İçindekiler Tablosu

1. Amaç ve Kapsam

ENYILDIZ KİŞİSEL VERİLERİN GÜVENLİĞİ, SAKLANMASI VE İMHA POLİTİKASI ("Politika"), **Enyıldız Matbaa Dijital Baskı Çözümleri ve Reklamcılık A.Ş. ("ENYILDIZ")** tarafından gerçekleştirilmekte olan işleme faaliyetlerine ve işlenmekte olan kişisel verilerin korunmasına ait alınan güvenlik tedbirlerinin usul ve esasları belirlemek, verilerin işlenmesi sırasında uyması gereken kuralları tanımlanmış, aynı zamanda saklanması ve imha süreçlerine yönelik iş ve işlemlerin belirlenmesi amacıyla hazırlanmıştır.

Bu Politika, **ENYILDIZ** tarafından kişisel verilerin korunması kanunu ve ilgili mevzuat ile ortaya konulan düzenlemelerin uygulanması bakımından yol gösterme amacı taşımaktadır.

2. Kavramlara Ait Tanımlar

Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemdir.
KVK Kanunu	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan, 24 Mart 2016 ta-rihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.
KVK Kurulu	Kişisel Verileri Koruma Kurulu
KVK Kurumu	Kişisel Verileri Koruma Kurumu
Komite	ENYILDIZ tarafından kişisel veri güvenliğinin temini, denetimi ve başvuruların değerlendirilmesi amacıyla görevlendirilmiş kişilerden oluşan komiteyi ifade eder.
Veri İrtibat Kişisi	Kişisel verileri koruma kurumu ile kurulacak iletişim için ENYILDIZ tarafından VERBİS'e kayıt esnasında bildirilen gerçek kişiyi ifade eder.
Kişisel Veri Sahibi	Kişisel verisi işlenen gerçek kişi. Örneğin; Müşteriler, çalışanlar…
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Özel Nitelikli Kişisel Veri	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.

Kişisel Veri İşleme Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.
Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ	10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ.
Aydınlatma Beyanı	Kişisel Verilerin İşlenmesi hususunda veri sahiplerinin aydınlatıldığı beyan
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ	10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ.
Kişisel Veri İşlenmesi ve Korunması Politikası	ENYILDIZ Kişisel Verilerin İşlenmesi ve Korunması Politikası
Müşteri	ENYILDIZ' ın sunmuş olduğu hizmet ve ürünlerden yararlanan gerçek kişileri ve Tüzel kişi Temsilcilerini ifade eder.
Çalışan	İş Sözleşmesine dayanarak ENYILDIZ' da istihdam edilen kişileri ifade eder.
Çalışan Adayı	ENYILDIZ' a iş başvurusunda bulunarak veya herhangi bir yolla özgeçmişini ve ilgili bilgilerini ENYILDIZ' a erişilebilir kılan gerçek kişileri ifade eder.
Taşeron Çalışanı	ENYILDIZ' ın hizmet aldığı firma çalışanlarını ifade eder.
Üçüncü Kişiler	Prosedürde tanımlanmamış olmasına rağmen işbu Prosedür çerçevesinde kişisel verileri işlenen tedarikçi, mağdur, aile bireyleri vb. dâhil fakat bunlarla sınırlı olmamak üzere diğer gerçek kişileri ifade eder.
Elektronik Ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
Elektronik Olmayan Ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.

İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Periyodik İmha	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re 'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Kişisel Verilerin Güvenliği	KİŞİSEL VERİ GÜVENLİĞİ REHBERİ (Teknik ve İdari Tedbirler)'de belirtilen güvenlik önlemleri

3. Roller ve Sorumluluklar

ENYILDIZ organizasyon şeması kapsamındaki tüm birimler ve çalışanları, KVK Komitesine ve KVK Uyum süreci ile ilgili hazırlanan bu Politika kapsamında alınmakta olan teknik ve idari tedbirlerin uygulanması, çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında KVK Komitesi başta olmak üzere aktif olarak destek verir.

Aynı zamanda, müşteriler, sigorta şirketleri, danışmanlar, dış hizmet sağlayıcıları, alt taşeron olarak hizmet veren gerçek ve tüzel kişiler ve sair surette ENYILDIZ nezdinde kişisel veri saklayan ve işleyen herkes bu gerekleri yerine getirmekten sorumludur.

İş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar doğmasına neden olabilecek periyodik imhalar, ilgili kişisel verinin türü, içinde yer aldığı sistemler ve veri sahibi iş birimi dikkate alınarak ilgili bilgi sistemleri bölümlerince yapılacaktır.

ENYILDIZ bünyesinde bir Kişisel Verilerin Korunması Komitesi kurar. Kişisel Verilerin Korunması Komitesi, ilgili kişilerin verilerinin hukuka, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve Kişisel Veri Güvenliği, Saklama ve İmha Politikasına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir.

4. Kişisel Verilerin İşlenmesi ve Aktarılması Sırasında Alınan Güvenlik Tedbirleri

4.1 Kişisel Veri İşlenme

Kişisel verilerin işlenmesi, Kanunun 3. Maddesinde tanımlanmıştır. Buna göre; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem, kişisel verilerin işlenmesi olarak kabul edilmiştir.

ENYILDIZ kişisel verilerin korunması konusunda şirket politikası olarak özel bir hassasiyet göstermekte olup bu doğrultuda aşağıdaki temel ilkelerin ışığında hareket etmektedir.

4.2 Kişisel Veri İşleme İlkeleri

Hukuka ve dürüstlük kurallarına uygun olma,

Doğru ve gerektiğinde güncel olma,

Belirli, açık ve meşru amaçlar için işlenme,

İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Kişisel verilerin işlenmesine ilişkin ilkeler, tüm kişisel veri işleme faaliyetlerinin özünde bulunmalı ve tüm kişisel veri işleme faaliyetleri bu ilkelere uygun olarak gerçekleştirilmelidir.

4.3 Kişisel Verilerin İşlenme Koşulları

Kişisel verilerin işlenme için gerekli olan koşullar Kanunun 5. maddesinde sayılmış olup, buna göre aşağıdaki hallerden en az birinin bulunması durumunda kişisel verilerin işlenmesi mümkündür.

- İlgili kişinin açık rızasının varlığı,
- Kanunlarda açıkça öngörülmesi,
- 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,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

Kişisel verilerin işlenme şartları, yani hukuka uygunluk halleri, Kanunda sayma yoluyla belirlenmiş olup, bu şartlar genişletilemez.

Kişisel veri işleme, Kanunda bulunan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmamaktadır. Veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılması, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacaktır. Nitekim, ilgili kişi tarafından verilen açık rızanın geri alınması halinde veri sorumlusunun diğer kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesi hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına gelecektir. Bu kapsamda, veri sorumlusu tarafından kişisel veri işleme faaliyetinin amacının öncelikli olarak açık rıza dışındaki işleme şartlarından birine dayanıp dayanmadığı değerlendirilmeli, eğer bu amaç Kanunda belirtilen açık rıza dışındaki şartlardan en az birini karşılamıyorsa, bu durumda veri işleme faaliyetinin devamı için kişinin açık rızasının alınması yoluna gidilmelidir.

4.4 Özel Nitelikli Kişisel Veri İşleme

Özel nitelikli kişisel veriler, öğrenilmesi halinde ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki verilerdir. Bu nedenle diğer kişisel verilere göre çok daha sıkı şekilde korunmaları gerekmektedir. Kanunda özel nitelikli kişisel veriler, sınırlı sayma yoluyla belirlenmiştir. Bunlar; 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 verileridir.

Kanun, bu verilere özel bir önem atfetmekte ve bu verilerle ilgili farklı bir düzenleme getirmektedir. Kanun bunları özel nitelikli kişisel veri ya da hassas veriler olarak kabul etmektedir. Özel nitelikli kişisel veriler ilgili kişinin açık rızası ile ya da Kanunda sayılan sınırlı hallerde işlenebilir.

Kanuna göre açık rıza halinde özel nitelikli kişisel veriler işlenebilir. Fakat, özel nitelikli kişisel verilerin işlenmesi, ilgili kişinin açık rızası dışında aşağıdaki hallerde de mümkündür:

• Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, ancak kanunlarda öngörülen hallerde,

• Sağlık ve cinsel hayata ilişkin kişisel veriler, 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 işlenebilir.

4.5 Kişisel Verilerin Aktarılması Şartları

Kişisel Verilerin Korunması Kanun' da belirtilen genel ilkeler çerçevesinde işlenmek üzere elde edilen kişisel verilerin, 8. madde hükmü uyarınca ilgili kişinin açık rızası alınmak suretiyle üçüncü kişilere aktarılabileceği hükme bağlanmıştır.

Veri aktarımına ilişkin alınacak teknik, idari ve hukuki tedbirler yurt içi ve yurtdışı veri aktarım türüne göre gruplandırılmalıdır.

4.5.1 Kişisel Verilerin Yurt İçerisinde Aktarım Şartları

Kanun, kişisel verilerin işlenmesi ile bu verilerin yurt içinde aktarılması bakımından ilgili kişinin açık rızası alınmak suretiyle üçüncü kişilere aktarılabilmektedir.

Diğer taraftan, kişisel verilerin yurtiçinde hukuka uygun şekilde işlenmesi bunların doğrudan aktarılabileceği anlamına gelmemektedir.

Bu kapsamda, kişisel verilerin aktarılması için aşağıdaki hallerden birinin bulunması gerekmektedir:

- İlgili kişinin açık rızasının alınması,
- Kanunlarda açıkça öngörülmesi,
- 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,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

Özel nitelikli kişisel verilerin yurtiçinde aktarılabilmesi için ise; aşağıdaki hallerden birinin bulunması gerekmektedir.

- İlgili kişinin açık rızasının alınması halinde,
- Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler bakımından kanunlarda açıkça öngörülmüş olması halinde,
- Sağlık ve cinsel hayata ilişkin kişisel veriler bakımından ise kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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 işlenebilmektedir.

Kişisel veriler üzerinde işlem gerçekleştiren her türlü gerçek veya tüzel kişi, veri işlenmesine ilişkin amaç ve yöntemlerine göre ya veri sorumlusu ya da veri işleyendir. Veri aktarımı yapılması gerektiğinde aktarım yapılacak gerçek veya tüzel kişiler ile aktarım amacına göre;

- Veri Sorumlusundan Veri Sorumlusuna Aktarım
- Veri Sorumlusundan Veri İşleyene Aktarım sözleşmelerinden uygun olan sözleşme yapıldıktan sonra veri aktarımı yapılmalıdır.

4.5.2 Kişisel Verilerin Yurt Dışına Aktarım Şartları

Kişisel verilerin yurt dışına aktarılması yurtdışına aktarımında yapılması gereken unsurlar;

- İlgili kişinin açık rızasının bulunması,
- Yeterli korumanın bulunduğu ülkelere (Kurul tarafından güvenli kabul edilen ülkeler) aktarımın sağlanması,
- Veri aktarımında, Kanunda belirtilen hallerin varlığı;
- Yeterli korumanın bulunmadığı ülkelere veri aktarımında Kanunda belirtilen hallerin varlığında yeterli korumanın yazılı olarak taahhüt edilmesi ve Kurulun izninin bulunması durumlarında gerçekleştirilebilir.

Kişisel verilerin işlenmesi ile bu verilerin yurt dışına aktarılması bakımından aynı şartları aramaktadır. Ayrıca kişisel verilerin yurt dışına aktarılmasında ek tedbirlerin alınmasını öngörülmüştür.

Yeterli korumanın bulunması halinde veri aktarımı

Kişisel veriler;

- Kanunlarda açıkça öngörülmesi,
- 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,

- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması halinde yurtdışına aktarılabilmektedir.

Özel nitelikli kişisel verilerin aktarımı,

Kişisel verilerin aktarılacağı ülkede yeterli korumanın bulunması halinde, sağlık ve cinsel hayat dışındaki kişisel veriler kanunda açıkça öngörülmesi halinde yurtdışına aktarılabilecektir.

Yeterli korumaya sahip ülkelerde kişilerin, sağlık ve cinsel hayata ilişkin kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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 yurtdışına aktarılabilecektir.

Yeterli korumanın bulunduğu ülkeler Kurul tarafından ilan edilecektir.

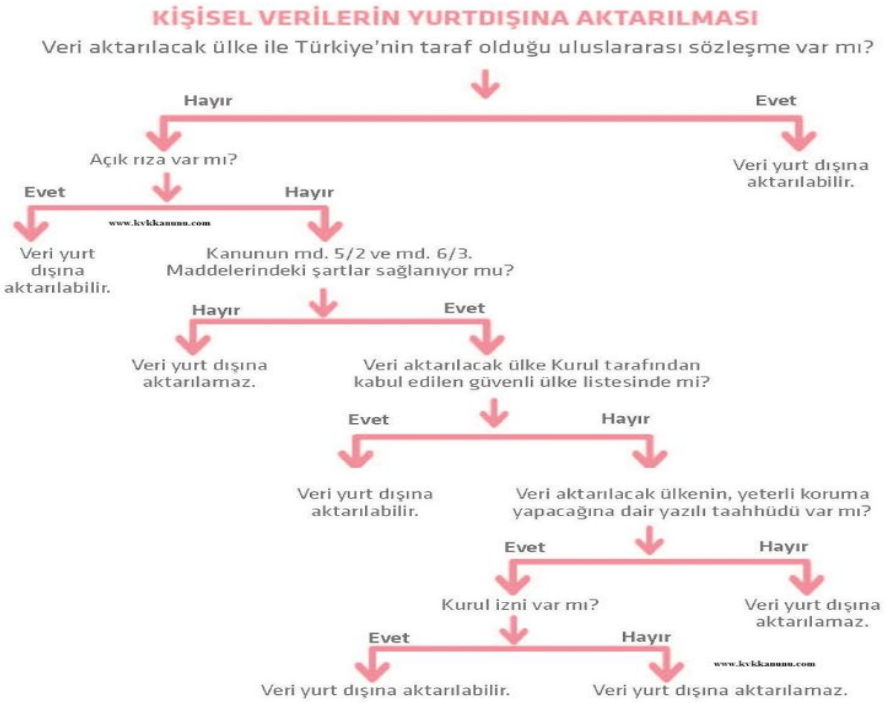
Yeterli korumaya sahip olmayan ülkelere veri aktarımı;

Kanunun 5 veya 6. Maddesinde sayılan kişisel veri ve özel nitelikli kişisel verilerin işlenme şartlarından en az birinin gerçekleşmesi,

Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri,

Kurulun izninin bulunması gerekmektedir.

Kişisel verileri Koruma Kurulu tarafından yayınlanan sözleşme türlerin uygun olan seçilerek, aktarım yapılan taraf ile yapılmalıdır.



5. Kişisel Verilerin Kayıt ve Saklandığı Ortamlar

ENYILDIZ tarafından kişisel veriler aşağıdaki kayıt ortamları aracılığıyla işlenmektedir, güncelliği sağlanmakta ve saklanmaktadır.

Tablo 1: Kişisel veri saklama ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
(1) Yazılımlar	**(1) Manuel Veri Kayıt Ortamları**
(a) Web , e-posta	(a) Formlar
(b) CRM Portal	(b) Tutanaklar
(c) Microsoft Office,WindowsServer,SQL Server (d) ERP Sistemi	(c) Belgeler
(2) Güvenlik Duvarı	**(2) Görsel – Yazılı Diğer Ortamlar**
(a) Sonicwall (b) Cyberoan (c) Juniper (d) Fortigate	*(a) Arşiv ve Dolaplarda Bulunan Dökmanlar (Eğitim Kayıtları, Sözleşmeler, Toplantı Tutanakları, Özlük Dosyaları,)*
(3) Saldırı Tespit Ve Engelleme Sistemi	*(b)Klasörler*
(a) Sophos	*(c)Birim dolapları*
(4) Antivirüs	*(d) Basın Haberleri*
(a) Sophos	
(5) Loglama	
(a) Sophos (b) Sonicwall	
(6) Kurum/Kişisel Bilgisayarlar	
(7) Cep Telefonları/Tabletler	
(8) Ortak Dosya Sunucu Sistemi	
(9) Optik Diskler ,USBbellek	
(10) Kamera Kayıt Sistemleri,	
(11) Ses Kayıt Sistemleri	
(12) Yazıcı, Fotokopi, Tarayıcı Makinaları	
(13) Geçiş Kontrol Sistem Kayıtları	
(14) Yedekleme Sunucusu ve Sistem Cihazları	
(15) Elektronik İmza ve Mühürler	
(16) Bulut Sistemler (O365, FTP, 5651 vb)	

6. Kişisel Veri İşleme Yöntemleri

Kişisel verilerin işlenmesi kavramı zincirleme bir döngüyü ifade etmektedir. Kanunun 2. maddesinde, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla ilk defa elde edilmesiyle başlayan bir süreç ve devamındaki her türlü işleme, veri işleme olarak tanımlanmıştır.

Kişisel verileri işlemesi olarak tanımlanan süreç aşağıdaki adımlardan oluşmaktadır.

• **Toplama veya kaydetme:** Kişisel verilerin ilk defa elde edildikleri an itibariyle işleme fiili başlamaktadır.

• **Organize etme/depolama:** Dijital ya da fiziksel ortamda, kişisel verilerin saklanması, barındırılması ya da depolanması işleme kapsamında kabul edilir.

• **Kullanma/değiştirme:** Kişisel verilerin, görüntülenmesi de dâhil olmak üzere, her türlü kullanımı işleme sayılır.

• **Aktarma:** Kişisel verilerin çeşitli yöntemlerle iletilmesi.

• **Yayma/erişilebilir kılma:** Fiziksel olarak dağıtmak veya paylaşmak gibi, verileri dijital ortamda üçüncü tarafların erişimine açmak da bir işleme türüdür.

• **Engelleme/silme/yok etme/anonim hale getirme:** Bunlar da bir işleme faaliyeti olarak kabul edilmektedir.

Kişisel verilerin otomatik yollarla işlenmesi: Bilgisayar, telefon, saat vb. işlemci sahibi cihazlar tarafından yerine getirilen, yazılım veya donanım özellikleri aracılığıyla önceden hazırlanan algoritmalar kapsamında insan müdahalesi olmadan kendiliğinden gerçekleşen işleme faaliyetidir.

Kişisel verilerin otomatik olmayan yollarla işlenmesi: Kişisel veriler otomatik işlemeye tabi tutulmasalar da, "veri kayıt sistemi" aracılığıyla işlendiklerinde de Kanun hükümlerine tabi olacaklardır. Kanun gerekçesinde veri kayıt sistemi, "kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi'ni ifade etmektedir.
Bu sistemler elektronik yahut fiziki ortamda oluşturulabilir. Buna göre, veri kayıt sisteminde kişisel veriler, ad, soyad veya kimlik numarası üzerinden sınıflandırılabileceği gibi, kredi borcunu ödemeyenlere ilişkin oluşturulacak sınıflandırma da bu kapsamda değerlendirilebilecektir. Kanun, otomatik olmayan yollarla veri işlenmesini tamamen Kanun kapsamı dışında tutmamaktadır. Yani, otomatik olmayan yolla veri işleme eğer veri kayıt sisteminin parçası ise, bu durumda veri işleme faaliyeti Kanun kapsamında kabul edilecektir.

7. Kişisel Verilerin Güvenliğinde Uyması Gereken Kurallar

Kişisel verileri işlenmesinde, öncelikle madde 4.2 'de bahsedilen Kişisel Veri İşleme İlkelerine uygun işlem yapılmalıdır. ENYILDIZ kişisel veri işleme süreçlerinde hizmet veren veri işleyen gruplarına ilgili yöntem ve kuralları tanımlamıştır.

7.1 Veri İşleyen Gerçek ve Tüzel Kişilerin Uyması Gereken Kurallar

Veri işleyen; Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler olarak tanımlanmaktadır. Bu kişiler, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen, veri sorumlusunun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği ayrı bir gerçek veya tüzel kişidir.
Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, gerekli tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur. Veri işleyenler de veri güvenliğinin sağlanması için tedbir alma yükümlülüğü altındadır.
ENYILDIZ' ın veri sorumlusu olarak, veri güvenliğine ilişkin olarak denetim yükümlülüğü mevcuttur. ENYILDIZ' ın, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

Veri işleyen taraf, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

ENYILDIZ aynı zamanda tüm veri işleyen taraflar ile **Kişisel Veri Aktarım Çerçeve Sözleşmesi** yapmaktadır. Veri işleyen, Kurul kararı ile açıklanan gerekli teknik ve idari tedbirleri almalıdır. Tedbir yöntemleri seçilirken, şirketin büyüklüğü veya cirosunun yanı sıra veri sorumlusunun yaptığı işin ve korunan kişisel verinin niteliği de önemlidir.

7.2 Firma Çalışanlarının Uyması Gereken Kurallar

7.2.1 Çalışanların ve Çalışan Adaylarının Kişisel Verilerinin İşlenmesinde Uyulacak Kurallar

Çalışanlara ait Özel Nitelikli Kişisel Veriler de dahil olmak üzere Kişisel Verilerin İş Kanunu ve diğer ilgili mevzuat uyarınca yahut ENYILDIZ tarafından belirlenen başka amaçlarla işlenebilmesi için, halihazırda ENYILDIZ çalışanı bulunan kişilere "Çalışan Veri Gizliliği Sözleşmesi' nin imzalatılması suretiyle aydınlatma ve açık rıza temini yükümlüğünün yerine getirilmesi gerekmektedir.

Halihazırda ENYILDIZ çalışanı durumunda bulunmayan, işe alım süreci olumlu şekilde tamamlanacak olan kişilere ilişkin kişisel verilerin işlenebilmesinin için, ilgili kişiye "Güncel İş Sözleşmesi'nin imzalatılması ve aydınlatma yükümlülüğünün yerine getirilmesi gerekmektedir.

7.2.2 Müşterilere Ait Kişisel Verilerin İşlenmesi ve Kullanılmasında Uyulacak Esaslar

Müşterilerin kişisel verilerini doğrudan veya dolaylı olarak pazarlama yapmak ve satış süreçlerindeki performansı arttırmak maksadıyla toplanması ve işlenmesi için, kişisel verilerin toplanmasından önce ilgili kişi müşterinin açık rızasının alınmış olması gerekir.

Satış süreçlerinde, hukuki yükümlülüklerin yerine getirilmesi veya Madde 4.3'de belirtilen koşullar sebebiyle işlenen bir kişisel veri mevcut ise Açık Rıza şartı aranmayacaktır.

Elektronik haberleşme yöntemleri SMS, Mailing gibi yöntemler ile kampanya ve tanıtım gönderimleri için müşterilerden ayrıca onay alınmasına verinin amacı dışında kullanımını önlemek için özellikle dikkat edilmelidir.

7.2.3 Görevi Gereği Kişisel Veri İşleyen Çalışanların Özel Olarak Dikkat Etmesi Beklenen Hususlar

Görevlerinin bir gereği olarak ve görevleri esnasında, ENYILDIZ adına Kişisel Verileri işlerken, çalışanlarımızın işbu prosedürde ve **Temiz Ekran – Temiz Masa Politikası'nda** yer alan hususların yanı sıra aşağıda sayılan hususları gözetmeleri beklenmektedir:

- Kişisel Verilerin KVK Mevzuatına uygun bir şekilde ve meşru yollarla işlenmesi gerekir.
- Kişisel Verilerin sadece izin verilen ve açıklanan yasal amaçlar için işlenmesi gerekir.
- İlgili kişiye açıklanmayan veya meşru olmayan bir amaç için kesinlikle veri işlenmemesi ve saklanmaması gereklidir.
- Kişisel Verilerin işlenme amacı için yeterli olması, bu amaçla ilişkili ve bağlantılı olması ve işlenme amacına kıyasla aşırı miktarda veya sayıda olmaması gerekir.
- Kişisel Verilerin doğru ve gerçek olması ve gerektiğinde güncellenmesi gerekir.
- Herhangi bir amaçla işlenen ve kullanılan Kişisel Verilerin bu amaç için gerekli olan süreden daha uzun bir süreyle tutulmaması ve saklanmaması gerekir.

7.2.4 Görevi Gereği Özel Nitelikli Kişisel Veri İşleyen Çalışanların Uyması Gereken Kurallar

Görevlerinin bir gereği olarak ve görevleri esnasında ENYILDIZ adına Özel Nitelikli Kişisel Veri işlemekte olan çalışanların işbu prosedürün diğer maddeleri ve 7.2.3 maddede sözü edilen hususları gözetmelerinin yanı sıra KVK Mevzuatı uyarınca Çalışan Veri Gizliliği Taahhütnamesini imzalamaları gerekmektedir.

7.2.5 Bayi, Şube ve Alt Yüklenici Firma Çalışanlarının Uyması gereken Kurallar

ENYILDIZ adına bayilik altyapısı veya şube sıfatıyla kişisel veri işleme yapan kurum çalışanları da Madde 7.2.3 kapsamı dahilinde hareket etmek ile yükümlüdür. Tarafına tahsis edilen her bilgi kaynağı **Bilgi Teknolojileri Kullanım Politikası'** na uygun kullanılmalıdır. Görevi gereği kişisel veri erişimi mevcut ise Gizlilik Sözleşmesi yapılmalıdır.

8. Kişisel Verilerin Güncelliğinin Korunması

Kişi gruplarının işlenen kişisel verilerinin doğru ve güncel olması için dönemsel kontrol **Kişisel Verilerin Kontrolü Formu** kontrol edilmekte gerektiğinde güncellemeler yapılmaktadır. Periyodik Kontroller dışında oluşan Veri güncelleme talepleri **Kişisel Veri Talepleri Formu** ile ilgili birimlere iletilmekte ve gerekli düzenleme ve/veya düzeltmeler sağlanmaktadır.

Bu kapsamda kişisel verilerin doğruluğunu kontrol etme ve gerekli düzeltmeleri yapmaya tedbirler ENYILDIZ bünyesinde oluşturulmuş olup, KVK Komite toplantılarında yılda en az 1 defa olacak şekilde gözden geçirilmektedir.

9. Kişisel Verilerin Güvenliği Sebebiyle Alınan Teknik ve İdari Tedbirler

Kişisel verilerin güvenliğini sağlamak adına yetkisiz erişim risklerini, kaza ile veri kayıplarını, verilerin kasti silinmesini veya verilerin zarar görmesini engelleyecek makul önlemler alınmaktadır.

Kişisel verilere, erişim yetkisi bulunan kişilerden başkasının erişmesini engellemek adına gereken her türlü teknik ve fiziki önlemler alınır. Bu kapsamda özellikle yetkilendirme sistemi, hiç kimsenin gereğinden fazla kişisel veriye erişmesinin mümkün olmayacağı şekilde kurgulanır. Sağlık verileri gibi özel nitelikli kişisel verilerin güvenliği sağlanırken diğer kişisel verilere göre daha katı önlemler alınır.

Kullanıcı erişimlerinin kısıtlanması, yetkilendirilmesi ve yetkilerin geri alınması için **Erişim Yönetimi Prosedürü** oluşturulmuştur. Mevcut yetki ve izin listesi **Mantıksal ve Fiziksel Erişim Listesi Yetki Matrisi'nde belirtilmiştir**. Yetkilendirilmiş kişilere ait yetkiler yılda en az 1 defa gereken güvenlik kontrollerinden geçirilir.

Ayrıca bu kişiler görev ve sorumlulukları hakkında eğitilir. Kişisel verilere ait tüm kurum çalışanlarına ait genel görev ve sorumluluklar görev tanımlarına eklenmiştir. Komite üyeleri aynı zamanda KVKK Komite sorumluklarını da yerine getirmek ile yükümlüdür.

Tüm kurum çalışanları ile bilgi güvenliği sözleşmeleri yapılmakta olup, Kişisel veri güvenliği hakkında çalışanların farkındalığını arttırmak üzere kurum içi eğitimler düzenlenmektedir. Aynı zamanda Bilgi Güvenliği Politikası hazırlanmış olup, çalışanlar ile paylaşılmıştır.

ENYILDIZ işlenen verilerin güvenliğinin sağlanması amacıyla aşağıdaki yükümlülüklere uyar:

- Kişisel verilerin korunmasına ilişkin konularda hukuka uygun ve dürüst davranma,
- Kişisel verileri doğru, tam ve eksiksiz işleme,

- Güncelliğini kaybeden kişisel verilerin güncellenmesi amacıyla gerekli çalışmaları yapma,
- Kişisel verilerin işlenmesinde herhangi bir hukuka aykırılık fark ettiğinde ilgili yöneticiyi bilgilendirme,
- Kişisel verilere ilişkin kanuni hakların kullanılabilmesi için gerekli yönlendirmeleri yapma.

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kişisel Verilerin Korunması Kanunu uyarınca ve Kişisel Verileri Koruma Kurulu tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde olmak üzere ENYILDIZ tarafından teknik ve idari tedbirler alınmaktadır.

9.1 Teknik Tedbirler

ENYILDIZ tarafından işlenmekte olan kişisel veriler bakımından alınan teknik tedbirler aşağıda sayılmıştır:

•Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

•Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakım kapsamındaki güvenlik önlemleri alınmaktadır.

•Erişim logları düzenli olarak tutulmaktadır.

•Güncel antivirüs sistemleri kullanılmaktadır.

•Güvenlik duvarları kullanılmaktadır.

•Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.

•Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.

•Mevcut risk ve tehditler belirlenmiştir.

•Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.

•Özel nitelikli kişisel veriler için güncel şifreleme/kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.

•Saldırı tespit ve önleme sistemleri kullanılmaktadır.

•Siber güvenlik önlemleri alınmış olup uygulaması sürekli takip edilmektedir.

•Şifreleme yapılmaktadır.

•Taşınabilir bellek, CD, DVD ortamından aktarılan özel nitelikli kişisel veriler şifrelenerek aktarılmaktadır.

•Veri kaybı önleme yazılımları kullanılmaktadır

•Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.

•Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.

•Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.

9.1.1 Bulut Teknolojileri Kullanımında Uyulması Gereken Kurallar

Kişisel verilerin bulutta depolanması, hukuka aykırı işlemenin ve erişimin önlenmesi ile hukuka uygun muhafaza yükümlülüğü olan veri sorumlusunun kendi bilgi teknolojileri sistemi ağından ayrılmasına ve kişisel verilerin bulut depolama hizmeti sağlayıcıları tarafından işlenmesine neden olduğundan, bu durum birtakım riskleri beraberinde getirmektedir.

Bu nedenle, bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının veri sorumlusunca değerlendirilmesi gerekmektedir.

Bu kapsamda, bulutta depolanan kişisel verilerin neler olduğunun detaylıca bilinmesi, yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması önerilmektedir.

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması, kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir.

Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmeye yarayabilecek şifreleme anahtarlarının tüm kopyalarının da yok edilmesi gerekir.

9.2 İdari Tedbirler

ENYILDIZ tarafından işlenmekte olan kişisel verilere ilişkin olarak alınan idari tedbirler aşağıda sayılmıştır:

•Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

•Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

•Çalışanlar için yetki matrisi oluşturulmuştur.

•Gizlilik taahhütnameleri yapılmaktadır.

•Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

•İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.

•Kâğıt yolu ile aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.

•Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.

•Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.

•Kişisel veri güvenliğinin takibi yapılmaktadır.

•Kişisel veriler mümkün olduğunca azaltılmaktadır.

•Kurum içi periyodik ve / veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

•Mevcut risk ve tehditler belirlenmiştir.

•Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmak-tadır.

•Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

•Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda farkındalığı sağlanmaktadır.

Kişisel verilere erişim kayıtları teknik imkânlar elverdiği ölçüde tutulur ve bu kayıtlar düzenli aralıklarla incelenir. KVK Komitesi, kurum içerisinde KVK Rehberi Teknik ve İdari Tedbirler kapsamında yılda az 1 defa olacak şekilde denetim yapmakla yükümlüdür. Denetim **İç Denetim Prosedürüne** uygun olarak **İç Denetim Raporu** hazırlanarak gerçekleştirilir. İç Denetim süresinde bulunan uygunsuzluklar **Düzeltici Faaliyet Raporuna** kaydedilir ve sürecin takibi sağlanır. KVK denetim raporları KVK Komite toplantısında sunulur. Düzeltici Faaliyet sonuçlanana kadar KVK Komitesi takibindedir.

Yetkisiz erişim söz konusu olduğunda derhal soruşturma başlatılır. Kurum soruşturma süreçlerinde KVK Komitesini yetkili kılmıştır. **Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü'** ne uygun olarak gerekli önlem ve tedbirler Komite üyelerince alınır. Herhangi bir veri ihlali veya veri sızıntısının olması veya olmasından şüphe

duyulması halinde KVK Kurumu tarafından yayınlanan Kişisel Veri İhlali Bildirimi Formu doldurularak, KVK Kurumuna bildirimde bulunulur.

10. Kişisel Verilerin Saklanması

10.1 Kişisel Verilerin Saklanma Süresinin Belirlenmesi

Bu kapsamda, öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediği tespit edilmekte, bir süre belirlenmişse bu süreye uygun davranılmakta, bir süre belirlenmemişse şirket uygulamaları ve ticari yaşamının teamülleri uyarınca veya yukarıda anılan işleme amaçlarının gerekli kıldığı süre boyunca saklanmaktadır. Kişisel verilerin saklanmasına ilişkin öngörülen süreler **Veri Envanteri** içerisinde tanımlanmıştır.

10.2 Kişisel Verilerin Saklanma Yöntemlerinin Belirlenmesi

Saklanan verilerin, saklama ve kayıt ortamlarına ilişkin bilgilerde **Veri Envanteri** içerisinde tanımlanmalıdır. Saklama ortamlarına ilişkin tanımlar Erişim Yetki Matrisi'nde belirlenmelidir. Fiziksel ortamlarda saklanan verilere ilişkin Fiziksel Çevresel güvenlik önlemleri alınmış olmalıdır.

10.3 Kişisel Verilerin Saklanmasını Gerektiren Hukuki Sebepler

- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket'in meşru menfaatleri için saklanmasının zorunlu olması,
- Kişisel verilerin Şirket'in herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

11. Kişisel Verilerin İmha Edilmesi

11.1 Kişisel Verilerin İmha Edilmesini Gerektiren Hukuki Sebepler

- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- İlgili kişinin, Kanuni hakları çerçevesinde kişisel verilerinin silinmesi veya yok edilmesi talebinin veri sorumlusu tarafından incelenerek uygun görülmesi,
- İlgili kişinin, Kanun'un 11. maddesindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
- Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması

veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,

- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın bulunmaması,

11.2 Kişisel Verilerin Silinmesi ve İmha Edilmesine Ait Yöntemler

Kişisel verilerin silinmesine ilişkin veri ortamlarına göre gruplandırılmış imha yöntemleri aşağıdaki tabloda belirtilmiştir.

VERİ KAYIT ORTAMI	SİLME YÖNTEMLERİ
Hizmet olarak Uygulama Türü Bulut Çözümleri	Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.
Merkezi Sunucularda Bulunan Dosya ve Klasörlerde Yer Alan Kişisel Veriler	Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir.
Elektronik Veritabanı Ortamlarında Yer Alan Kişisel Veriler	Elektronik veri tabanında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile silinmesi gerekir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlar da ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Taşınabilir ve sabit disklerde tutulan ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

11.3 Veri Kategorisi Bazında Saklanma Süresine Göre İmha Edilecek Veriler

VERİ SAHİBİ	VERİ KATEGORİSİ	VERİ SAKLAMA SÜRESİ
Çalışan	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri	Hizmet akdinin devamında ve hitamından itibaren de 50(elli) yıl müddetle muhafaza edilir.

Çalışan	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri dışında kalan özlük verileri	Hizmet akdinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 10(on) yıl müddetle muhafaza edilir.
Çalışan	İşyeri Kişisel Sağlık Dosyası İçeriğindeki Veriler	Hizmet akdinin devamında ve hitamından itibaren 30(otuz) yıl müddetle muhafaza edilir.
İş Ortağı/Çözüm Ortağı/Danışman	İş Ortağı/Çözüm Ortağı/Danışman ile ENYILDIZ arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, İş Ortağı/Çözüm Ortağı/Danışman çalışanı verileri	İş Ortağı/Çözüm Ortağı/Danışmanın, ENYILDIZ ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.
Ziyaretçi	ENYILDIZ'e ait fiziki mekana girişte alınan Ziyaretçi'ye ait ad, soyad, T.C.K.N., araç plakası ile kamera kayıtları, telefon aramalarında alınan ses kayıtları	2 yıl süre ile saklanır.
İnternet Sitesi Ziyaretçisi	İnternet Sitesi Ziyaretçisi'ne ait ad, soyad, e-posta adresi, gezinme hareketleri bilgileri	2 yıl süre ile saklanır.
Çalışan Adayı	Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler	En fazla 2 yıl olmak üzere özgeçmişin güncelliğini kaybedeceği süre kadar saklanır.
Stajyer(öğrenci)	Stajyere ait staj dosyasında yer alan bilgiler	Staj ilişkisinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 10(on) yıl müddetle muhafaza edilir.
Müşteri	Müşteri'ye ait ad, soyad, T.C.K.N., iletişim bilgileri, ödeme bilgileri ve yöntemleri, gezinme hareketleri bilgileri, telefon aramalarında alınan ses kayıtları, ürün/hizmet tercihleri, işlem geçmişi, özel gün bilgileri	Müşteri'nin, satın almış olduğu her bir ürün/hizmetin sunulmasından itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.
Müşteri	Kamera görüntüleri, araç plaka bilgisi	2 yıl süre ile saklanır.

Eğitim Katılımcısı/Müşteri	Adı Soyadı, Telefon Numarası, e- mail adresi	2 yıl süre ile saklanır.
Potansiyel Müşteri	Potansiyel Müşteri ile ENYILDIZ arasındaki ticari ilişki kurulmasına dair sözleşme görüşmeleri sırasında alınan kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları	2 yıl süre ile saklanır.
ENYILDIZ'in İş birliği İçinde Olduğu Kurum/Firmalar (Tedarikçi, Alt Taşeron, Hizmet Tedarikçisi, Müşteri, Potansiyel Müşteri)	ENYILDIZ' in İş birliği İçinde Olduğu Kurum/Firmalar ile ENYILDIZ arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, ENYILDIZ 'in İş birliği İçinde Olduğu Kurum/Firma çalışanı verileri	ENYILDIZ' in İş birliği İçinde Olduğu Kurum/Firmaların, ENYILDIZ ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.
SÜREÇLER BAZINDA SAKLAMA SÜRELERİ		
Sözleşmelerin hazırlanması	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Takip Sistemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi ve Toplantı	Etkinliğin sona ermesini takiben 2 yıl	Saklama süresinin bitimini takip eden

11.4 Kişisel Verilerin Silinmesi, İmha ve Anonim Edilme Süreçleri

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinde Kanun'a ve ilgili mevzuat hükümlerine, Kurul kararlarına ve işbu Politikaya tamamen uygun hareket edilmektedir.

İmha süreçlerinin takibi için, imha edilen verilere ait veri kategorisi, verinin bulunduğu ortam (Elektronik veya Elektronik olmayan ortam), imha sebebi ve imha tarihi ile imha süreç sorumlusu tarafından kayıt altına alınmalıdır.

11.4.1 Periyodik İmha Süreci

6698 sayılı KVKK Kanununda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda; ENYILDIZ "işleme şartları ortadan kalkmış olan kişisel verileri, işbu Kişisel Verilerin İşlenmesi ve Korunması, İşlenmesi, Saklama ve İmha Politikasında belirtilen silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

Yönetmeliğin 11 inci maddesi gereğince Kurum, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, ENYILDIZ'da her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir. Periyodik imha süreçleri ilk kez 02.10.2023 tarihinde başlar ve her 6 (altı) ayda bir tekrar eder.

11.4.2 Başvuru, Talep veya İstek Üzerine Gerçekleştirilen İmha Süreci

ENYILDIZ, Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Aydınlatma Beyanı ve işbu Kişisel Verileri Saklama ve İmha Politikası uyarınca sorumlu olduğu kişisel verileri İlgili kişi, Kanunun 13'ncü maddesine istinaden ENYILDIZ' a Aydınlatma Beyanın 'da tanımlanmış başvuru yöntemlerini ile başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

1. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; ENYILDIZ talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir.
2. Kişisel verileri işleme şartları tamamen ortadan kalkmamışsa, bu talep ENYILDIZ tarafından Kanunun 13'ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

12. Yürürlülük ve Güncellenebilirlik

İşbu Politika yayımı 02.10.2023 tarihinde yürürlüğe girmiştir. Politika değişen koşullara ve mevzuata uyum amacıyla güncellenebilecektir.