POLİTİKA

KİŞİSEL VERİ SAKLAMA, İŞLEME VE İMHA POLİTİKASI

PT.HM.02

04.12.2020

Revizyon No : 00

Hazırlayan : Kurumsal Teknik, Satış, Hukuk ve Reasürans Genel Müdür Yardımcısı

Yürürlük Onayı : Yönetim Kurulu

YAPILAN SON DÜZENLEME		
Rev.No	**Revizyon Tarihi**	**Değişiklik Açıklaması**
00	04.12.2020	• Data Governance Projesi ile oluşturulan Veri Yönetişim Komitesi'nin tanımı eklendi. • Yönetim tarafından belirlenen 15 yıl muhafaza süremiz Verbis girişleri sonrasında uyumlu olabilmek adına madde 6.9 'da revize edildi. • Kişisel verilerin korunması ile ilgili yönetişim yapısı, veri yönetişim organizasyonunun rol ve sorumluluklarına madde 6.10 'da yer verildi.

Genel

		• IT ile mutabık kalınarak madde 6.3'da yer alan ortamlar sadeleştirilerek daha genel versiyona dönüştürüldü.

1.0 AMAÇ

Bu politika, Aksigorta Anonim Şirketi ("**Aksigorta**") tarafından ve/veya adına gerçekleştirilmekte olan kişisel veri, işleme saklama ve imha faaliyetlerine ilişkin iş ve işlemler sırasında, tüm Kişisel Verilerin (aşağıdaki tanımlara bakınız) gizli tutulmasını ve Türkiye'de yürürlükte bulunan 6698 sayılı Kişisel Verilerin Korunması Kanunu (Bundan böyle **"KVKK"** olarak anılacaktır.) ve hukuki dayanağını ondan alan ikincil mevzuat ile Kişisel Verileri Koruma Kurulu'nun almış olduğu kararlara (Hepsi birlikte bu doküman içerisinde **"Veri Koruma Mevzuatı"** olarak anılacaktır.) uyulmasını sağlamak amacıyla tasarlanmış ve çıkartılmış bulunmaktadır.

2.0 KAPSAM

Bu Politika, kişisel verileri Aksigorta tarafından ve/veya Aksigorta adına tamamen veya kısmen otomatik olan veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmekte olan tüm gerçek kişilere yönelik olarak gerçekleşecek kişisel veri işleme faaliyetlerini düzenlemek maksadıyla düzenlenmiştir ve Aksigorta adına kişisel veri işleme faaliyetinde bulunan herkes bakımından uygulanmaktadır.

3.0 REFERANS VE EKLER

YK.HM.07. Aksigorta Kişisel Verilerin Korunması ve İşlenmesi Yönetmeliği

PR.HM.10 Güvenlik Olaylarına Müdahale Prosedürü

PR.HM.11 Başvuru Yanıtlama Prosedürü

Ek-1 Kişisel Verilerin Korunması Aydınlatma Metni

Ek-2 Tedarikçilere Veri Gizliliği Bildirimi

Ek-3 Aksigorta Çalışanlarının Kişisel Verilerinin İşlenmesine İlişkin Aydınlatma Metni ve Aksigorta A.Ş. Çalışanı Kişisel Verilerin Korunması ve İşlenmesi Açık Rıza Metni

Ek-4 Kişisel Veri Gizliliği Taahhütnamesi

6098 Sayılı Türk Borçlar Kanunu

5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

6361 Sayılı İş Sağlığı ve Güvenliği Kanunu

6305 Sayılı Afet Sigortaları Kanunu

6102 Sayılı Ticaret Kanunu

4857 Sayılı İş Kanunu

2918 Sayılı Karayolları Trafik Kanunu

6502 Sayılı Tüketicinin Korunması Hakkında Kanun

İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik

4.0 TANIMLAR

Acente: Aksigorta ile bir sözleşmeye dayanarak muayyen bir yer veya bölge içinde daimî bir surette Aksigorta'nın nam ve hesabına sigorta sözleşmelerine aracılık etmeyi ve bunları Aksigorta adına yapmayı meslek edinen, sözleşmenin akdinden önce hazırlık çalışmalarını yürüten ve sözleşmenin uygulanması ile tazminatın ödenmesinde yardımcı olan gerçek kişi.

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza

Broker: Sigorta veya reasürans sözleşmesi yaptırmak isteyenleri temsil ederek, bu sözleşmelerin yaptırılacağı şirketlerin seçiminde tamamen tarafsız ve bağımsız davranarak ve teminat almak isteyen kişilerin hak ve menfaatlerini gözeterek sözleşmelerin akdinden önceki hazırlık çalışmalarını yürütmeyi ve gerektiğinde sözleşmelerin uygulanmasında veya tazminatın tahsilinde yardımcı olmayı meslek edinen gerçek kişi.

Veri Yönetişimi: Veriyi, kurum içinde uçtan uca yönetmeyi sağlayan bir yöntemler bütünüdür. Veri Yönetişimi, politikalar, süreçler, standartlar, teknolojiler ve kişileri işin içine dahil ederek doğru, tutarlı ve zamanında karar verilmesini hedefler.

Veri Yönetişim Komitesi: Aksigorta'nın büyüyen veri ekosisteminin etkin yönetilmesi için Veri Yönetişim Komitesi kurulmuştur. Komite Bilgi Teknolojileri ekiplerinden ve Uyum departmanından ana üyelerden oluşur. İş birimlerinden iş süreçleri kapsamında veri yöneten ekiplerden farklı üyeleri de dahil eder. Komite, Aksigorta veri değerini en üst düzeye çıkaran, maliyetleri düşüren, güvenliği ve kaliteyi artıran, riski azaltan veri odaklı bir kültür oluşturmayı hedefler. Veri yaşam döngü sürecini kurgular, verinin kalitesini desteklemek ve geliştirmek için uygun stratejileri tanımlar; analitiği desteklemek için verilerin eksiksiz olmasını ve geçerliliğini hedefler. Aksigorta verisinin ilgili yasal düzenlemelere ve politikalarına uygun olarak güvenliğini gözetler.

Çalışan: Bir iş Sözleşmesine dayanarak Aksigorta'da istihdam edilen kişiler.

Çalışan adayı: Aksigorta'ya iş başvurusunda bulunarak veya herhangi bir yolla özgeçmişini ve ilgili bilgilerini Aksigorta'ya erişilebilir kılan gerçek kişiler.

Kişisel Veri: İsim, adres, telefon numarası, e-posta adresi veya benzeri kimlik bilgileri gibi Veri Süjesiyle ilgili her türlü bilgi anlamına gelir.

Kişisel verilerin işlenmesi: 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.

Müşteriler/ Müşteri Adayları: Herhangi bir sözleşmesel ilişki olup olmadığına bakılmaksızın Aksigorta tarafından yürütülen faaliyetler kapsamında iş ilişkileri dolayısıyla kişisel verileri elde edilen gerçek kişiler.

Özel Nitelikli Kişisel Veriler: Bir kişinin 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.

Üçüncü Kişiler: Politika'da tanımlanmamış olmasına rağmen işbu Politika çerçevesinde kişisel verileri işlenen tedarikçi, mağdur, aile bireyleri vb. dâhil fakat bunlarla sınırlı olmamak üzere diğer gerçek kişiler**.**

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişi.

Veri Süjesi ya da İlgili Kişi: Verinin ait olduğu, kimliği belirlenmiş veya belirlenebilir bir gerçek kişi.

Ziyaretçiler: Aksigorta'nın fiziksel tesislerine çeşitli amaçlarla girmiş olan veya internet sitelerini ziyaret eden gerçek kişiler.

Genel

5.0 SORUMLULAR

Aksigorta dahilindeki tüm iş birimleri, çalışanlar, Aksigorta adına veri işleme faaliyetinde bulunan kişiler işbu Politika ve Aksigorta Kişisel Verilerin Korunması ve İşlenmesi Yönetmeliği kapsamında belirtilmiş olan teknik ve idari tedbirlerin gereği gibi uygulanması, veri işleme faaliyeti yürüten kişilerin, çalışanların, acentelerin, iş ortaklarının eğitimi ve farkındalığının artması, takibi gibi sürekli denetimi ile kişisel verilerin hukuka uygun şekilde işlenmesini teminen tüm veri işleme ortamlarında veri güvenliğini sağlamaya dönük olarak teknik ve idari tedbirlerin uygulanmasına destek verir ve sorumlu birimlerle işbirliği içinde çalışır.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların görev yapmakta olduğu hususlar şu şekilde oluşmuştur;

a) Bu Politikayı ve bu Politikada yapılan tüm revizyon ve değişiklikleri incelemek ve onaylamak Veri Yönetişim Komitesi'nin sorumluluğundadır. Veri Yönetişim Komitesi aynı zamanda Politikayı geliştirmek ve gerekli eğitimleri vermek ile Politikanın yorumlanması konusunda Aksigorta adına veri işleyenlere kılavuzluk etmekle görevlidir. Veri Yönetişim Komitesi ayrıca bu Politikaya uyulup uyulmadığını denetler ve uyulması için gerekli desteği verir.

b) Veri Yönetişim Komitesi işbu Politika'nın 6.9 maddesinde yer alan periyodik imha süreçlerinin kontrolünden, belirtilen verilerin ilgili muhafaza süreleri boyunca muhafaza edilmesinden, bu sürelerin takibinden ve muhafaza süresi dolan verilerin imha edilmesinden sorumludur.

c) Veri Yönetişim Komitesi'nin takibinden sorumlu olduğu Aksigorta periyodik imha süreci 6 ay olarak belirlenmiştir. Kurumsal Hukuk ve Uyum Bölümü'nün görevi, Politikayı ve Politikada yapılan tüm değişiklikleri incelemek, onaylamak ve Veri Koruma Mevzuatıyla uyumlu hukuki tavsiyelerde bulunmaktır.

d) Genel Müdür ve Kurumsal Hukuk ve Uyum Bölümü'nün desteğiyle yürüteceği görev, Politikadan sapma ve istisna taleplerini incelemek ve onaylamaktır.

6.0 AKSİGORTA KİŞİSEL VERİ SAKLAMA VE İŞLEME FAALİYETLERİ

İlgili kişilere ait kişisel veriler, iş faaliyetleri sırasında, detayları Aksigorta Kişisel Verilerin Korunması ve İşlenmesi Yönetmeliği'nde belirtilmiş olan Kişisel Verileri işbu Politika'da ve Aksigorta Kişisel Verilerin Korunması ve İşlenmesi Yönetmeliği'nde öngörülmüş usullerle toplamakta, işlemekte ve saklamakta ve imha etmektedir.

Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

6.1 Saklamaya İlişkin Açıklamalar

KVKK'nın 3.(üçüncü) maddesinde "kişisel verilerin işlenmesi" kavramı tanımlanmış 4.(dördüncü) maddesinde işlenen kişisel verinin "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi" gerektiği belirtilmiş, 5(beş) ve 6.(altıncı) maddelerde ise "kişisel verilerin işleme şartları" sayılmıştır.

Buna göre, kişisel veriler, Aksigorta iş faaliyetleri çerçevesinde ilgili mevzuatta öngörülen veya işleme amaçlarına uygun ve işbu Politika'nın 6.9 maddesinde belirtilmiş olan sürelerde saklanır.

6.1.1 Saklamayı Gerektiren Hukuki Sebepler

Aksigorta, iş faaliyetleri çerçevesinde işlenen kişisel verileri ilgili mevzuatta öngörülen sürelere uygun olarak muhafaza eder. Bu kapsamda kişisel veriler;

- 6098 Sayılı Türk Borçlar Kanunu
- 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu

- 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 6361 Sayılı İş Sağlığı ve Güvenliği Kanunu
- 6305 Sayılı Afet Sigortaları Kanunu
- 6102 Sayılı Ticaret Kanunu
- 4857 Sayılı İş Kanunu
- 2918 Sayılı Karayolları Trafik Kanunu
- 6502 Sayılı Tüketicinin Korunması Hakkında Kanun
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik

Bu kanunlar uyarınca, yürürlükte olan ikincil düzenlemeler ve bunlarla sınırlı olmamak üzere Aksigorta'nın uyması gereken mevzuat ve idari düzenlemeler uyarınca öngörülen saklama süreleri boyunca kişisel veriler saklanmakta ve işlenmektedir.

6.1.2 Saklamayı Gerektiren İşleme Amaçları

Kişisel veriler Aksigorta Kişisel Verilerin Korunması ve İşlenmesi Yönetmeliği'nde detaylandırılmış bulunan ve aşağıda sıralanmış amaçlarla saklanmaktadır:

- Kurum güvenliğini sağlamak,
- İstatiksel çalışmalar yapabilmek,
- Reklam ve kampanya süreçlerinin yürütülmesi,
- Satış ve pazarlama süreçlerinin yürütülmesi,
- İnsan kaynakları süreçlerini yürütmek,
- İmzalanan sigorta sözleşmeleri kapsamında iş ve işlemlerin ifası kapsamında destek hizmet sağlayıcılarına ilişkin süreçlerin yürütülmesi, sigorta tazminatlarının hesaplanması, sigortalı ve lehtara ödemelerin ve rücu takiplerinin yapılması,
- Prim ödemelerinin tahsilatına ilişkin işlemlerin yapılması,
- Tedarikçilerle ilgili süreçlerin yürütülmesi,
- Acentelik başvurusu ve acentelik sözleşmeleri kapsamında ilgili süreçlerin yürütülmesi,
- Poliçe teklifi oluşturulması, poliçelerin düzenlenmesi, poliçe yenileme tekliflerinin sunulması ve poliçe iptal işlemlerinin gerçekleştirilmesi,
- Aksigorta ile iş ilişkisi bulunan gerçek/tüzel kişilerle irtibat sağlamak,
- Finans ve muhasebe işlerinin yürütülmesi,
- Yasal raporlamalar yapmak,
- Çağrı merkezleri ile ilgili süreçleri yönetmek,
- Risk değerlendirme süreçlerinin yönetilmesi,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü,
- Sigorta sözleşmesinin kurulması ve hasar durumunda gerekli hizmetlerin verilmesi için iş ortaklığı yapılmakta olunan gerçek kişi brokerlar, acenteler ve aktüerlerle Aksigorta arasındaki sözleşmelerin kurulması ve hizmetlerin karşılıklı olarak ifa edilmesi,

- Asistans hizmetlerinin verilmesi,
- İletişim faaliyetlerinin yürütülmesi,
- Sigorta tazminatlarının hesaplanması, sigortalı veya lehtara ödenmesi ve rücu takibinin gerçekleştirilebilmesi,
- Muallak hasar dosyalarının takibi,
- Hasar dosyasının hazırlanması ve hasar sonucu ödeme mutabakatı yapılması,
- Eksper ve ekspertiz raporlarının oluşturulup, eksper performans takibinin yapılması,
- Reasürans ve koasürans süreçlerinin yürütülmesi,
- Sigorta şirketleri ve üçüncü kişilere rücu taleplerinin yapılması ve bu taleplerin takibi,
- Sigorta şirketleri ve üçüncü kişiler tarafından iletilen rücu taleplerinin değerlendirilmesi ve cevaplandırılması,
- Ziyaretçi kayıtlarının oluşturulması ve takibi,
- Müşteri talep ve şikâyetlerinin değerlendirilmesi,
- Müşteri memnuniyet anket ve görüşmelerinin yapılması,
- Pazarlama, reklam ve kampanya süreçlerinin yürütülmesi,
- Hukuki iş ve işlemlerin yürütülmesi ve takibi,
- Yetkili kurum ve kuruluşlara ilgili mevzuattan doğan yükümlülüklere istinaden bilgi verilmesi,
- Faaliyetlerin Aksigorta prosedürleri ve ilgili mevzuata uygun olarak yürütülmesinin sağlanması için gerekli iç denetim faaliyetlerinin planlanması ve yürütülmesi,
- Şirketler hukukundan doğan süreçlerin gerçekleştirilmesi,
- Sigortacılık Mevzuatı uyarınca risk değerlendirme süreçlerinin yönetilmesi

6.2 İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11'inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Aksigorta tarafından kabul edilmesi,
- Aksigorta'nın, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya KVKK'da öngörülen süre içinde cevap vermemesi hallerinde; Kişisel Verileri Koruma Kurulu'na şikâyette bulunması ve bu talebin Kişisel Verileri Koruma Kurulu tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

durumlarında, Aksigorta tarafından ilgili kişinin talebi üzerine ya da re'sen silinir, yok edilir veya anonim hale getirilir.

6.3 KAYIT ORTAMLARI

Kişisel veriler Aksigorta tarafından Tablo 1'de listelenen ortamlarda hukuka uygun olarak ve güvenli bir şekilde saklanır.

Tablo 1: Kişisel veri saklama ortamları

Elektronik ortamlar	Elektronik olmayan ortamlar
a) Sigortacılık uygulamaları yazılımı (a)OLTP system (b)DWH (c)CRM (d)Veri Bilimi uygulamaları (e)Big Data b) Veri depolama alanları 1. Veritabanı 2. Doküman yönetim sistemi 3. Mail ortamı 4. File Server- Ortak folder	(1) Veri depolama alanları Manuel veri kayıt ortamları (a)Formlar, (b)Belgeler

6.4 KİŞİSEL VERİ İŞLEME KOŞULLARI

Kişisel verilerin bu Politikaya ve Aksigorta Kişisel Verilerin Korunması ve İşlenmesi Yönetmeliği'ne uygun olarak işlenebilmesi ve kullanılabilmesi için, Veri Süjesine işleme faaliyetlerine dair **aydınlatma yapılması**, Kişisel Verilerin işlenmesi konusunda izin istenmesi ve Veri Süjesinin **açık rızasının alınması** gerekir.

Bu amaçla, Kurumsal Hukuk ve Uyum Bölümü tarafından onaylanan onam formlarını ve aydınlatma metinleri kullanılmalıdır.

Ancak aşağıda sayılan **istisnalardan birinin söz konusu olması halinde** Veri Süjesinden açık rıza alma şartı **uygulanmamalıdır:**

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

d) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

e) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

g) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

6.4.1 Veri Sorumlusu Olarak Aksigorta'nın Aydınlatma Yükümlülüğü

Veri Sorumlusu olarak işbu Politika'nın 6.4 maddesinde anıldığı şekilde Kişisel Verilerin işlenmesi için her zaman Veri Süjesinden açık rıza alınması şartı bulunmasa dahi, Aksigorta'nın her zaman Veri Süjelerine aşağıdaki konularda bilgi verme yükümlülüğü bulunmaktadır:

- Veri Sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- İşbu Politika'nın 6.6 maddesinde sayılmış Veri Süjesinin diğer hakları.

Aydınlatma yükümlülüğü Ek-1 Kişisel Verilerin Korunması Aydınlatma Metni'ni kullanmak suretiyle yapılabilir.

Aksigorta zaman zaman iş süreçlerinin yürütülmesi, iletişim sağlanması amaçlarıyla tedarikçilerinin yetkililerinin kişisel verilerine ihtiyaç duyabilir. Bu durumda sözü edilen tedarikçi çalışanlarına karşı Aksigorta'nın aydınlatma yükümlülüğünün yerine getirilmesini teminen ilgili Aksigorta yetkililerinin Ek-2 Tedarikçilere Veri Gizliliği Bildirimi gönderilmesi mümkündür.

6.4.2 Özel Nitelikli Kişisel Verilerin işlenmesinde Uyulacak Kurallar:

İş kanunları ve mevzuatından doğan belirli hakların kullanılması veya belirli yükümlülüklerin yerine getirilmesi amaçlarıyla gerekli olmadıkça ve Veri Koruma Mevzuatı başta olmak üzere yürürlükteki sair mevzuat gereğince izin ve yetki verilen durumlar haricinde, Özel Nitelikli Kişisel Veriler işlenmeden önce bu verileri işlemek için ilgili kişinin açık izin ve rızasını mutlaka ve daima almak gerekir.

6.4.3 Çalışanların 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 Aksigorta tarafından belirlenen başka amaçlarla işlenebilmesi için, halihazırda Aksigorta çalışanı bulunan kişilere Ek-3 Aksigorta Çalışanlarının Kişisel Verilerinin İşlenmesine İlişkin Aydınlatma Metni ve Aksigorta A.Ş. Çalışanı Kişisel Verilerin Korunması ve İşlenmesi Açık Rıza Metni'nin imzalatılması suretiyle aydınlatma ve açık rıza temini yükümlüğünün yerine getirilmesi gerekmektedir.

6.4.4 Müşterilere Ait Kişisel Verilerin Pazarlama Amaçlarıyla İşlenmesi ve Kullanılmasında Uyulacak Esaslar

Müşterilerin kişisel verilerini doğrudan veya dolaylı olarak pazarlama yapmak maksadıyla toplanması ve işlenmesi için, kişisel verilerin toplanmasından önce Veri Süjesi müşterinin açık rızasının alınmış olması gerekir. Bunun haricinde Veri Süjelerine ticari iletişim kurulması rızasından vazgeçme imkanlarının hem alınacak rıza sırasında hem de her iletişimde sağlanması gerekir.

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

Görevlerinin bir gereği olarak ve görevleri esnasında, Aksigorta adına Kişisel Verileri işleyen kişilerin, Politika'da yer alan hususların yanı sıra aşağıda sayılan hususları gözetmeleri beklenmektedir:

- Kişisel Verilerin Veri Koruma Mevzuatı'na uygun bir şekilde, meşru yollarla ve adil bir biçimde işlenmesi gerekir.
- Kişisel Verilerin sadece izin verilen ve açıklanan yasal amaçlar için işlenmesi gerekir.
- Veri Süjesine açıklamayan 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.

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

Görevlerinin bir gereği olarak ve görevleri esnasında Aksigorta adında Özel Nitelikli Kişisel Veri işlemekte olan çalışanların işbu Politika'nın diğer maddeleri ve 6.4 maddede sözü edilen hususları gözetmelerinin yanı sıra Veri Koruma Mevzuatı uyarınca Ek-4 Veri Gizliliği Taahhütnamesi'ni imzalamaları gerekmektedir.

6.4.7 Kişisel Verilerin Transferi ve Devri Gerçekleştirirken Uyulması Gereken Kurallar

Kişisel veriler ancak 6.4 maddede sayılan istisnalardan birinin mevcut olması halinde ilgili kişinin açık rızası olmaksızın yurtiçindeki üçüncü kişilere aktarılabilir. Kişisel Verilerin yurt dışına aktarılabilmesi için ise Veri Koruma Mevzuatı uyarınca öngörülen şartlar yerine getirilmeli ve gerekli hallerde ilgili kişinin açık izin ve rızası alınmalıdır. Bu kapsamda:

a) Kişisel Veriler, Veri Koruma Mevzuatı'nın uyarınca belirlenen koşullar haricinde herhangi bir üçüncü kişiye transfer edilmeyecektir.

b) Kişisel Veriler, İlgili Kişi'nin açık rızası bulunmadıkça, Kişisel Verileri Koruma Kurulu tarafından belirlenecek ve ilan edilecek olan 'Yeterli Korumanın Bulunduğu Ülkeler' dışında bir ülkeye transfer edilmeyecektir.

c) Kişisel Veriler, bahsi geçen 'Yeterli Korumanın Bulunduğu Ülkeler' dışındaki bir ülkeye, ancak ve sadece ilgili Veri Süjesi tarafından bu transfere açık izin ve rızası verildiği takdirde transfer edilebilecektir.

6.5 TEKNİK ve İDARİ TEDBİRLER

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'nu uyarınca ve Kişisel Verileri Koruma Kurulu tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde olmak üzere Aksigorta tarafından teknik ve idari tedbirler alınmaktadır.

6.5.1 Teknik Tedbirler

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

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakım kapsamındaki güvenlik önlemleri alınmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Erişim logları düzenli olarak tutulmaktadır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- 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.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulaması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Verilere uzaktan erişim gerekiyorsa iki kademeli kimlik doğrulama mekanizması uygulanmaktadır.
- Farklı fiziksel ortamlardaki sunucular arasındaki veri aktarımı gerçekleştirilirken, sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımı yapılmaktadır.
- Taşınabilir bellek, CD, DVD ortamından aktarılan özel nitelikli kişisel veriler şifrelenerek aktarılmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.
- Veri sınıflandırma yazılımları kullanılmaktadır.

6.5.2 İdari Tedbirler

Aksigorta 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 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 veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- 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 uygulanmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda farkındalığı sağlanmaktadır.

6.6 VERİ SÜJELERİNİN HAKLARI

Aksigorta tarafından kişisel verileri işlenmekte olan veri süjeleri Aksigorta'ya başvurarak kendisi ile ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

d) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

e) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

f) Veri Koruma Mevzuatı'nda öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

g) (e) ve (f) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

h) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

i) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.

Kişisel Verilerin doğrudan, pazarlama çabalarının bir parçası olarak toplandığı durumlarda, Veri Süjesi, kendisine ait Kişisel Verilerin üçüncü şahıslara verilmesine veya pazarlama amaçlarıyla kullanılmasına itiraz etme hakkına ya da Kişisel Verileri üçüncü şahıslara verilmeden veya pazarlama amaçlarıyla kullanılmadan önce durumun kendisine bildirilmesini talep etme hakkına sahiptir.

İlgili kişilerin bu başvurularının, değerlendirilmesinin ve yanıtlanmasının Aksigorta Başvuru Yanıtlama Politikası içinde anıldığı şekilde gerçekleşmesi gerekmektedir.

6.7 GÜVENLİK KOŞULLARI

Genel

Aksigorta Kişisel Verileri kazayla veya yasadışı bir şekilde imha olma, kaybolma, tahrif edilme, yetkisiz ifşa veya yetkisiz erişim risklerine (Güvenlik Olayı) karşı koruma amacıyla aşağıdaki de dahil tüm makul güvenlik önlemlerini alır;

- Kişisel Verilere erişimi, sadece görevlerinin ifası esnasında bu bilgilere erişmesi zorunlu olan kişilerle sınırlı tutmak.
- Uygunsa, şifre korumalı elektronik dosyaları kullanmak.
- Kişisel Verileri içeren dosyaları düzenli saklamak ve bu dosyalara fiziksel erişimi gerektiği gibi ve uygun şekilde kısıtlamak.
- Çalışanın kişisel Verilere yetkisiz erişim veya Kişisel Verilerin usulsüz kullanımı gibi olay ve durumlardan haberdar olduğunda bunları derhal âmirine ve bilgi güvenliğine bildirmek.
- Kişisel Verileri ilk belirtilen amacı dışında bir amaçla kullanmadan önce ilgili Veri Süjesinden Veri Koruma Mevzuatı uyarınca açık rıza almak ve işleme konusuyla ilgili aydınlatma yükümlülüğünü yerine getirmek.

Kişisel Verileri korumak için sağlanan güvenlik koşulları ve alınan teknik tedbirler periyodik olarak Veri Yönetişim Komitesi tarafından incelenmekte ve değerlendirilmektedir. Böylelikle kişisel verilerin korunması için ilave güvenlik tedbirlerine veya prosedürlerine ihtiyaç olup olmadığı tespit edilir.

Herhangi bir Güvenlik Olayı'nın oluşması halinde Aksigorta tarafından izlenmesi gereken adımlar "PR.BT.12 Olay Yönetimi Prosedürü" ekinde yer alan Siber Güvenlik Olayı Müdahale Planında belirtilmiştir.

6.8 KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Aksigorta tarafından re'sen (periyodik imha süreleri) veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

6.8.1 Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-1'de verilen yöntemlerle silinir.

Tablo 1: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	**Açıklama**
Sistemlerde Yer Alan Kişisel Veriler	Sistemlerde yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için ilgili kullanıcılar hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.

Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.8.2 Kişisel Verilerin Yok Edilmesi

Tablo 2: Kişisel Verilerin Yok edilmesi

Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

6.8.3 Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

Teknik tedbirler kapsamında alınan teknolojik araç ile sistematik şekilde ve belirli kural setleri dahilinde anonim hale getirme yapılmaktadır.

6.9 VERİ TÜRLERİNE GÖRE SAKLANMA ve İMHA SÜRELERİ

Aşağıdaki tabloda belirtilen verilerin ilgili muhafaza süreleri boyunca muhafaza edilmesinden, Veri Yönetişim Komitesi sorumludur.

Veri Yönetişim Komitesi'nin takibinden sorumlu olduğu Aksigorta periyodik imha süresi 6 ay olarak belirlenmiştir. Veri Yönetişim Komitesi bu sürelere uygun olarak imhaların gerçekleştirilmesinden ve muhafaza süresi dolan kişisel verilerin imhasına ilişkin gerekli hatırlatmaları yapmak bakımından görevli ve yetkilidir.

Tablo 3: Kişisel veri saklama ve imha süreleri

VERİ TÜRÜ	MUHAFAZA SÜRESİ	İMHA SÜRESİ
Müşteri Kayıtları	**Sözleşmesel ilişkinin sona ermesini takip eden 15 yıl boyunca**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Kayıtları	**İşten ayrılmalarını takip eden 15 yıl boyunca**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanlara Ait Özlük ve Adli Sicil Bilgileri	**İşten ayrılmalarını takip eden 10 yıl boyunca**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Adaylarına İlişkin Kayıtlar	**Başvuruyu takip eden 2 yıl boyunca**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş Ortaklarına ve Çalışanlarına İlişkin Kayıtlar	**İş ilişkisinin sona ermesini takip eden 15 yıl boyunca**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Muhasebe ve Finans Kayıtları	**15 yıl**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket İçi Belge ve Kayıtlar	**15 yıl**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ses ve Görüntü Kayıtları	**6 ay**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

6.10 KİŞİSEL VERİLEN KORUNMASI ve İLGİLİ ŞİRKET İÇİ YÖNETİM YAPISI

Şirket bünyesinde, Kanun'a uyum için gerekli aksiyonların takibi ve yönetilmesi KVK Aksigorta Veri Yönetişim Komitesinin ana hedefleri arasındadır. Bu Komitenin KVKK uyum kapsamındaki başlıca görevleri;

- Kişisel verilerin korunması ve işlenmesi ile politika ve prosedürleri hazırlamak ve yürürlüğe konulması için gerekli aksiyonları almak,
- Politika ve prosedürlerin uygulanması için gerekli görev dağılımını yapmak ve ilgili aksiyonların alındığının takibinin gerçekleştirmek,
- Kanun ve/veya politika ve prosedürün uygulanması ile ilgili ortaya çıkabilecek soru ve sorunların çözümü için gerekli aksiyonların alınmasını sağlamak,
- Gereken hallerde veri süjesi başvurularının çözümü için gerekli aksiyonları almak,
- Kişisel Verileri Koruma Kurumu ile olan ilişkileri yürütmektir.

Veri Yönetişimi Organizasyonu

Veri yönetişimi organizasyonu yapısı piramitte sunulmuştur.

Roller	Sorumluluklar
Executive SteerCo	• Genel Müdür, ALT, Kurumsal Hukuk ve Uyum Bölüm Müdürü, BT Yönetişim ve servis Yönetimi Müdürü, Dijital, Finansal ve Kurumsal Uygulamalar Bölüm Müdürü, Bilgi Güvenliği Birim Yöneticisi tarafından oluşur. • CEO tarafından başkanlık edilir. • Veri Yönetişim Stratejisini ve politikalarını onaylar. • Veri Yönetişimi alanında sponsorluk ve üst yönetim desteğini sağlar. • Veri Yönetişim komitesi tarafından çözülemeyen sorunları çözüme kavuşturur.
Veri Yönetişimi Komitesi (Data Governance Committe)	Ana üyeleri Kurumsal Hukuk ve Uyum Bölüm Müdürü, BT Yönetişim ve servis Yönetimi Müdürü, Dijital, Finansal ve Kurumsal Uygulamalar Bölüm Müdürü, Bilgi Güvenliği Birim Yöneticisidir. • Alt üyeler; Teknik Yönetişim Bölüm Müdürü, Strateji, Dönüşüm ve Dijital Kanallar Bölüm Müdürü, Pazarlama Grup Müdürü, Muhasebe Bölüm Müdürü, Performans, Ücret ve Organizasyonel Gelişim Bölüm Müdürü, Kurumsal Hukuk ve Uyum Bölümü, Veri Analitiği ve Performans Yönetimi Bölüm Müdürü, Banka Kanal Yönetimi Grup Müdürü'nden Oluşmaktadır. • Veri yönetişimi ve politikalarla ilgili kararları belirleyen çapraz fonksiyonel ekiptir. • Veri yetkilisi konseyinin çözemediği sorunları çözüme kavuşturur. • Data Governance süreçleri için kilit rol oynayan veri yetkililerini atama ve değiştirme sorumluluğuna sahiptir. • Data governance süreçlerindeki durumu görüşmek ve işletim için gerekli kararları almak üzere Veri Yönetişim komitesi periyodik olarak 2 ayda bir toplanır.
Veri Yetkilisi Konseyi (Data Stewardship Council)	Veri komitesinin atadığı teknik, iş birimi ve proje veri yetkililerinden oluşur. Veri varlıklarının operasyonel sahibidir, veri hayat döngüsü ve akışıyla ilgili kararları işletir.

Genel

Veri Yetkilisi (Data Stewards)	• Data Governance komitesi tarafından atanır. • Veri yetkilisi, sorumlu olduğu alanda bilgi ve tecrübe sahibi kimselerden atanır. • Veri Yöneticileri kendilerine atanan veri varlıklarından sorumludur. Bu varlıkların toplanması, işlenmesi, korunması ve veriyle ilgili sorunların çözülmesinden sorumludur.
İş Birimi Veri Yetkilisi	• Veri kalitesinden, anlamından ve kullanımından sorumlu anahtar roldür. • Belirli bir iş alanında (hasar, bankasürans, tahsilat vb) bilgi ve tecrübe sahibidir. • İş birimi gözünden veri ihtiyacını, kullanımını ve saklanmasını tanımlar • İhtiyaç halinde sisteme üzerinde veri envanterini ve veri sözlüğünü günceller. • İş veri kalite politikalarını işler.
Proje Veri Yetkilisi	• Projelerde veri varlıklarının ve işleme ihtiyaçlarının doğru tanımlanmasından sorumludur. Çoğunlukla IT analist ekiplerinden atanır. • Veri analizi, bağımlılık, kullanım ve entegrasyon konularında bilgi/tecrübe sahibidir. • İş birimi veri yetkilisi ile beraber çalışır, Teknik veri yetkilisi ve iş birimi veri yetkilisi arasında köprü vazifesi görür.
Teknik Veri Yetkilisi	• ETL, veritabanı, veri depolama, veri mühendisliği, veri güvenliği gibi konularda teknik bilgi ve tecrübe sahibidir. • Veri varlığının teknik izdüşümünün sahibidir. • Teknik veri kalite politikalarını işler.
Veri Sorumlusu	• Verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
Veri Sahibi	• Veri Sahipleri bir Veri Yöneticisi tarafından yetkilendirilmiştir. • Varlıkların uygun kullanımı yönlendirmek için etkili yerel protokolleri uygular. Kurumsal verilere erişim ve bunların kullanımı genellikle uygun Veri Sahibi tarafından yönetilir. • Verilerin sınıflandırılmasından sorumludur. • Veri Sınıflandırma Standardı uyarınca; Veri Sahipleri, verilerin yasal düzenlemelere uygunluğunu sağlamaktan, düzenleme, değişim ve operasyonel işlerin yürütmekten sorumludur.