlığı Avrupa Birliği Başkanlığı tarafından AB (Avrupa Birliği) desteğiyle uygulanan ve Sivil Toplum Destek Programı III kapsamında desteklenen “Paydaşlarla Güçlü Ağlar” isimli proje 01.04.2021 başlayıp 30.06.2022 tarihinde tamamlandı.

Bu Rehber “Paydaşlarla Güçlü Ağlar Projesi” kapsamında hazırlanmıştır. Rehber; Türkiye Eğitim Gönüllüleri Vakfı'nın katkılarıyla Çetinkaya Pehlivan Hukuk Bürosu tarafından hazırlanmıştır.

Rehber'in amacı, Sivil Toplum Kuruluşlarını KVKK konusunda genel kapsamda ve pratikte faydalı olacak şekilde bilgilendirmek ve yönlendirmektir.

Teşekkür

Rehberin hayata geçirilmesi için fırsat veren T.C. Dışışleri Bakanlığı Avrupa Birliği Başkanlığı ve Maliye Bakanlığı Merkezi Finans ve İhale Birimi'ne ve katkılarından dolayı TEGV Genel Müdürü Sn. Sait Tosyalı ve tüm TEGV Çalışanlarına ve Avukat Sn. Çağrı Çetinkaya'ya teşekkür ederiz.

İçindekiler

1. GİRİŞ VE AMAÇ	3
1.1 Giriş ve Amaç	4
1.2 Tanımlar	5
2. KİŞİSEL VERİLERİN İŞLENMESİ VE AKTARILMASI	5
2.1 Kişisel Verilerin İşlenmesinde Genel İlkeler	5
2.2 Özel Nitelikli Olmayan Kişisel Verilerin İşlenme Şartları	6
2.3 Özel Nitelikli Kişisel Verilerin İşlenme Şartları	6
2.4 Kişisel Verilerin Aktarılma Şartları	7
2.4.1 Yurtiçi Aktarım Şartları	7
2.4.2 Yurtdışına Aktarım Şartları	7
3. KİŞİSEL VERİLERİN İŞLENME VE AKTARILMA AMAÇLARI, AKTARILACAKI KİŞİLER	8
3.1 Kişisel Verilerin İşlenme ve Aktarılma Amaçları	8
3.2 Kişisel Verilerin Aktarılacağı Kişiler	8
4. KİŞİSEL VERİLERİN TOPLANMA YÖNTEMİ VE HUKUKİ SEBEBİ, SİLİNMESİ, YOK EDİLMESİ VE ANONİM HALE GETİRİLMESİ İLE SAKLANMA SÜRESİ	9
4.1 Kişisel Verilerin Silinmesi	9
4.2 Kişisel Verilerin Yok Edilmesi	9
4.3 Kişisel Verilerin Anonim Hale Getirilmesi	10
4.4 Kişisel Verilerin Saklanma Süreleri	11
5. TEKNİK İDARİ TEDBİRLER VE VERİ GÜVENLİĞİ	11
6. İLGİLİ KİŞİNİN HAKLARI, HAKLARIN KULLANILMASI VE DEĞERLENDİRİLMESİ	11
6.1 İlgili Kişinin Aydınlatılması	11
6.2 İlgili Kişinin KVKK Uyarınca Hakları	12
6.3 İlgili Kişinin Haklarını Kullanması	12
7. SİVİL TOPLUM KURULUŞLARINA YÖNELİK VERBİS KAYIT SİSTEMİ	13
8. KİŞİSEL VERİ MEVZUATINA UYUM HAKKINDA UYGULAMAYA YÖNELİK TAVSİYELER	14
EK-1	16
Veri Güvenliğine İlişkin Alınabilecek Örnek Tedbirler	16
EK-2	18
Kurul Tarafından Önerilen Teknik ve İdari Tedbirler	18
EK-3	19
Özel Nitelikli Kişisel Verilere İlişkin İlave Tedbirler	19

1. GİRİŞ VE AMAÇ

1.1 Giriş ve Amaç

İşbu Kişisel Verilerin Korunması ve İşlenmesi Rehberi ("**Rehber**") ile 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**KVKK**" veya "**Kanun**") uyarınca, Türkiye Cumhuriyeti kanunları kapsamında genellikle vakıf ve dernek olarak faaliyet göstermekte olan Sivil Toplum Kuruluşları için, kişisel verilerin işlenmesi ve korunmasına ilişkin prensipler açıklanmaktadır.

Rehber'in amacı, Sivil Toplum Kuruluşlarını KVKK konusunda genel kapsamda ve pratikte faydalı olacak şekilde yönlendirmektir.

1.2 Tanımlar

İşbu Rehberde yer verilen kavramlar aşağıda belirtilen anlamları ifade eder:

Açık Rıza	:	İlgili Kişinin Kişisel Verilerinin işlenmesine dair bilgilendirilmeye dayalı olarak ve özgür iradeyle açıkladığı rızayı ifade eder.
Elektronik Ticaret Mevzuatı	:	Elektronik ticaret usul ve esaslarını düzenleyen, 5 Kasım 2014 tarihli ve 29166 sayılı Resmi Gazete'de yayımlanan 6563 sayılı kanun ve ilgili mevzuatı ifade eder.
İlgili Kişi/Kişiler	:	Sivil Toplum Kuruluşları çalışanları, çalışan adayları, gönüllü, gönüllü adayları ve bağışçıları başta olmak üzere Kişisel Verisi işlenen gerçek kişileri ifade eder.
Kişisel Veri/Veriler	:	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.
Kişisel Verilerin İşlenmesi	:	Otomatik yöntemlerle gerçekleştirilsin yahut gerçekleştirilmesin Kişisel Veriler üzerinde yürütülen toplama, kayıt altına alma, işleme, saklama, değiştirme, geri getirme, konsültasyon, kullanma, aktarma, yayma yahut başka bir yöntemle ifşa etme, birleştirme, bloke etme, silme ve yok etme vb. tüm işlemleri ifade eder.
Kişisel Verilerin Korunması Kanunu/KVKK/Kanun	:	Kişisel verilerin korunması esaslarını düzenleyen, 7 Nisan 2016 tarihli ve 6698 sayılı kanunu ifade eder.

Kurul	:	Kişisel Verileri Koruma Kurulu'nu ifade eder.
Özel Nitelikli Kişisel Veri/Veriler	:	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri ifade eder.
Veri Sorumluları Sicil Bilgi Sistemi (VERBİS)	:	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemini ifade eder.
Rehber	:	Sivil Toplum Kuruluşları için hazırlanan ve Kişisel Verilerin işlenmesi ile korunmasına ilişkin genel prensipler ve pratikteki uygulamalara yönelik bilgilendirmeyi içeren işbu dokümanı ifade eder.
Veri İşleyen	:	Veri Sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişiyi ifade eder.
Veri Sorumlusu	:	Kişisel Verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan, ulusal hukuk veya toplumsal hukuk yahut düzenlemeler ile yetkilendirilen gerçek veya tüzel kişiyi ifade eder.

2. KİŞİSEL VERİLERİN İŞLENMESİ VE AKTARILMASI

2.1 Kişisel Verilerin İşlenmesinde Genel İlkeler

Sivil Toplum Kuruluşları tarafından Kişisel Verilerin işlenmesinde aşağıdaki ilkelerle hareket edilmesi tavsiye edilmektedir:

- Kişisel Veriler, ilgili **hukuk kurallarına ve dürüstlük kuralının gereklerine uygun** olarak işlenmelidir.
- Kişisel Verilerin **doğru ve güncel olması** sağlanır. Bu kapsamda verilerin elde edildiği kaynakların belirli olması, doğruluğunun teyit edilmesi, güncellenmesi gerekip gerekmediğinin değerlendirilmesi gibi hususlar özenle dikkate alınır.
- Kişisel Veriler; **belirli, açık ve meşru amaçlarla** işlenir. Amacın meşru olmasının değerlendirilmesinde, Sivil Toplum Kuruluşlarının işlediği Kişisel Verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar

için gerekli olması dikkate alınır.

- Kişisel Veriler, Sivil Toplum Kuruluşları tarafından belirlenen amaçların gerçekleştirilebilmesi için amaçla bağlantılı olmalıdır, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan Kişisel Verilerin işlenmesinden kaçınılmalıdır. İşlenen veri, sadece amacın gerçekleştirilmesi için gerekli olanla sınırlı tutulmalıdır. Bu kapsamda işlenen Kişisel Veriler, **işlendikleri amaçla bağlantılı, sınırlı ve ölçülü** olmalıdır.
- Sivil Toplum Kuruluşları, ilgili mevzuatta Kişisel Verilerin saklanması için öngörülen bir süre bulunması halinde bu sürelerle uyum göstermelidir; aksi durumda Kişisel Verileri, ancak **işlendikleri amaç için gerekli olan süre kadar muhafaza** edilmelidir.

2.2 Özel Nitelikli Olmayan Kişisel Verilerin İşlenme Şartları

Özel nitelikli olmayan Kişisel Verilerin işlenmesi için İlgili Kişinin Açık Rızası olması veya KVKK'da bulunan aşağıdaki istisnalara dahil olması gerekmektedir.

- a) Kanunlarda açıkça öngörülmesi.
- b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait Kişisel Verilerin işlenmesinin gerekli olması.
- d) Veri Sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- e) İlgili Kişinin kendisi tarafından alenileştirilmiş olması.
- f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- g) İlgili Kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Veri Sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

2.3 Özel Nitelikli Kişisel Verilerin İşlenme Şartları

Özel Nitelikli Kişisel Verilerin işlenmesi için İlgili Kişinin Açık Rızası olması gerekir. Bunun dışında, KVKK'da bulunan aşağıdaki istisnalara dahil bir durum olması halinde, söz konusu Kişisel Verilerin İlgili Kişinin Açık Rızası aranmaksızın işlenmesi mümkündür.

- a) Sağlık ve cinsel hayat dışındaki Özel Nitelikli Kişisel Veriler, kanunlarda öngörülen hâllerde İlgili Kişinin Açık Rızası aranmaksızın işlenebilir.

- b) Sağlık ve cinsel hayata ilişkin Kişisel Veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin Açık Rızası aranmaksızın işlenebilir.

Özel Nitelikli Kişisel Verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

2.4 Kişisel Verilerin Aktarılma Şartları

2.4.1 Yurtiçi Aktarım Şartları

- Özel nitelikli olmayan Kişisel Verilerin hukuka uygun olarak yurtiçindeki üçüncü kişilere aktarılması için İlgili Kişinin Açık Rızasının olması veya KVKK'da bulunan, yukarıda Madde 2.2'de belirtilen istisnalardan birinin bulunması gerekmektedir.
- Özel Nitelikli Kişisel Verilerin hukuka uygun olarak yurtiçindeki üçüncü kişilere aktarılması için İlgili Kişinin Açık Rızasının olması veya KVKK'da mevcut aşağıdaki hallerden birinin bulunması gerekmektedir.
 - a) Sağlık ve cinsel hayat dışındaki Özel Nitelikli Kişisel Veriler bakımından, kanunlarda açıkça öngörülmesi,
 - b) Sağlık ve cinsel hayata ilişkin Kişisel Veriler bakımından ise kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından söz konusu işlemin yapılması.

2.4.2 Yurtdışına Aktarım Şartları

Kişisel Verilerin hukuka uygun olarak yurtdışına aktarılması için İlgili Kişinin Açık Rızasının olması veya aşağıdaki hallerden birinin bulunması gerekmektedir.

Yukarıda Madde 2.2. ve Madde 2.3'de belirtilen istisna hallerinin bulunması ve ilaveten Kişisel Verinin aktarılacağı yabancı ülkede;

- a) Yeterli korumanın bulunması,
- b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulu izninin bulunması gerekmektedir.

Yeterli korumanın bulunduğu ülkeler listesi Kurul tarafından açıklanacaktır.

3. KİŞİSEL VERİLERİN İŞLENME VE AKTARILMA AMAÇLARI, AKTARILACAĞI KİŞİLER

3.1 Kişisel Verilerin İşlenme ve Aktarılma Amaçları

Kişisel Veriler, Kanun'a uygun olarak, İlgili Kişi aydınlatma metinlerinde gerekli detayda belirtilen amaçlar dahilinde Sivil Toplum Kuruluşları tarafından işlenebilirler.

Bu minvalde, Sivil Toplum Kuruluşları'nın Kişisel Veri işleme amaçları İlgili Kişi gruplarına göre değişiklik göstermektedir.

Bu noktada örnek olarak bazı kişisel veri işleme süreçleri aşağıda paylaşılmıştır:

1. Çalışan adaylarının başvuru, seçme ve yerleştirme süreçlerinin yürütülmesi,
2. Fiziksel mekân güvenliğinin temini,
3. Gönüllü adaylarının başvuru ve seçme süreçlerinin yürütülmesi,
4. Etkinlik, gezi ve eğitim gibi faaliyetlerde yer alacak gönüllülerin ve çalışanların görevlerinin belirlenmesi
5. Sivil toplum kuruluşunun faaliyetlerinin iyileştirilmesi, görevlendirmelerin ihtiyacı karşılayacak şekilde yapılabilmesi ve bu hususların değerlendirilebilmesi adına gönüllüler ve ihtiyaca ilişkin tespit, analiz ve/veya raporlama çalışmalarının yürütülmesi
6. Eğitim işbirlikleri çerçevesinde diğer sivil toplum kuruluşları, okullar ve benzeri kurumlar ile faaliyetlerin gerçekleştirilmesi
7. Bağışçı ilişkisinin kurulması kapsamında ayni ve/veya nakdi bağış sürecinin yürütülmesi
8. İlgili Sivil Toplum Kuruluşunun ticari işletmesi vasıtasıyla ürün satışı gerçekleştirilmesi
9. İlgili Sivil Toplum Kuruluşunun ticari işletmesi vasıtasıyla satışını yaptığı ürünlere ilişkin olarak ticari elektronik ileti vasıtasıyla tanıtım faaliyetlerinin sürdürülmesi.

3.2 Kişisel Verilerin Aktarılacağı Kişiler

Kişisel Veriler, Sivil Toplum Kuruluşları tarafından sunulan hizmetler ve kurulan ilişkiler çerçevesinde Kanun'a uygun olarak İlgili Kişi aydınlatma metinlerinde gerekli detayda belirtilen üçüncü kişiler ile paylaşılabilmektedir.

Bu minvalde, Sivil Toplum Kuruluşları'nın faaliyetleri kapsamında Kişisel Veri paylaşmasının söz konusu olabileceği bazı üçüncü kişilere ilişkin örnekler aşağıdaki gibidir:

- i. İş birliği yapılan ve/veya hizmet alınan çağrı merkezi faaliyeti sürdüren

- şirketler
- ii. Bordrolama hizmeti alınan şirketler
- iii. Sosyal medya şirketleri, prodüksiyon şirketleri, ajanslar ve reklam şirketleri
- iv. Hukuk, muhasebe, mali müşavirlik gibi alanlarda destek alınan kişiler
- v. Kanunen yetkili kurum ve kuruluşlar (ör: adli makamlar ve kolluk kuvvetleri)

4. KİŞİSEL VERİLERİN TOPLANMA YÖNTEMİ VE HUKUKİ SEBEBİ, SİLİNMESİ, YOK EDİLMESİ VE ANONİM HALE GETİRİLMESİ İLE SAKLANMA SÜRESİ

Kişisel Verilerin saklanması, silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili detaylı düzenlemeler Kurul tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("**Yönetmelik**") ile düzenlenmiştir.

Söz konusu Yönetmelik ışığında kişisel veri saklama ve imha politikasında belirtilen usul ve esaslara uygun olarak Kişisel Verilerin silinmesi ve yok edilmesinin hangi yöntemlerle gerçekleştirilebileceği aşağıda açıklanmıştır.

4.1 Kişisel Verilerin Silinmesi

Kişisel Verilerin silinmesi ilgili verilerin hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.

Kişisel Verilerin silinmesi işleminde öncelikle silme işlemine konu Kişisel Veriler belirlenecektir ardından her bir Kişisel Veri için erişim yetkisi bulunan ilgili kullanıcılar tespit edilecektir. İlgili kullanıcıların tespiti ile Kişisel Veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılacak ve ortadan kaldırılacaktır.

Silinme yöntem ve usulleri belirlenirken Kişisel Verilerin kayıt altına alındıkları ortam önem taşıyacak olup hangi kayıt ortamında tutulduysa ona ilişkin bir teknik usulle silinecektir. Sivil Toplum Kuruluşları teknik hizmet uygulamaları kullanmalarının yanı sıra kağıt doküman yöntemi ile de Kişisel Verileri saklayabilmektedir. İşbu halde kağıt üzerinde bulunan kişisel veriler karartma yöntemi kullanılarak silinecektir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, kesilmesi, geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde ilgili kullanıcılar tarafından görünemez hale getirilmesidir.

4.2 Kişisel Verilerin Yok Edilmesi

Kişisel Verilerin yok edilmesi, ilgili verilerin hiç kimse tarafından hiçbir şekilde

erişilemez, geri getirilemez ve tekrar kullanılamaz duruma getirilmesidir.

Kişisel Verilerin yok edilmesi için, verilere ait tüm kopyaların tespit edilmeli ve verilerin bulunduğu sistemlerin türüne göre çeşitli yok etme yöntemleri kullanılmalıdır.

Bu yöntemlerden özel teknik yolları dışında bahsedilmesi gerekir ise de-manyetize etme yolu ile manyetik medyanın özel nitelikli bir cihazdan geçirilerek yüksek değerde bir manyetik alana maruz bırakılarak veriler okunamaz bir biçime getirilebilecektir. Fiziksel yok etme yolu da optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesidir. Özel yazılımlar kullanılarak eski verinin kurtarılmasının önüne geçilmesi işlemi olan üzerine yazma metodu da bir diğer yok etme yöntemidir.

Verilerin bulunduğu ortam türüne bağlı olarak kullanılabilecek diğer teknik yok etme yöntemleri ise başlık olarak ağ cihazları, manyetik cihazlar, flash tabanlı ortamlardır.

4.3 Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel Verilerin başka verilerle eşleştirilmesi durumunda bile hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi Kişisel Verilerin anonim hale getirilmesi olarak tanımlanmıştır.

Kişisel Verilerin anonim hale getirilmesi kapsamında; veri sorumlusu veya alıcı grupları tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve teknik bilgilerin kullanılması yoluyla dahi gerçek kişiyle ilişkilendirilemez .

Kişisel Verilerin anonim hale getirilmesi; anonim hale getirme kavramından hareketle verileri tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin belirlenebilmesinin engellenmesi veya bir topluluk içinde ayırt edilebilir olma özelliğini kaybettirilmesidir. Anonim hale getirilme işleminin sonucu olarak tespit eden veriler ve bilgiler ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir.

Tüm bu açıklamalar ışığında belirtmek gerekir ki veri sorumlusu, silinen Kişisel Verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması , yok edilmesi ve Kişisel Verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

4.4 Kişisel Verilerin Saklanma Süreleri

Kişisel verilerin süresiz olarak saklanmaması gerekmektedir. Sivil Toplum Kuruluşlarının, kişisel veri saklama ve imha politikalarında belirtilen saklama sürelerine (ilgili mevzuat veya işleme amacına göre belirlenecektir) riayet ederek, silme, yok etme ve anonim hale getirmesi süreçlerini işletmeleri gerekmektedir.

5. TEKNİK İDARİ TEDBİRLER VE VERİ GÜVENLİĞİ

Kanun kapsamında Veri Sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, Kişisel Verilere hukuka aykırı olarak erişilmesini önlemek, verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

Sivil Toplum Kuruluşları, Kanun'un 12. maddesine uygun olarak, işlemekte olduğu verilerin güvenliğini sağlamak için uygun ve gerekli güvenlik tedbirlerini kendi imkanları ve operasyonel faaliyetleri doğrultusunda almalıdır.

Bununla birlikte veri kayıt sistemlerinde kişisel veri güvenliğine ilişkin çeşitli riskler meydana gelebilmektedir ve söz konusu risklerin önüne geçilebilmesi için gerekli kaynak ve uzmanlığın sağlanması gereklidir.

İlgili kapsamda öncelikli olarak tavsiye edilen bir risk değerlendirmesi yapılmasıdır. Bu riskler belirlenirken; Kişisel Verilerin özel nitelikli kişisel veri olup olmadığı, niteliği gereği hangi derecede gizlilik seviyesi gerektirdiği, güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararlar dikkate alınmalıdır

Sivil Toplum Kuruluşları tarafından alınabilecek ilgili tedbirler işbu rehber ekinde sunulmaktadır. (EK-1, EK-2, EK-3)

6. İLGİLİ KİŞİNİN HAKLARI, HAKLARIN KULLANILMASI VE DEĞERLENDİRİLMESİ

6.1 İlgili Kişinin Aydınlatılması

Sivil Toplum Kuruluşları, Kanunun 10. maddesine uygun olarak, Kişisel Verilerin elde edilmesi sırasında İlgili Kişileri aydınlatmaları gerekmektedir. Bu kapsamda veri sorumlusu Sivil Toplum Kuruluşu'nun bilgileri (ünvanı, adresi, iletişim bilgileri), Kişisel Verilerin hangi amaçla işleneceği, işlenen Kişisel Verilerin kimlere ve hangi

amaçla aktarılabileceği, Kişisel Veri toplamanın yöntemi ve hukuki sebebi ile İlgili Kişinin sahip olduğu hakları konusunda aydınlatma yapılmalıdır.

Aydınlatma yükümlülüğünün yerine getirilmesi, İlgili Kişilere ilişkin yürütülecek süreçlerin en önemlilerindedir ve ilgili faaliyetin açık rıza gerektirip gerektirmemesinden bağımsız olarak sürdürülmelidir.

6.2 İlgili Kişinin KVKK Uyarınca Hakları

İlgili Kişinin Kanun'un 11.maddesi uyarınca hakları aşağıdaki gibidir:

- Kişisel Veri işlenip işlenmediğini öğrenme,
- Kişisel Verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel Verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında Kişisel Verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel Verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme,
- Kanun'un 7. maddesinde öngörülen şartlar çerçevesinde Kişisel Verilerin silinmesini veya yok edilmesini isteme,
- Kanun'un 11. maddesinin (d) ve (e) bentleri uyarınca yapılan işlemlerin, Kişisel Verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel Verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme.

6.3 İlgili Kişinin Haklarını Kullanması

İlgili Kişilerin sahip oldukları ve yukarıda belirtilen haklarını kullanmak için yapacağı ve kullanmayı talep ettiği hakka ilişkin açıklamaları içeren başvuruda; talep edilen hususun açık ve anlaşılır olması, kişinin şahsı ile alakalı olması veya başkası adına hareket ediyorsa bu konuda özel olarak yetkili olması gerekmektedir.

Başvurulara ilişkin olarak cevap verme usul ve süresi ise ilgili kuruluş tarafından başvuruda yer alan talepler, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde sonuçlandırır.

Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; İlgili Kişi, cevabı öğrendiği tarihten itibaren

otuz ve herhâlde başvuru tarihinden itibaren altmış gün içinde Kurul'a şikâyetle bulunma hakkına sahiptir.

Sivil Toplum Kuruluşlarının, İlgili Kişilerin her türlü taleplerini yerine getirme yükümlülüğü bulunmamaktadır. Örneğin, kanuni olarak saklaması gereken belgelerin (ör: fatura veya özlük dosyasındaki gerekli belgeler) silinmesi taleplerini, gerekli cevabı vererek reddetmeleri mümkündür.

7. SİVİL TOPLUM KURULUŞLARINA YÖNELİK VERBİS KAYIT SİSTEMİ

Kanun ve ilgili mevzuat kapsamında, bazı kriterleri sağlayan (ör: çalışan sayısı) Veri Sorumluları için Veri Sorumluları Sicil Bilgi Sistemine ("**VERBİS**") kayıt olma yükümlülüğü getirilmiştir.

VERBİS esasen, Kişisel Verileri işleyen söz konusu gerçek ve tüzel kişilerin, Kişisel Veri işlemeye başlamadan önce kaydolmaları gereken ve işlemekte oldukları Kişisel Verilerle ilgili kategorik olarak bilgi girişi yapacakları bir kayıt sistemidir.

Kanun; işlenen Kişisel Verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir hükmünü düzenlemiştir.

Bu hüküm doğrultusunda Kurulca bazı veri sorumluları için Sicile kayıt yükümlülüğüne istisna getirilmiştir. Kurul'un 02.04.2018 tarihinde verdiği 2018/32 sayılı kararı uyarınca, yalnızca ilgili mevzuat ve amaçlarına uygun faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılara yönelik kişisel veri işleyen derneklerin, vakıfların ve sendikaların VERBİS kaydından istisna tutulması söz konusu olmuştur.

Bununla birlikte Kurul, yukarı belirtilen kayıt yükümlülüğüne ilişkin istisnai hale 09.06.2021 tarihli ve 2021/571 sayılı kararı uyarınca; *"yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye'de yerleşik dernek, vakıf ve sendikalarından kendisine bağlı herhangi bir iktisadi işletmesi bulunmayanlar"* şeklinde bir ifade eklemiştir.

Tüm bu açıklamalar ışığında kendisine bağlı herhangi bir iktisadi işletmesi bulunan Sivil Toplum Kuruluşları bakımından VERBİS'e kayıt yükümlülüğü getirilmiştir.

Fakat Sivil Toplum Kuruluşlarından kendisine bağı herhangi bir iktisadi işletmesi bulunanların Sicile kayıt olmaları yönünden VERBİS kaydının yalnızca iktisadi işletmenin faaliyetlerine ilişkin olarak yapılması gerekmektedir.

Sivil Toplum Kuruluşlarından Türkiye’de yerleşik dernek, vakıf ve sendikalara ait iktisadi işletmelerden veri sorumlusu sıfatını haiz olanların İlgili Kurul kararlarında belirtilen kriterler (yıllık çalışan sayısı, yıllık mali bilanço ve ana faaliyeti kapsamında özel nitelikli kişisel veri işleme) açısından değerlendirilmesi ve bu kriterleri taşıyan iktisadi işletmelerin kendi adlarına VERBİS’e kayıt olması gerekmektedir.

8. KİŞİSEL VERİ MEVZUATINA UYUM HAKKINDA UYGULAMAYA YÖNELİK TAVSİYELER

Sivil Toplum Kuruluşlarının, KVKK uyum süreçlerine ilişkin bazı uygulamaya yönelik tavsiyeler aşağıda sunulmuştur:

- **Farkındalık:** Kişisel Verilerin Korunması Kanunu gereklilikleri ve kişisel veri mahremiyeti, ülkemizde önemi nispeten yeni anlaşılmaya başlanmış hususlardır. Bu nedenle, Sivil Toplum Kuruluşları için ilk adım, çalışanlarının ve gönüllülerinin eğitimler vasıtasıyla bu konuda belirli bir farkındalık seviyesinde olmasını sağlamak olacaktır.
- **Sahiplenme ve süreklilik:** KVKK uyumu sürekli bir çaba gerektiren bir husustur. Bir uyum projesinin tamamlanması veya birkaç seferlik verilen eğitimler, gerekli uyum seviyesinin yakalanmasında yetersiz kalabilmektedir. Bu nedenle, üst yönetim seviyesinde konunun sahiplenilmesi, sorumlu kişilerin belirlenmesi ve sorumlu kişiler dahil olmak üzere konuyla ilgisi olabilecek çalışan ve gönüllülerin hedefleri arasına KVKK uyumunun eklenmesi önem arz etmektedir.
- **Veri azaltılması prensibi:** Sivil Toplum Kuruluşları tarafından işlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olması, güncel olması ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirmektedir. Örneğin, bağışçıların veya gönüllülerin verilerinin toplandığı bir formda, ilgili faaliyet için gerekmeyen (ör: anne kızlık soyadı) bulunmaması veya ileride gerekli olabilir düşüncesiyle veri toplanmaması tavsiye edilmektedir.
- **Şeffaflık ve aydınlatma:** Sivil Toplum Kuruluşları, faaliyet konularına göre, çok çeşitli kişi gruplarına ilişkin Kişisel Verileri, oldukça kapsamlı amaçlar çerçevesinde

işleyebilmektedir. Bu noktada kişisel verisi işlenen kişi gruplarının iyi belirlenmesi ve söz konusu kişilerin şeffaf bir biçimde bilgilendirilmesi elzemdir.

- **Özel kişi grupları:** Özel kişi gruplarına yönelik veri işleyen Sivil Toplum Kuruluşları için ilave hassasiyet göstermeleri gereken durumlar söz konusudur. Örnek vermek gerekir ise; reşit olmayanların zihinsel veya fiziksel gelişimine, eğitim hayatına yardımcı olan Kuruluşlar belirli bir yaşı altındaki çocuklardan yasal olarak açık rıza alamazlar ve ilgili süreçlere ebeveynlerin dahil edilmesi gerekmektedir.
- **KVKK ve Elektronik Ticaret Mevzuatı ilişkisi:** Kişisel Verilerin Korunması Kanunu Kişisel verilerin işlenmesini (kaydedilmesi, depolanması, yeniden düzenlenmesi vs.) düzenlemektedir. Bununla birlikte Elektronik Ticaret Mevzuatı (diğer hususların yanında) gerçek ve tüzel kişilerin, mal ve hizmetlerini tanıtmak, pazarlamak ya da işletmesini tanıtmak veya bunları başkaları adına yapmak amacıyla ve elektronik araçlarla (SMS, e-mail vs.) yaptıkları her türlü ticari iletişimi kapsar.

Söz konusu çerçevede, ilgili Sivil Toplum Kuruluşu'nun faaliyetlerini inceleyerek, Elektronik Ticaret Mevzuatı kapsamındaki yükümlölüklerini de (ör: İleti Yönetim Sistemi kaydı, elektronik ticari ileti izni vb.) yerine getirmesi gerekmektedir.

- **Üçüncü kişi riskleri:** Sivil Toplum Kuruluşları, faaliyetleri çerçevesinde tedarikçilerle çalışmakta ve diğer tüzel kişilerle iş birliği yapmaktadır. İlgili hizmet alımı veya iş birliği kapsamında, kişisel veri aktarımı veya erişime açılması söz konusu ise ilgili Sivil Toplum Kuruluşu, üçüncü kişi KVKK risklerini en aza indirmek için gerekli adımları (ör: sözleşme maddeleri, üçüncü kişi teknik ve idari tedbirlerinin denetlenmesi, itibar araştırması vb.) atmalıdır.

EK-1

Veri Güvenliğine İlişkin Alınabilecek Örnek Tedbirler

1. Ağ güvenliği ve uygulama güvenliği sağlanması.
2. Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılması.
3. Anahtar yönetimi uygulanması.
4. Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınması.
5. Bulutta depolanan kişisel verilerin güvenliği sağlanması.
6. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri.
7. Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılması.
8. Çalışanlar için yetki matrisi oluşturulması.
9. Erişim logları düzenli olarak tutulması.
10. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanması.
11. Gerektiğinde veri maskeleyme önlemi uygulanması.
12. Gizlilik taahhütnameleri
13. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılması.
14. Güncel anti-virüs sistemleri kullanılması
15. Güvenlik duvarları kullanılması.
16. İmzalanan sözleşmeler veri güvenliği hükümleri içermesi.
17. Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmesi.
18. Kişisel veri güvenliği politika ve prosedürleri belirlenmesi.
19. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanması.
20. Kişisel veri güvenliğinin takibi yapılması.
21. Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınması.

22. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanması.
23. Kişisel veri içeren ortamların güvenliği sağlanması.
24. Kişisel veriler mümkün olduğunca azaltılması.
25. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliğinin sağlanması.
26. Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanması ve takip edilmesi.
27. Kurum içi periyodik ve/veya rastgele denetimler yapılması.
28. Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulması.
29. Mevcut risk ve tehditler belirlenmesi.
30. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmesi.
31. Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmesi.
32. Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılması ve farklı birimlerce yönetilmesi.
33. Saldırı tespit ve önleme sistemleri ve Sızma testi uygulamaları kullanılması.
34. Siber güvenlik önlemleri alınması ve takibi ve şifreleme yapılması.
35. Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılması.
36. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanması.
37. Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanması.
38. Veri kaybı önleme yazılımları kullanılması.

EK-2

Kurul Tarafından Önerilen Teknik ve İdari Tedbirler

Teknik Tedbirler	İdari Tedbirler
Yetki Matrisi	Kişisel Veri İşleme Envanteri Hazırlanması
Yetki Kontrol	Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
Erişim Logları	Sözleşmeler (Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen Arasında)
Kullanıcı Hesap Yönetimi	Gizlilik Taahhütnameleri
Ağ Güvenliği	Kurum İçi Periyodik ve/veya Rastgele Denetimler
Uygulama Güvenliği	Risk Analizleri
Şifreleme	İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi)
Sızma Testi	Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.)
Saldırı Tespit ve Önleme Sistemleri	Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)
Log Kayıtları	Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim
Veri Maskeleye	
Veri Kaybı Önleme Yazılımları	
Yedekleme	
Güvenlik Duvarları	
Güncel Anti-Virüs Sistemleri	
Silme, Yok Etme veya Anonim Hale Getirme	
Anahtar Yönetimi	

EK-3

Özel Nitelikli Kişisel Verilere İlişkin İlave Tedbirler

I. Özel Nitelikli Veri İşleyen Veri Sorumlusu Çalışanlarına İlişkin Düzenlemeler

1. Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak çalışanlara eğitimler verilmesi
2. Gizlilik sözleşmelerinin yapılması,
3. Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,
4. Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
5. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması, bu kapsamda veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması.

II. Özel Nitelikli Kişisel Verilerin Bulunduğu Ortama İlişkin Özel Düzenlemeler

Söz konusu ortam elektronik ise ;

1. Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi ve kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
2. Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak tutulması, verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması, test sonuçlarının kayıt altına alınması,
3. Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması,
4. Verilerin bulunduğu ortamlar için gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması
5. Verilere uzaktan erişim gerekiyorsa yeterli düzeyde kimlik doğrulama sisteminin sağlanması gerekmektedir.

Söz konusu ortam fiziksel ortam ise;

Ortamın niteliğine göre yeterli güvenlik önlemlerinin alındığından emin olunması ve bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi gerekmektedir.

III. Özel Nitelikli Kişisel Verilerin Aktarımına İlişkin Düzenlemeler

KVKK, özel nitelikli kişisel verilerin aktarılması sırasında seçilecek platforma göre

farklı güvenlik tedbirler öngörmüştür. Bu bağlamda verilerin;

1. E-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,
2. Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
3. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,
4. Fiziki ortamda aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” formatında gönderilmesi gerekmektedir.

Son olarak (i) özel nitelikli kişisel verilere ilişkin ayrı bir politika ve prosedür belirlenmelidir (ii) Kurul’un Kişisel Veri Güvenliği Rehberi’nde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirlerinin de dikkate alınması gerekmektedir.