KİŞİSEL VERİLERİ
SAKLAMA VE İMHA POLİTİKASI

Şubat 2020

İÇİNDEKİLER

1. AMAÇ

1.1. Bu Saklama ve İmha politikası (**"Politika"**), Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in (**"Yönetmelik"**) 5. Maddesi gereği Şirket'in Kişisel Veri İşleme Envanteri ("**Envanter**") ile birlikte uygulanmak üzere hazırlanmıştır.

1.2. Bu Politika, **Uzman Ticaret ve İnşaat A.Ş.'**nin ("**Şirket**") tabi olduğu Kanun ve ikincil mevzuata uyumu sağlayabilmek adına ŞİRKET içinde kişisel verilerin saklanması ve imhasına ilişkin genel prosedürlerini ortaya koymaktadır.

1.3. Bu Politika ile ŞİRKET'in kişisel veri içeren belge ve ortamlarının güvenli şekilde saklanmasını, işleme amacı ve şartlarının ortadan kalktığı kişisel verilerin imhasının sağlanması amaçlanmaktadır.

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

2. TANIMLAR VE KISALTMALAR

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	ŞİRKET'in faaliyetleri kapsamında aktif olarak kullanılmakta olan verileri ifade eder.
Aktif Olmayan Kayıtlar	Aktif Kayıtlar kapsamına girmeyen doğrudan ŞİRKET 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.
BT Departmanı	ŞİRKET'in Bilgi Teknolojileri Departmanını ifade eder.

Envanter /Kişisel Veri İşleme Envanteri	ŞİRKET'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	Kişisel Verileri Koruma Kurulu tarafından çıkarılan Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik, Anonimleştirme Yönetmeliği, Sicil Yönetmeliğini, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliği ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği, ileride çıkarılabilecek 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; ŞİRKET organizasyonu içerisinde veya ŞİRKET'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.
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.
ŞİRKET	**Uzman Ticaret ve İnşaat A.Ş.**'yi 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	Bu Saklama ve İmha Politikası'nı ifade eder.

Rehber	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.
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 ŞİRKET'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.

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 ŞİRKET genelinde uygulanmakta, Kişisel Veriler'e ilişkin kurumsal bir çerçeve teşkil etmektedir.

5. VERİ KORUMA KOMİTESİ

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

5.2. Veri Koruma Komitesi, ŞİRKET içerisinde Kişisel Veri işleme, saklama ve anonimleştirme dahil her türlü kişisel veri aktivitesini izler, ilgili tavsiyeleri verir ve organizasyonları yapar. Veri Koruma Komitesi'nde yer alan kişilerin unvan ve birimlerine EK-2'de yer verilmiştir.

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

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

5.5. Tüm ŞİRKET departmanları, çalışanları ve tedarikçileri Veri Koruma Komitesi ile uyumlu bir şekilde faaliyet göstermek zorundadır. Veri Koruma Komitesi ile birlikte her departman yöneticisi bu Politika'nın uygulanmasından sorumludur. Veri Koruma Komitesi'nin kurulması veya faaliyet göstermesi departman yöneticilerinin sorumluluğunu ortadan kaldırmaz.

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

6. SAKLAMA

6.1. Kişisel Veriler'in Saklanmasını Gerektiren Sebepler

ŞİRKET tarafından Kişisel Veriler, Envanter'de beher veri işleme sürecine ilişkin özel olarak belirtilen sebepler doğrultusunda işlenmektedir. Bu sebepler Kanun'un 5. maddesi 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) İlgili kişinin kendisi tarafından alenileştirilmiş olması,
f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve
g) İlgili kişinin 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, mikrofiş ve benzeri ortamlarda bulunan kayıtlardan oluşur.

Aktif Kayıtlar ve günlük faaliyetler gereği kolayca erişilmesi gereken Kayıtlar, ŞİRKET'in aktif çalışma alanlarında saklanmaktadır.

Aktif Olmayan Kayıtlar, ŞİRKET'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 dahil 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 elektronik ortamlarda 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

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.

i. Veri Sahibi'nin Kişisel Veri'nin imhasını talep ettiğinde,
ii. Açık rızaya dayanan Kişisel Veri işleme ve saklama süreçlerinde Veri Sahibi'nin açık rızasını geri alması halinde,
iii. Kurul'un usulüne uygun olarak Kişisel Veri'nin imhasını talep etmesi halinde,
iv. Kişisel Veriler'in işleme şartlarının tamamının veya Kişisel Veriler'in işlenmesine ilişkin amaçların ve kanuni/sözleşmesel gerekliliklerin ortadan kalkması halinde ve
v. Belirlenmiş olan Kişisel Veri saklama süresinin sona ermesi halinde.

7.2. Veri Sahibi'nin İmha Talebi

Veri Sahibi'nin Kişisel Veriler'inin İmhası'nı talep ettiğinde; ŞİRKET 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, 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 30 (otuz) gün içerisinde talepte bulunan Veri Sahibi'ne yazılı olarak bilgi verilir.

7.3. Veri Sahibi'nin Açık Rızasını Geri Alması

Veri Sahibi'nin Kişisel Verileri'nin imhasından farklı olarak açık rızasını geri aldığını iletmesi halinde; ŞİRKET tarafından öncelikle ilgili Kişisel Veriler'in sadece açık rızaya dayanılarak işlenip işlenmediği değerlendirilir. Bu noktada Envanter'de ilgili işleme sürecinin amacı tespit edilir ayrıca herhangi bir ek veya değişik amaç olup olmadığı teyit edilir. İşleme faaliyetinin açık rızaya dayanmadığı veya açık rıza yanında başkaca amaçların olduğu sonucuna varılırsa, Veri Sahibi'nin talebi, gerekçesi belirtilerek yazılı olarak reddedilebilir. Yazılı karar, 30 (otuz) gün içerisinde talepte bulunan Veri Sahibi'ne gönderilir. Veri işleme faaliyetinin sadece açık rızaya dayandığı sonucuna varılırsa aşağıda yer alan İmha işlemleri uygulanır ve yine 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 ŞİRKET içerisinde 6 (altı) ayda bir periyodik olarak gözden geçirme işlemi uygulanır.

Gözden geçirme işlemi, Veri Koruma Komitesi gözetiminde her bir ŞİRKET departmanı tarafından kendi iç süreçlerine ilişkin olarak yürütülür ve sonuçlar Veri Koruma Komitesi'ne raporlanır. Raporlarda özellikle departman içinde hangi türde Aktif Kayıtlar'ın bulunduğu, hangi Kayıtlar'ın arşivleneceği ve hangi Kayıtlar'ın imha 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 imha [takvim yılının sonunda], ikinci ise her yıl [Haziran ayının 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 imha 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)* imha 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 *(örneğin; parmak izli kapı geçiş sistemi)* 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 departman tarafından, hangi tarihte ŞİRKET arşiv yetkililerine teslim edildiği üç nüsha halinde tutanak altına alınır.
- Tutanakların bir nüshası Kayıtlar'ı teslim eden departmana, 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 ŞİRKET departmanı ve çalışanın erişemeyeceği şekilde arşivlenir.
- İlgili arşiv alanına ancak temizlik, bakım-onarım ve gözetim amacıyla erişilebilir bunun dışında Veri Koruma Komitesi'nin yazılı kararı olmadıkça ŞİRKET 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.

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. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI, HUKUKA AYKIRI OLARAK İŞLENMESİ, ERİŞİLMESİNİN ÖNLENMESİ VE HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ ÖNLEMLER

8.1. ŞİRKET, 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. ŞİRKET çalışanları, departmanları, tedarikçileri 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.

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

8.4. 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.

8.5. 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.

8.6. Veri Koruma Komitesi'nin kararı ile ŞİRKET 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.

8.7. 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.

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

8.9. 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.

8.10. 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.

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

9. POLİTİKA'NIN İHLALİ

9.1. ŞİRKET 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. ŞİRKET 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 Yönetim Kurulu, ihlali gerçekleştiren ŞİRKET çalışanı veya başkaca kişilere ilişkin inceleme yapma yetkisine sahiptir. Yönetim Kurulu 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 ŞİRKET yönetiminin onayına tabi olabilir.

10. ÇEŞİTLİ HÜKÜMLER

10.1. Politika'nın Yayınlanması ve Yürürlüğe Girmesi

Şirket Yönetim Kurulu tarafından ŞİRKET çalışanların erişimine yazılı olarak sunulacaktır.

10.2. Politika'nın Yürütülmesi

Bu Politika'nın uygulanması ve yürütülmesi ile Politika'ya uyumun sağlanmasından Yönetim Kurulu sorumludur.

10.3. Değişiklikler

Bu Politika'da her zaman değişiklikler yapılabilir. Önemli değişikliklerin bildirimi tüm kişi gruplarına Yönetim Kurulu tarafından seçilen uygun bir mekanizma aracılığıyla iletilecektir.

EKLER

1- **Azami Saklama ve İmha Süreleri Tablosu**
2- **Saklama ve İmha Görevlerinde Yer Alacak Kişilerin Unvan ve Birimleri**

EK-1: AZAMİ SAKLAMA VE İMHA SÜRELERİ TABLOSU

- Bu Saklama ve İmha Süreleri Tablosu, ŞİRKET Kişisel Verilerin Saklanması ve İmhası Politikası'nın eki olarak düzenlenmiştir.
- ŞİRKET içerisinde her bir veri işleme faaliyetine ilişkin özel saklama sürelerine Envanter'de yer verilmiştir. ŞİRKET 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.

KİŞİ GRUBU	AZAMİ SAKLAMA VE İMHA SÜRELERİ
Hissedar/Hissedar Yetkilisi	Şirket tüzel kişiliğine ilişkin belgelerde yer alan bilgiler, şirketin devamlılığı sebebiyle tüzel kişilik sona erene kadar saklanmaktadır.
İştirak Çalışanı	Düzenlenen vekaletnamelerin geçerlilik süresince saklanmaktadır.
Tedarikçi yetkilisi ve çalışanları	Azami olarak tedarikçi sözleşmelerinin sona ermesinden itibaren 10 yıllık zamanaşımı süresi boyunca saklanmaktadır.

EK-2: Saklama ve İmha Görevlerinde Yer Alacak Kişilerin Unvan ve Birimleri