KİŞİSEL VERİLERİ
SAKLAMA VE İMHA POLİTİKASI

İÇİNDEKİLER

1. AMAÇ

1.1. İşbu Kişisel Verileri Saklama ve İmha politikası (**"Politika"**), Yönetmeliğin 5. maddesi gereği İnci GS Yuasa Akü Sanayi ve Ticaret Anonim Şirketi'nin (**"Şirket**") Envanter'i ile birlikte uygulanmak üzere hazırlanmıştır.

1.2. Bu Politika, Şirketi'n tabi olduğu Kanun ve İkincil Mevzuat'a uyumu sağlayabilmek adına Şirket içinde Kişisel Verilerin saklanması ve İmhasına ilişkin genel prosedürlerini ortaya koymaktadır.

1.3. Bu Politika Şirket'in Kişisel Veri içeren belge ve ortamlarının güvenli şekilde saklanmasını, işleme amacı ve şartlarının ortadan kalktığı Kişisel Verilerin İmhasının sağlanmasını amaçlanmaktadır.

1.4. Bu Politika, Şirket'in veri işleme faaliyetleri doğrultusunda düzenlenmiş olup, asılları ve kopyaları dâhil tüm fiziksel ve elektronik belgelere/ortamlara uygulanır.

2. TANIMLAR

2.1. Özel isim olmadıkça ve Politika içerisinde ayrı bir yerde tanımlanmadıkça, büyük harfle yazılan terimler aşağıda tanımlandığı anlamlara gelir.

"Açık Rıza"	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.
"Aktif Kayıtlar"	Şirket'in faaliyetleri kapsamında aktif olarak kullanılmakta olan verileri ifade eder.
"Aktif Olmayan Kayıtlar"	Aktif Kayıtlar kapsamına girmeyen doğrudan Şirket tarafından kullanılmayan ancak ihtiyaç duyulabilecek olan verileri ifade eder.
"Anonim Hale Getirme"	Kişisel Verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder.
"Azami Saklama ve İmha Süreleri Tablosu / Tablo"	EK-1'de yer alan Azami Saklama ve İmha Süreleri Tablosu'nu ifade eder.
"Birim Temsilcisi"	Madde 5.6.'da kendisine verilen anlamı ifade eder.
"BT Departmanı"	Şirket'in Bilgi Teknolojileri Departmanını ifade eder.
"Envanter"	Şirket'in iş süreçlerine bağlı olarak gerçekleştirmekte olduğu Kişisel Veri işleme faaliyetlerinin; Kişisel Veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturulan ve Kişisel Verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen Kişisel Verileri ve veri güvenliğine ilişkin alınan tedbirlerin

	yer verildiği liste/tabloyu ifade etmektedir.
"İkincil Mevzuat"	Kurul ve/veya Kurum tarafından çıkarılan ve/veya ileride çıkarılacak yönetmelikler, ilke kararları, rehberler, talimatlar, emsal kararlar, tebliğ, idari veya yargısal karar ve ilkeleri ifade eder.
"İlgili Kullanıcılar"	Verilerin genel anlamda teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere; Şirket organizasyonu içerisinde veya Şirket'ten aldığı yetki ve talimat doğrultusunda Kişisel Verileri işleyen kişi, birim ve departmanları ifade eder.
"İmha"	Silme, Yok Etme ve/veya Anonim Hale Getirme işlemlerinden herhangi birini veya tamamını ifade eder.
"İrtibat Kişisi"	30.12.2017 tarih ve 30286 sayılı Resmi Gazete'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik'te tanımlandığı üzere, Kurum ile iletişimi sağlamak amacıyla Kurum'a bildirilen gerçek kişiyi ifade eder.
"Kanun"	6698 Sayılı Kişisel Verilerin Korunması Kanunu'nu ifade eder.
"Kayıtlar"	Aktif ve Aktif Olmayan Kayıtlar'ın oluşturduğu bütün kayıtları ifade eder.
"Kişisel Veri/ler"	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.
"Kurul"	Kişisel Verileri Koruma Kurulu'nu ifade eder.
"Kurum"	Kişisel Verileri Koruma Kurumu'nu ifade eder.
"Özel Nitelikli Kişisel Veri"	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.
"Politika"	Madde 1.1.'de kendisine verilen anlamı ifade eder.
"Rehber"	İşbu Politika'nın EK-2'sinde yer verilen; Kurum tarafından 28/29 Kasım 2017 tarihinde yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi'ni ifade eder.
"Silme"	Kişisel Verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini ifade eder.
"Şirket"	Madde 1.1.'de kendisine verilen anlamı ifade eder.
"Veri İşleyen"	Veri sorumlusunun verdiği yetkiye dayanarak onun adına Kişisel Verileri işleyen gerçek veya tüzel kişiyi ifade eder.
"Veri Koruma Komitesi"	İşbu Politika kapsamında kendisine verilen görevleri ve Şirket'in mevzuat kapsamında yükümlülüklerini yerine getirmek üzere; seçilmiş kişilerden oluşan komiteyi ifade eder.

"Veri Sahibi"	Kişisel Verisi işlenen veya yönetilen gerçek kişiyi ifade eder.
"Veri Sorumlusu"	Kişisel Verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.
"Yok Etme"	Kişisel Verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini ifade eder.
"Yönetmelik"	28 Ekim 2017 tarihinde Resmî Gazete'de yayımlanan ve 1 Ocak 2018 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'i ifade eder.

2.2. İşbu Politika'da büyük harfle başlayıp başlamadığına bakılmaksızın "veri işleme" faaliyeti, "*Kişisel Veriler'in 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 işlemi*" ifade etmektedir.

3. İLKELER

Bu Politika, Kanun'da belirlenen aşağıdaki ilkeleri gözetmektedir. Kanun uyarınca Kişisel Verilerin işlenmesinin;

- Hukuka ve dürüstlük kurallarına uygun olması;
- Doğru ve gerektiğinde güncel olması;
- Belirli, açık ve meşru amaçlar için işlenmesi;
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekmektedir.

4. KAPSAM

4.1. Bu Politika Şirket genelinde uygulanmakta, Kişisel Veriler'e ilişkin kurumsal bir çerçeve teşkil etmektedir.

4.2. Şirket, yürüttüğü araştırma ve geliştirme faaliyetleri gereği; T.C. Sanayi ve Teknoloji Bakanlığı, T.C. Ticaret Bakanlığı, TÜBİTAK, AR-GE merkezleri ve teknokent yönetimleri gibi kurum ve kuruluşlarının karar, ilke ve talimatlarına uygun hareket etme yükümlülüğü altında olabilmektedir.

4.3. Şirket'in herhangi bir vesileyle Veri İşleyen sıfatıyla hareket etmesi durumunda işbu Politika yerine, ilgili Veri Sorumlusu sıfatına sahip ilgili kamu kurum ve kuruluşlarına veya kişilere ait politika, prosedür ve ilgili mevzuat hükümleri uygulanacaktır.

5. VERİ KORUMA KOMİTESİ VE BİRİM TEMSİLCİLERİ

5.1. Şirket yetkili organlarınca oluşturulan Veri Koruma Komitesi'nin amacı, Şirket içerisinde başta Envanter'in güncellenmesi, değiştirilmesi ve yönetilmesi, Kişisel Veriler'in saklanması ve İmhası, Kişisel Veriler'e ilişkin Şirket dışından gelecek taleplerin değerlendirilmesi ve yanıtlanması, Kişisel Veriler'e ilişkin Şirket departmanları arasındaki koordinasyonun sağlanması başta olmak üzere Şirket'in ilgili mevzuat kapsamında yükümlülüklerini ve bu Politika'da kendisine verilen görevleri yerine getirmektir.

5.2. İrtibat Kişisi, Kanun ve İkincil Mevzuat tahtındaki yükümlülüklerini Veri Koruma Komitesi'nin bilgi, gözlem ve talimatları dâhilinde yerine getirir. Kanun ve İkincil Mevzuat tahtında İrtibat Kişisi tarafından yerine getirileceği ifade edilen iş ve işlemlerin işbu Politika tahtında "*Veri Koruma Komitesi tarafından yerine getirileceği*" minvalindeki hükümler, "*Veri Koruma Komitesi bilgi, gözlem ve talimatları dâhilinde İrtibat Kişisi tarafından yerine getirilir*" minvalinde anlaşılmalıdır.

5.3. Veri Koruma Komitesi, Şirket içerisinde Kişisel Veri işleme, saklama ve anonimleştirme dâhil her türlü Kişisel Veri aktivitesini izler, ilgili tavsiyeleri verir ve organizasyonları yapar. Veri Koruma Komitesi'ne yönelik bilgileri EK-4'te yer verilmiştir.

5.4. Veri Koruma Komitesi, Kurum ve Kurul gibi Kişisel Veriler'e ilişkin yetkilendirilmiş kurumlar ile iş birliği yapar, Kişisel Veriler'e ilişkin İrtibat Kişisi vasıtasıyla iletişim ve temasları yürütür. Kişisel Veri işleme faaliyetleri ile ilgili olarak, Kurum ve Kurul gibi Kişisel Verilere ilişkin denetleme otoriteleri için İrtibat Kişisi vasıtasıyla irtibat ve iletişim noktası görevini üstlenir ve gerektiği takdirde ilgili kurum ve kuruluşlarla İrtibat Kişisi vasıtasıyla yazışmaları yapar.

5.5. Veri Koruma Komitesi, görevini yerine getirirken, işleme faaliyetlerine ilişkin riskleri gözetir ve işleme faaliyetinin niteliğini, kapsamını, içeriğini ve amaçlarını dikkate alır.

5.6. Veri Koruma Komitesi'ne ilaveten, her bir Şirket içi birim tarafından Kişisel Veriler konusundaki hassasiyetin gözetilmesi ve Şirket tarafından yükümlülüklerin yerine getirilmesinin koordine edilmesi amacıyla bir çalışan ("**Birim Temsilcisi**") temsilci olarak belirlenir.

5.7. Veri Koruma Komitesi, Şirket içi birimlerin Kanun ve İkincil Mevzuat'a uyumu konusundaki tetkik, inceleme ve soruşturmalarını Birim Temsilciler'i üzerinden yerine getirir.

5.8. Birim Temsilcileri, Veri Koruma Komitesi tarafından kendilerine verilen talimatları yerine getirmek, sorulan sorulara cevap vermek ve istenen organizasyonun ilgili birim nezdinde yerine getirilmesini gözetlemek ve raporlamakla yükümlüdür.

5.9. Birim Temsilcileri, Veri Koruma Komitesi tarafından kendilerine bildirim yapılıp yapılmadığına bakılmaksızın kendi birimlerinin Kanun ve İkincil Mevzuat'a uygun hareket edip etmediğini; verilerin hukuka uygun işlenip işlenmediğini, muhtemel veri ihlaline sebep olabilecek uygulamaların bulunup bulunmadığını, ilgili birim nezdinde Kişisel Verilerin işlenmesi, korunması ve aktarılmasına ilişkin meydana gelebilecek tereddütleri Veri Koruma Komitesi'ne iletmek ve raporlamakla yükümlüdür.

5.10. Veri Koruma Komitesi ve Birim Temsilcileri, Kanun'a, İkincil Mevzuat'a, Politika'ya, Envanter'e ve Kişisel Verilere ilişkin Şirket tarafından kullanılmakta olan doküman, plan ve ilkelere hâkim ve vakıf olmakla yükümlüdür.

5.11. Tüm Şirket içi birimleri ve çalışanları Veri Koruma Komitesi ile uyumlu bir şekilde faaliyet göstermek zorundadır. Veri Koruma Komitesi ile birlikte Birim Temsilcileri bu Politika'nın uygulanmasından sorumludur.

5.12. Bu Politika'nın uygulanmasıyla ilgili olan sorular, Veri Koruma Komitesi'ne iletilir.

6. SAKLAMA

6.1. Kişisel Veriler'in Saklanmasını Gerektiren Sebepler

Şirket tarafından Kişisel Veriler, Envanter'de her bir veri işleme sürecine ilişkin özel olarak belirtilen hukuki sebepler doğrultusunda işlenmektedir. Bu hukuki sebepler Kanun'un 5. maddesinin 2. fıkrasında da zikredilen ve aşağıda sayılanlardır:

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) Veri Sahibi'nin kendisi tarafından alenileştirilmiş olması,
f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve
g) Veri Sahibi'nin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

6.2. Fiziksel Kayıtlar'ın Saklanması

Fiziksel Kayıtlar, kâğıt üzerindeki kayıtlar, sözleşmeler, tutanaklar, faturalar ve fotoğraflar gibi kâğıt ve benzeri ortamlarda bulunan kayıtlardan oluşur.

Aktif Kayıtlar ve günlük faaliyetler gereği kolayca erişilmesi gereken Kayıtlar, Şirket aktif çalışma alanlarında saklanmaktadır.

Aktif Olmayan Kayıtlar, Şirket'in arşivine iletilir ve burada arşivlenir. Arşive gönderilen verilere, İlgili Kullanıcı'nın erişimi kesilir ve sadece arşiv yönetimince, arşivin korunması, düzenlenmesi ve bakımı amacıyla erişilebilir.

6.3. Elektronik Kayıtlar'ın Saklanması

Elektronik Kayıtlar, ses kayıtları, fotoğraflar, videolar, ve görsel ve işitsel ortamlar dâhil birçok ortamda yer alan dijital kayıtlardan oluşmaktadır. Kişisel Veriler'in yer aldığı Elektronik Kayıtlar, doğru, güncel ve Kişisel Verileri işlemesi gereken kişilerce erişilebilir olacak şekilde, yetkisiz üçüncü kişilerce erişimi ve işlemeyi engelleyecek düzeyde güvenli yazılımlarda, Şirket'e ait ve/veya Şirket'in kullandığı veri tabanlarında, program ve uygulamalarda, e-posta hesaplarında, kişisel bilgisayarlarda ve mobil cihazlarda saklanmaktadır.

Elektronik Kayıtlar'ın, kaybedilmeye, değiştirilmeye ve izinsiz yok edilmeye, saklanma süreçlerinde erişime karşı korunmalarını sağlamak ve eksiksiz, doğru ve okunaklı olmasını temin etmek için yeterli koruma önlemleri, BT Departmanı'nın önerisi ve Veri Koruma Komitesi'nin onayı ile alınmakta ve uygulanmaktadır.

6.4. Saklama Süreleri

Saklama süreleri, ilgili süreç ve faaliyetlerin kendi içinde farklılık göstermesi sebebiyle Envanter'de özel olarak her bir veri işleme süreci bazında tespit edilmiştir. Bu sebeple saklama sürelerinin belirlenmesinde öncelikli olarak Envanter'e başvurulur. Bununla birlikte; Veri Sahibi ilgili kişi gruplarına yönelik herhangi bir veri işleme faaliyeti kapsamında uygulanan en uzun saklama süreleri, EK-1'de yer alan Azami Saklama ve İmha Süreleri Tablosu'nda verilmiştir.

7. İMHA

İmha işlemi temel olarak Kişisel Veri'yi silme, Yok Etme ve Anonim Hale Getirmeyi ihtiva etmektedir. Silme, Yok Etme ve Anonim Hale Getirme eylemlerinden her birisi ayrı bir İmha yöntemidir. Diğer bir deyişle İmha eylemini icra ederken sayılan 3 yöntemden birisi tercih edilmelidir.

Silme, Yok Etme ve Anonim Hale Getirmeye ilişkin detaylar, işbu 7. maddenin alt başlıklarında detaylı olarak izah edilmektedir. Söz konusu detayların örnekler ile açıklandığı ve bu noktada okuyucunun daha iyi anlamasına imkân verir mahiyetteki Rehber, işbu Politika'nın EK-2'sinde yer almaktadır.

7.1. Kişisel Veriler'in İmhasını Gerektiren Sebepler

İşbu Politika kapsamında "İmha" terimi, Tanımlar kısmında da yer verildiği üzere, silme, Yok Etme ve Anonim Hale Getirme işlemlerinin tamamını kapsayan bir üst kavram olarak kullanılmaktadır.

Kişisel Veriler'in İmha edilmesine ilişkin haller aşağıda belirtilmektedir. İmha'nın nasıl gerçekleştirileceğine yönelik aksiyonlar, somut olayın koşullarına ve Kanun, Yönetmelik ve İkincil Mevzuat hükümlerine göre Veri Koruma Komitesi tarafından belirlenir.

- Veri Sahibi Kişisel Veri'nin İmhasını talep ettiğinde,
- Açık Rıza'ya dayanan Kişisel Veri işleme ve saklama süreçlerinde Veri Sahibi'nin Açık Rızası'nı geri alması halinde,
- Kurul'un usulüne uygun olarak Kişisel Veri'nin İmhasını talep etmesi halinde,
- Kişisel Veriler'in işleme şartlarının tamamının veya Kişisel Veriler'in işlenmesine ilişkin amaçların ve kanuni/sözleşmesel gerekliliklerin ortadan kalkması halinde ve

- Belirlenmiş olan Kişisel Veri saklama süresinin sona ermesi halinde.

7.2. Veri Sahibi'nin İmha Talebi

Veri Sahibi Kişisel Veriler'inin İmhası'nı talep ettiğinde; Şirket tarafından öncelikle Envanter'de yer verilen ve ek olarak tespit edilecek işleme amaçları ve veri işleme şartlarının tamamının ortadan kalkıp kalkmadığı değerlendirilir. Amaç ve şartların devam ettiği yönünde sonuca varılırsa Veri Sahibi'nin talebi ve gerekçesi belirtilerek yazılı olarak reddedilebilir. Yazılı karar, en kısa sürede ve en geç 30 (otuz) gün içerisinde talepte bulunan Veri Sahibi'ne gönderilir. Amaç ve şartların devam etmediği sonucuna varılırsa aşağıda yer alan İmha işlemleri uygulanır ve yine en kısa sürede ve en geç 30 (otuz) gün içerisinde talepte bulunan Veri Sahibi'ne yazılı olarak bilgi verilir.

7.3. Veri Sahibi'nin Açık Rızası'nı Geri Alması

Veri Sahibi'nin Kişisel Verileri'nin İmhasından farklı olarak Açık Rızası'nı geri aldığını iletmesi halinde; Şirket tarafından öncelikle ilgili Kişisel Veriler'in sadece Açık Rıza'ya dayanılarak işlenip işlenmediği değerlendirilir. Bu noktada Envanter'de ilgili işleme sürecinin amacı tespit edilir ve işlemeye neden olacak herhangi bir ek veya değişik amaç olup olmadığı teyit edilir. İşleme faaliyetinin Açık Rıza'ya dayanmadığı veya Açık Rıza yanında başkaca hukuki sebeplerin olduğu sonucuna varılırsa, Veri Sahibi'nin talebi, gerekçesi belirtilerek yazılı olarak reddedilebilir. Yazılı karar, en kısa sürede ve en geç 30 (otuz) gün içerisinde talepte bulunan Veri Sahibi'ne gönderilir. Veri işleme faaliyetinin sadece Açık Rıza'ya dayandığı sonucuna varılırsa aşağıda yer alan İmha işlemleri uygulanır ve yine en kısa sürede ve en geç 30 (otuz) gün içerisinde talepte bulunan Veri Sahibi'ne yazılı olarak bilgi verilir.

7.4. Periyodik Gözden Geçirme ve İmha

İmha sebeplerinden Kişisel Veriler'in işleme şartlarının tamamının veya amaçların veya kanuni/sözleşmesel gerekliliklerin ortadan kalkıp kalmadığını ve belirlenmiş olan Kişisel Veri saklama sürelerinin sona erip ermediğini tespit etmek amacıyla Şirket içerisinde 6 (altı) ayda bir periyodik olarak gözden geçirme işlemi uygulanır.

Gözden geçirme işlemi, Veri Koruma Komitesi gözetiminde her bir Şirket departmanı tarafından kendi iç süreçlerine ilişkin olarak yürütülür ve sonuçlar Veri Koruma Komitesi'ne raporlanır. Birim Temsilcisi, bir önceki cümlede ifade edilen departman içi süreçlerin gözlemlenmesi, raporlanması ve tereddütlerin giderilmesi konusunda sorumludur. Raporlarda özellikle departman içinde hangi türde Aktif Kayıtlar'ın bulunduğu, hangi Kayıtlar'ın arşivleneceği ve hangi Kayıtlar'ın İmha edileceği belirtilir.

Veri Koruma Komitesi kendisine iletilen raporları değerlendirir, gerekli kontrolleri yapar, arşivleme ve İmha'ya ilişkin kararları verir. İmha edilmesine karar verdiği Kayıtlar'a ilişkin İmha yöntemlerinden uygun olanı seçer.

İlk periyodik İmha her yıl Haziran ayının sonunda, ikincisi ise her takvim yılının sonunda yapılır. Periyodik gözden geçirme dönemi haricinde işleme şartları ve amaçlarının ortadan kalktığı tespit edilen Kayıtlar, takip eden ilk periyodik İmha esnasında İmha edilir.

7.5. İmha Prosedürünün Başlatılması

Fiili olarak İmha prosedürü, Veri Koruma Komitesi'nin kararı ile başlatılır. Kararda, İmha edilecek verilerin türlerine, İmha gerekçelerine, İmha yöntemine, fiziken İmha'yı gerçekleştirecek kişilerin kimler olduğuna İmha tarihine ve İmha işleminin ispat edilebilir şekilde nasıl kayıt altına alınacağına yer verilir.

7.6. İmha Yöntemleri

7.6.1. Yok Etme:

Kayıtlar'ın yok edilmesi, Kişisel Verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi ile sağlanır. Kişisel Veriler'in yok edilmesi için verilerin bulunduğu tüm kopyaların tespit edilmesi, geri getirilememesi, tekrar kullanılamaması ve Kişisel Veriler'e hiçbir şekilde erişilememesi gerekir.

i. Fiziksel Kayıtlar'ın Yok Edilmesi

Fiziksel Kayıtlar, kağıt İmha veya kırpma makineleri ile anlaşılmaz boyutta (mümkünse hem dikey hem de yatay şekilde parçalanarak) veya okunmasını imkânsız kılacak başka yöntemlerle (örneğin; birleştirilemeyecek ufak parçalara keserek veya fiziksel kaydı uygun bir ortamda yakarak) İmha edilir.

ii. Elektronik Kayıtlar'ın Yok Edilmesi

Elektronik Kayıtlar'a ilişkin tüm işlemlerde BT Departmanı'nın onay veya gözetimi aranır.

Elektronik Kayıtlar, aşağıdaki şekillerde yok edilebilir:

- Elektronik kaydın bulunduğu fiziksel cismi Yok Etme suretiyle (Örneğin: CD, DVD'lerin yakılması, küçük parçalara ayrılması, eritilmesi),
- Üzerine yazma suretiyle,
- De-manyetize etme suretiyle,
- Kişisel Verilerin yer aldığı flash tabanlı sabit disklerin silme komutlarını kullanmak, bulunmuyorsa üreticisinin önerdiği yöntemleri kullanmak suretiyle,
- Geri getirilemeyeceği, tekrar erişilemeyeceği veya kullanılamayacağı teknik olarak teyit edilmek suretiyle mümkün olan diğer yöntemleri kullanmak suretiyle.

Verilerin kayıt edildiği birimi/parçası/bölümü/ortamı çıkartılabilir olan elektronik ortamlarda yer alan Kişisel Veriler, tüm veri kayıt ortamlarının söküldüğü doğrulandıktan sonra birimin özelliğine uygun Yok Etme yöntemi seçilir.

Bulut sistemlerinde saklanan Kişisel Veriler teknik açıdan genel kabul gören kriptografik yöntemlerle şifrelenir. Farklı bulut depolama alanı kullanılması veya farklı bulut hizmet sağlayıcılardan hizmet alınması halinde, her biri için farklı şifreleme anahtarı kullanılır. Hizmet sağlayıcılardan alınan bulut

hizmetinin sona erdirilmesi halinde Kişisel Veriler'in tekrar erişilmesini veya kullanılmasını sağlayan şifre ve anahtarlar yok edilir.

7.6.2. Silme:

Silme işlemi, Kişisel Veriler'in İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi ile gerçekleştirilir. Kısaca İlgili Kullanıcılar ile Kişisel Veriler arasındaki bağlantının ortadan kaldırılmasıdır.

i. Fiziksel Kayıtlar'ın Silinmesi

Fiziksel Kayıtlar'da yer alan Kişisel Veriler, karartma veya arşivleme yöntemi kullanılarak silinebilir. Karartma yönteminde ilgili evrak üzerindeki Kişisel Veriler'in, mümkün olan durumlarda kesilmesi veya çıkartılması, bunun mümkün olmaması halinde ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemez hale getirilmesi şeklinde yapılabilir.

Arşivleme yönteminde ise Aktif Kayıtlar'ın arşivlenerek Aktif Olmayan Kayıtlar'a dönüştürülmesi suretiyle İlgili Kullanıcılar ile Kayıtlar arasındaki bağlantı ortadan kaldırılabilir. Bu durumda;

- Arşive kaldırılacak olan Kayıtlar belirlenir,
- Kayıtlar'ın içeriği, adedi veya Kişisel Veri içermeyen belirlenebilir unsurları, hangi birim tarafından, hangi tarihte Şirket arşiv yetkililerine teslim edildiği üç nüsha halinde tutanak altına alınır.
- Tutanakların bir nüshası Kayıtlar'ı teslim eden birime, bir nüshası arşiv yetkililerine ve bir nüshası da Veri Koruma Komitesi'ne verilir.
- Arşiv yetkililerince Kişisel Veri içeren Kayıtlar, arşiv alanında ayrı bir bölümde, İlgili Kullanıcılar başta olmak üzere herhangi bir Şirket birimi ve çalışanın erişemeyeceği şekilde arşivlenir.
- İlgili arşiv alanına ancak temizlik, bakım-onarım ve gözetim amacıyla erişilebilir. Bu durumlar haricinde Veri Koruma Komitesi'nin yazılı kararı olmadıkça Şirket çalışanı ve üçüncü kişiler alana ve Kayıtlar'a erişemez.

ii. Elektronik Kayıtlar'ın Silinmesi

Elektronik Kayıtlar için silme işlemi gerçekleştirilirken genel olarak aşağıdaki sıralama izlenir:

- Silme işlemine konu teşkil edecek Kişisel Veriler'in ve bulunduğu ortamın belirlenmesi,
- Yetki matrisi kullanılarak İlgili Kullanıcılar'ın tespit edilmesi,
- İlgili Kullanıcılar'ın erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi,
- İlgili Kullanıcılar'ın Kayıtlar'a erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması,
- Yukarıda yer alan işlemler gerçekleştirilemiyorsa İlgili Kullanıcılar'ın erişiminin olmadığı bir dijital alana gerekli tüm teknik güvenlik önlemleri alınarak geçirilmesi ve ilk ortamda herhangi bir Kayıt bırakılmaması,

- Yapılan işlemlerin kayıt altına alınması.

Silinen Elektronik Kayıtlar'ın bulunduğu ortama, dosyaya veya sunucuya sadece sistemin çalışmasının sürdürülebilmesi ve güvenliğinin sağlanması amacıyla Veri Koruma Komitesi tarafından belirlenecek BT Departmanı çalışanları erişebilecektir.

7.6.3. Anonim Hale Getirme:

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartarak ya da değiştirerek, Veri Sahibi'nin kim olduğunun saptanabilmesinin veya ayırt edilebilir olmasının önlenmesidir.

Saptama veya ayırt edebilmeye ilişkin niteliklerinin kaybolması veya engellenmesi sonucunda bir kişiyi işaret etmeyen veriler, anonim hale getirilmiş sayılır. Sonuç olarak; Anonim Hale Getirme işlemi yapılmadan önce bir kişiyi tespit etmeye yarayan veriler, işlem sonrasında gerçek kişi ile bağlantı kurulamayacak hale getirilmiş olacaktır.

Anonim hale getirme işlemi için gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle kullanılabilmektedir. Bunlardan bir kısmı aşağıda yer almaktadır:

i. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

- Değişkenleri Çıkartma
- Kayıtları Çıkartma
- Alt ve Üst Sınır Kodlama
- Bölgesel Gizleme
- Örnekleme
- Genelleştirme
- Global Kodlama

ii. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

- Mikro-Birleştirme
- Veri Değiş-Tokuşu
- Gürültü Ekleme

iii. Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler

- K-Anonimlik
- L-Çeşitlilik
- T-Yakınlık

8. TEKNİK VE İDARİ ÖNLEMLER

8.1. Şirket, Kişisel Veriler'in saklanması ve güvenliğinin sağlanması için Kişisel Veriler'in niteliğini ve durumunu gözeterek, yetkisiz değiştirilmeyi, kaybolmayı, muhtemel hasarı, izinsiz işleme veya erişimi, insan eylemi veya doğal veya fiziksel ortamın etkilerine maruz kalmak suretiyle ortaya çıkacak riskleri ve benzeri diğer zararları önlemek için fiziksel, teknik ve idari önlemleri teknik şartlar ve ekonomik koşulları gözeterek almayı hedefler.

8.2. Bu minvalde Şirket, kendi içindeki her bir iş süreci ve faaliyet için almakta olduğu teknik ve idari tedbirleri, Envanter'de detaylı olarak belirtmiştir. Veri Koruma Komite'si Envanter'de her bir iş süreci ve faaliyet için alındığı ifade edilen tedbirlerin gözetilmesinden, kontrolünden ve tetkikinden sorumludur. Veri Koruma Komitesi, söz konusu kontrol işlemlerini bizzat veya Birim Temsilcileri eliyle yerine getirebilir. Alınan teknik ve idari tedbirler, ayrıca işbu Politika'nın EK-5'inde yer almaktadır.

8.3. Kişisel Verilere erişim yetkisi bulunan tüm Şirket çalışanları, Kişisel Veri güvenliği konusundaki farkındalığın artması ve bilinçlenmenin sağlanması amacı ile periyodik eğitimlerden geçirilir.

8.4. Şirket çalışanları ve birimleri işledikleri veya eriştikleri bütün Kişisel Veriler'in güvenli şekilde tutulmasını temin etmekle yükümlüdürler. Kişisel Veriler, herhangi yetkisiz bir üçüncü kişiyle sözlü, yazılı veya başka şekilde paylaşılamaz, ifşa edilemez.

8.5. Kişisel Veri içeren fiziksel kopyalar kilitli dolaplarda veya kilitli çekmecelerde tutulur; elektronik kopya ise şifrelenir, taşınabilir bir ortamda tutulmakta ise dosyanın kendisi de şifrelenir.

8.6. Kişisel Veriler'i içeren Kayıtlar, genel ilke olarak elektronik veya fiziksel olarak personelin evinde, dizüstü bilgisayarlarda veya diğer kişisel taşınabilir cihazlarda ve işyeri dışındaki diğer sahalarda tutulamaz. Şahsi cihazlar ile erişilebilen e-posta hesaplarının güvenliği mutlaka çalışanın kendisi tarafından alınır, iş amaçlı kullanılan mobil cihazlar ekran kilidiyle koruma altına alınır.

8.7. Kişisel Veriler'in işin gereği olarak işyeri sahası dışında tutulmasının gerekli veya uygun olduğuna kanaat getirilirse, ilgili birim veya departman durumu derhal Veri Koruma Komitesi'ne bildirir. Veri Koruma Komitesi, Kişisel Veriler'in güvenliğinin sağlanabileceğine kanaat getirirse bu duruma izin verebilir.

8.8. Veri Koruma Komitesi'nin kararı ile Şirket ve ilgili birim veya çalışan arasında işyeri sahası dışında Kişisel Veri tutmaya ilişkin belirlenecek özel usul ve esasların yer aldığı bir protokol imzalanır ve bu protokolde çalışanın sorumlulukları belirtilir.

8.9. Taşınabilir elektronik cihazlarda veya silinebilir dijital veya fiziki ortamlarda depolanan verilerden söz konusu ekipmanı yöneten veya alanı idare eden çalışan sorumludur. Bu kişi, aynı zamanda aşağıdaki unsurları sağlamakla yükümlüdür:

- İlgili cihaz, ortam ve alanlarda yer alan verilerin zarara uğrama ihtimallerine karşılık bu verilerin yeterli güvenlik önlemlerinin alındığı ortamlarda saklanan yedeklerini almaya ve alınmasını sağlamaya,

- Özel Nitelikli Kişisel Veriler'in ve diğer hassas verilerin ayrı bir alanda saklamaya, bu alanları uygun şekilde şifreli veya kilitli tutmaya,
- Özel Nitelikli Kişisel Veriler'i ve diğer hassas verileri içeren dizüstü bilgisayar, mobil cihazlar ve bilgisayar bazlı kayıt ortamlarını (USB cihazlarları, CDler gibi) ofiste gözetimsiz bırakmamaya,
- Gerekli gördüğü ek güvenlik ve koruma önlemlerinin alınması için Veri Koruma Komitesi'ne başvurmaya.

8.10. Flash disk, harici bellek gibi taşınabilir medya ortamlarında yer alan Kişisel Veriler, şifreli olarak saklanır ve bu ortamlara uygun yazılımlar kullanılarak silinir.

8.11. Çalışanlar, programlar üzerinde kayıtlı olan, Kişisel Veri içeren Kayıtlar'ı gerekmedikçe kullandıkları bilgisayara kopyalayamaz veya indiremez, indirmesinin veya kopyalamasının gerekli olması halinde kullanım amacı sona erdiğinde kopyayı derhal siler.

8.12. Arızalanan ya da bakıma gönderilen cihazlar olması halinde, öncelikle içerisinde Kişisel Veri içeren Kayıt olup olmadığı kontrol edilir. İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara teslim edilmesi gerekiyorsa içlerinde yer alan Kişisel Veriler, "Yok Etme" başlığı altında detayları belirtildiği şekilde önceden yok edilir. Yok Etme'nin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamı sökülerek saklanır veya sadece arızalı olan parça üretici, satıcı, servis gibi üçüncü kurumlara gönderilir.

8.13. Şirket'e hizmet vermek üzere Şirket tesislerine giren veya uzaktan Şirket sistemlerine erişen tedarikçilerin Kişisel Veriler'e erişmesi engellenir, kopyalayarak Şirket dışına çıkartmaması için gerekli teknik önlemler alınır. BT Departmanı bu hususlara ilişkin gerekli bilgiyi ve önerilerini derhal Veri Koruma Komitesi'ne bildirir.

8.14. Veri Koruma Komitesi, Şirket'in sözleşmesel ilişkiye girdiği ve gireceği üçüncü kişiler ile, söz konusu üçüncü kişilerin Kişisel Veri alıcısı olması veya aktarıcısı olma ihtimallerini dikkate alarak bunlar ile veri koruma ve gizlilik sözleşmelerinin tanzim edilmesine yönelik gerekli önlemleri bizzat veya Birim Temsilcisi eliyle almaya özen gösterir.

8.15. Şirket'in verdiği yetkiye dayanarak onun adına Kişisel Verileri işleyen Veri İşleyenler'in de Kişisel Verilerin korunması noktasında kontrol edilmesi ve gözlemlenmesinden, hukuka aykırılıkların tespiti ve risklerin belirlenmesinden Veri Koruma Komitesi sorumludur. Kimlerin Veri İşleyen olarak nitelendirilebileceğine yönelik detaylı izahat, işbu Politika'nın EK-3'ünde yer alan; Kurum tarafından hazırlanarak yayımlanan Örneklerle Kişisel Verilerin Korunması Rehberi'nde (59. Ve devamı sayfalarında) ifade edilmektedir.

9. POLİTİKA'NIN İHLALİ

9.1. Şirket çalışanlarının, Kişisel Veriler'i yetkisiz olarak paylaşmaları veya bu Politika'yı ihlal etmeleri halinde; bu durum, bir disiplin cezası gerektirebilir ve/veya duruma göre çalışanın İş Kanunu'nun 25. maddesi uyarınca iş akdinin haklı sebeple feshine neden olabilir.

9.2. Şirket tedarikçilerinin Kişisel Veriler'i yetkisiz olarak paylaşmaları veya işbu Politika'yı ihlal etmeleri halinde; bu durum, tedarikçiler aleyhine yaptırım uygulanmasına ve/veya tedarik sözleşmesinin feshine neden olabilir.

9.3. İşbu Politika'nın ihlal edilmesi halinde Veri Koruma Komitesi, ihlali gerçekleştiren Şirket çalışanı veya başkaca kişilere ilişkin inceleme yapma yetkisine sahiptir. Veri Koruma Komitesi gerekli gördüğü takdirde, ihlalden kaynaklanan riski azaltmak için uygun düzenleyici önlemleri alır.

9.4. İhlalin ciddiyeti dikkate alınarak, çalışan, tedarikçi veya üçüncü kişiler hakkında yaptırım kararı alabilir ancak alınan kararın niteliğine bağlı olarak (Örn: çalışanın işten çıkarılması veya tedarikçinin sözleşmesinin feshedilmesi) kararın uygulanması Şirket yönetiminin onayına tabi olabilir.

10. ÇEŞİTLİ HÜKÜMLER

10.1. Politika'nın Yayınlanması ve Şirket İçi Birimlere Bildirimi

Bu Politika Şirket web sitesinde yayınlanır. Ayrıca Şirket birimlerine ve çalışanlarına bildirilir.

10.2. Politika'nın Yürütülmesi

Bu Politika'nın uygulanması ve yürütülmesi ile Politika'ya uyumun sağlanmasından Veri Koruma Komitesi ve Birim Temsilcileri sorumludur.

10.3. Değişiklikler

Şirket bu Politika'da her zaman değişiklik ve güncelleme yapma yetkisini uhdesinde tutmaktadır.

EKLER

1- EK-1: Azami Saklama ve İmha Süreleri Tablosu
2- EK-2: Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi
3- EK-3: Örneklerle Kişisel Verilerin Korunması Rehberi
4- EK-4: Veri Koruma Komitesi Hakkında
5- EK-5: Teknik ve İdari Tedbirler

EK-1: AZAMİ SAKLAMA VE İMHA SÜRELERİ TABLOSU

Bu Saklama ve İmha Süreleri Tablosu, İnci GS Yuasa Akü Sanayi ve Ticaret Anonim Şirketi'nin Kişisel Verilerin Saklanması ve İmhası Politikası'nın eki olarak düzenlenmiştir.

Şirket içerisinde her bir veri işleme faaliyetine ilişkin özel saklama sürelerine Envanter'de yer verilmiştir. Şirket tarafından aynı kişi grubuna ilişkin farklı veri işleme faaliyetleri kapsamında farklı saklama süreleri belirlenmiş ve uygulanmaktadır.

Tablo'da, Envanter'de Veri Sahibi ilgili kişi grubuna yönelik herhangi bir veri işleme faaliyeti kapsamında uygulanan en uzun saklama süresine yer verilmiştir.

Tablo'da yer verilen saklama sürelerinin azami olmasından dolayı herhangi bir başka veri işleme sürecinde aynı kişi grubuna yönelik belirlenmiş daha kısa bir saklama süresi bulunabilir. Bu nedenle her bir veri işleme sürecinde öncelikli olarak Envanter'de yer alan süreler uygulama alanı bulacaktır.

Kişi Grubu	Azami Saklama ve İmha Süreleri
Çalışan	Azami olarak iş akdinin sona ermesinden itibaren 15 yıl boyunca saklanmaktadır.
Çalışan Adayı	Azami olarak iş başvurusu değerlendirme sürecinin sona ermesini takip eden ilk periyodik İmha faaliyetine dek saklanmaktadır.
Çalışan Aile Bireyi	Azami olarak iş akdinin sona ermesinden itibaren 10 yıl boyunca saklanmaktadır.
Habere/Paylaşıma Konu Olan Kişiler	Kanuni zorunlulukların ortaya çıkması, açık rızanın geri alınması veya mahkeme kararı ile haberlerin/paylaşımların yayından kaldırılması hükmedilene kadar saklanacaktır.
Hissedar/ Ortak	Azami olarak hukuki ilişkinin sona ermesinden itibaren 10 yıl boyunca saklanmaktadır.
İş Ortakları	Azami olarak hukuki ilişkinin sona ermesinden itibaren 10 yıl boyunca saklanmaktadır.
Potansiyel İş Ortakları	İlgili kişinin verisini alenileştirmiş olması durumunda, kişisel verilerinin silinmesini talep edene kadar; açık rızaya binaen işlenmesi halinde açık rıza geri alınana kadar saklanmaktadır.
Müşteri	Azami olarak müşterilerle akdedilmiş sözleşmelerin süresinin sona ermesinden itibaren 10 yıl boyunca saklanmaktadır.
Potansiyel Müşteri	Şirket ile hukuki bir ilişkiye girilmiş olması halinde azami olarak hukuki ilişkinin sona ermesinden itibaren 10 yıl boyunca saklanmaktadır. Şirket ile herhangi bir hukuki ilişkiye girilmemiş olması durumunda azami olarak 3 yıl boyunca saklanmaktadır. Potansiyel müşteri tarafından verilerin işlenmesine açık rıza gösterilmiş olması halinde açık rıza geri alınana

	kadar saklanmaktadır.
Tedarikçi	Azami olarak tedarikçi sözleşmelerinin sona ermesinden itibaren 10 yıl boyunca saklanmaktadır.
Topluluk Şirketleri	Azami olarak hukuki ilişkinin sona erdiği tarihten itibaren 10 yıl boyunca saklanmaktadır.
Stajyer	Azami olarak iş ilişkisinin sona ermesinden itibaren 10 yıl boyunca saklanmaktadır.
Stajyer Adayı	Azami olarak iş başvurusu değerlendirme sürecinin sona ermesini takip eden ilk periyodik İmha faaliyetine dek saklanmaktadır.
3. Kişiler	Hukuki ilişkinin tesis edilmediği ihtimallerde azami olarak 1 yıl boyunca saklanmaktadır.
Kiraya Veren	Azami olarak hukuki ilişkinin sona erdiği tarihten itibaren 10 yıl boyunca saklanmaktadır.
Ziyaretçiler	Güvenlik kamera kayıtları 6 ay boyunca, bunlar dışındaki veriler azami olarak verinin elde edilmesini takip eden ilk periyodik İmha sürecine dek saklanmaktadır. Çerez kullanımlarında ise çerezler silinene kadar saklanmaktadır.

EK-2: Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi

Not 1: Rehber'i açmak için aşağıda resme farenin sol tuşu ile çift tıklatınız.

Not 2: Rehber'i açmada sorun yaşadıysanız lütfen aşağıdaki linki tıklayınız:

https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20S%C4%B0L%C4%B0NMES%C4%B0,%20YOK%20ED%C4%B0LMES%C4%B0%20VEYA%20ANON%C4%B0M%20HALE%20GET%C4%B0R%C4%B0LMES%C4%B0%20REHBER%C4%B0.pdf

EK-3: Örneklerle Kişisel Verilerin Korunması Rehberi

Not 1: Belgeyi açmak için aşağıda resme farenin sol tuşu ile çift tıklatınız.

Not 2: Belgeyi açmada sorun yaşadıysanız lütfen aşağıdaki linki tıklayınız:

https://www.kvkk.gov.tr/Icerik/5520/Orneklerle-Kisisel-Verilerin-Korunmasi

EK-4: Veri Koruma Komitesi Hakkında

Şirket yönetimi, en az 3 (üç) kişiden müteşekkil bir Veri Koruma Komitesi kurar.

Veri Koruma Komitesi, işbu Politika'da kendisine verilen görevleri yerine getirmekle yükümlüdür.

Veri Koruma Komitesi üyeleri azami ölçüde farklı Şirket içi birimlerden belirlenecek kişilerden oluşur.

Şirket, Veri Koruma Komitesi'nin oluşumu ile görev ve yetkileri konusunda Şirket'in çalışanlarına ve birimlerine bilgilendirme yapar.

Şirket gerekli görmesi halinde Veri Koruma Komitesi üyelerini değiştirebilir, komitenin üye sayısını artırabilir veya azaltabilir.

Veri Koruma Komitesi Üyeleri Aydınlatması - Veri Sorumlusu İnci GS Yuasa Akü Sanayi ve Ticaret A.Ş.'dir ("**Şirket**"). Veri işleme amacı, Şirket'in Kişisel Veriler'i Saklama ve İmha Politikası ("**Politika**") uyarınca tesis ettiği Veri Koruma Komitesi'nin oluşturulmasıdır. Kişisel Verileriniz, Şirket ile hukuki (istihdam) ilişkinizin başlaması sürecinde fiziki ve dijital olarak toplanmıştır. Veri işlemenin hukuki sebebi, kanunlarda açıkça öngörülmesi ve Şirket'in hukuki yükümlülüklerini yerine getirmesidir. Verileriniz gerekmesi halinde kamu kurum ve kuruluşlarına aktarılmakta; ayrıca Veri Koruma Komitesi'nin kimlerden oluştuğunun bildirilmesi amacıyla Şirket'in diğer çalışanlarına aktarılmaktadır. Kişisel Verileriniz, Şirket'in Veri İşleyenleri'nin denetlenmesi sürecinde hizmet sağlayıcılara ve tedarikçilere Komite'nin amacı ve yetkileri bağlamında aktarılabilir. 6698 sayılı KVK Kanunu'nun 11. maddesinde belirtilen haklarınızı kullanabilirsiniz.

EK-5: Teknik ve İdari Tedbirler

İdari Tedbirler

- Şirket tarafından yürütülen faaliyetlere ilişkin çalışanlara veri güvenliği ve gizlilik sözleşmeleri imzalatılmaktadır.
- Kişisel Veri işlemeye başlamadan önce Şirket tarafından, Veri Sahipleri'ni aydınlatma yükümlülüğü yerine getirilmektedir.
- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, Kişisel Veriler'in hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması hakkında eğitimler verilmektedir.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak yaptırımlar sözleşmelerde belirlenmiştir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Şirket içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

Teknik Tedbirler

- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için donanımsal ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Sızma testleri ile Şirket bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Şirket'in bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu Veri Sahibi'ne ve Kurula bildirmek için Şirket tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.

- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Şirket internet sayfasına erişimde güvenli protokol (HTTPS) kullanılmaktadır.
- Özel Nitelikli Kişisel Veriler'in güvenliğine yönelik ayrı politika belirlenmiştir.
- Özel Nitelikli Kişisel Veri işleme süreçlerinde yer alan çalışanlara yönelik Özel Nitelikli Kişisel Veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel Nitelikli Kişisel Veriler'in işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması sağlanmaktadır.
- Özel Nitelikli Kişisel Veriler'in işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Özel Nitelikli Kişisel Veriler'in e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmaktadır.