PROSEDÜR

KİŞİSEL VERİ SAKLAMA, İŞLEME VE İMHA PROSEDÜRÜ

PR.HM.09

26.06.2019

Revizyon Numarası: 00

Hazırlayan	: Kurumsal Hukuk Birim Yöneticisi
1.Onay	: İç Kontrol ve Risk Yönetimi Birim Yöneticisi
2.Onay	: Kurumsal, Teknik, Satış, Hukuk ve Reasürans Genel Müdür Yardımcısı
Yürürlük Onayı	: Genel Müdür

1.0 AMAÇ

Bu Prosedür, Aksigorta Anonim Şirketi ("**Aksigorta**") tarafından gerçekleştirilmekte olan kişisel veri saklama ve imha faaliyetlerine ilişkin iş ve işlemler ile çalışanlarımızın görevlerini ifa ederken ellerine geçen ya da bilgileri dahiline giren tüm Kişisel Verileri (aşağıdaki tanımlara bakınız) gizli tutmalarını 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.) uymalarını sağlamak amacıyla tasarlanmış ve çıkartılmış bulunmaktadır.

2.0 KAPSAM

Bu Prosedür, görevleri kapsamında Kişisel Verileri tamamen veya kısmen otomatik yol ve araçlarla işleyen ya da bir kayıt sisteminin bir parçasını oluşturan ya da bir kayıt sisteminin bir parçasını oluşturması amaçlanan Kişisel Verileri (otomatik yol ve araçlar dışında) başka yol ve araçlarla işleyen tüm çalışanlarımıza; Aksigorta çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin işlenmesi faaliyetlerine ilişkin olarak uygulanır.

3.0 REFERANS VE EKLER

Kalite El Kitabı

Aksigorta Kişisel Verilerin Korunması ve İşlenmesi Yönetmeliği

PR.HM.10	Güvenlik Olaylarına Müdahale Prosedürü
PR.HM.11	Başvuru Yanıtlama Prosedürü
FR.HM.09.01	Kişisel Verilerin Korunması Aydınlatma Metni (Genel)
FR.HM.09.02	Kişisel Verilerin Korunması Aydınlatma Metni (Çalışan)
FR.HM.09.03	Tedarikçilere Veri Gizliliği Bildirim Formu
FR.HM.09.04	Çalışan Veri Gizliliği Taahhütnamesi
FR.HM.09.05	İş Sözleşmesine Eklenecek Kişisel Veri Koruma Maddesi

4.0 TANIMLAR

Acente: Aksigorta ile bir sözleşmeye dayanarak muayyen bir yer veya bölge içinde daimi 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.

KVKK CFT: Genel Müdür Yardımcıları tarafından ilgili departmanlardan üyelerin atanması ile oluşmuş 24.09.2018 tarihli Kurumsal Hukuk Birimi Kararı ile kurulmuş olan komitedir.

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.

Kişisel sağlık verisi: Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgiler.

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: Prosedürde tanımlanmamış olmasına rağmen işbu Prosedür çerçevesinde kişisel verileri işlenen tedarikçi, mağdur, aile bireyleri vb. dâhil fakat bunlarla sınırlı olmamak üzere diğer gerçek kişiler**.**

VERBİS: Veri sorumluları (Aksigorta) veri sicil bilgi sistemi

Veri İrtibat Kişisi: Kişisel verileri koruma kurumu ile kurulacak iletişim için Aksigorta Yönetim Kurulu tarafından VERBİS'e kayıt esnasından bildirilen gerçek kişi.

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 gerçek kişi.

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

5.0 SORUMLULULAR

Aksigorta dahilinde tüm iş birimleri ve çalışanları işbu Prosedür ve Aksigorta Kişisel Verilerin Korunması ve İşlenmesi Yönetmeliği kapsamında belirtilmiş olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının 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 Prosedür ve bu Prosedürde yapılan tüm revizyon ve değişiklikleri incelemek ve onaylamak KVKK CFT'nin sorumluluğundadır. KVKK CFT aynı zamanda prosedürü geliştirmek ve gerekli eğitimleri vermek ile prosedürün yorumlanması konusunda çalışanlara kılavuzluk etmekle görevlidir. KVKK CFT ayrıca bu prosedüre uyulup uyulmadığını denetler ve uyulması için gerekli desteği verir.

b. KVKK CFT işbu prosedürün 6.8. 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. KVKK CFT'nin takibinden sorumlu olduğu Aksigorta periyodik imha süreci 6 ay olarak belirlenmiştir.

d. Kurumsal Hukuk Birimi'nin görevi, Prosedürü ve prosedürde yapılan tüm değişiklikleri incelemek, onaylamak ve Veri Koruma Mevzuatıyla uyumlu hukuki tavsiyelerde bulunmaktır.

e. Genel Müdür veri irtibat kişisinin Prosedürden sapma ve istisna taleplerini incelemek ve onaylamaktadır.

6.0 UYGULAMA

6.1 AKSİGORTA KİŞİSEL VERİ SAKLAMA VE İŞLEME FAALİYETLERİ

İş faaliyetleri sırasında çalışanlarımız, detayları şekilde Aksigorta Kişisel Verilerin Korunması ve İşlenmesi Yönetmeliği'nde belirtilmiş olan Kişisel Verileri işbu prosedürde 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.

6.1.1 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 prosedürün 6.8 maddesinde belirtilmiş olan sürelerde saklanır.

6.1.2 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.

6.1.3 Saklamayı Gerektiren İşleme Amaçları

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

- Kurumsal iletişimi sağlamak,
- Kurum güvenliğini sağlamak,
- İstatiksel çalışmalar yapabilmek,
- Reklam ve kampanya süreçlerinin yürütülmesi,
- **Satış ve pazarlama:** Çalışanlar, müşteri şikayetleri izleme sistemleri yoluyla ve aracılığıyla, müşteriler hakkında Kişisel Verileri işbu prosedürde anılmış şartlarla toplayabilir, işleyebilir ve aktarabilirler.
- **İnsan kaynakları süreçlerini yürütmek:** Çalışanlar, Aksigorta çalışanlarının işe alınması, ücretleri, yan hakları ve bağlantılı konulara ilişkin Kişisel Verileri Türkiye'deki mevcut yasalar çerçevesinde toplayabilir, işleyebilir ve aktarabilirler. Çalışanlar, iş başvuruları hakkında da Kişisel Verileri Türkiye'deki mevcut yasalar çerçevesinde toplayabilir, işleyebilir ve aktarabilirler.
- İmzalanan sigorta sözleşmeleri kapsamında iş ve işlemlerin ifası kapsamında destek hizmet sağlayıcılarına ilişkin süreçlerin yürütülmesi, sigorta tazminatlarının hesaplanması, sigortalı ve lehdara ödemelerin ve rücu takiplerinin yapılması,
- Prim ödemelerinin tahsilatına ilişkin işlemlerin yapılması,
- **Tedarikçiler:** Birlikte çalışılacak, hizmet alınacak herhangi bir şahıs şirketi olması durumunda yetkili gerçek kişinin verileri toplanabilir, işlenebilir ve aktarılabilir.
- Acentelik başvurusu ve acentelik sözleşmeleri kapsamında ilgili süreçlerin yürütülmesi,
- Aksigorta ile iş ilişkisi bulunan gerçek/tüzel kişilerle irtibat sağlamak,
- Yasal raporlamalar yapmak,
- Çağrı merkezleri ile ilgili süreçlerini yönetmek,
- Risk değerlendirme süreçlerinin yönetilmesi,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü

6.1.4 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.

6.2 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
(1)Yazılımlar (a) SAT, (b) AKTİF, (c) JIRA (d) CRM (e) Web (f) Filenet (g) Oracle (h) HR-web (i) Bizbize (j) Kolay Ofis (k) Thos (l) Afus (m) Akçözüm (2)Güvenlik duvarı (a) Cisco (3)Saldırı tespit ve engelleme sistemi (a) Cisco (4)Antivirüs (a) Mcaffe (5)Loglama (a) IBM Qradar (6)Bulut depolama sistemleri (a) Office 365 (7)Kişisel bilgisayarlar	(1) Manuel veri kayıt ortamları (a)Formlar, (b)Belgeler (c)Ziyaretçi kayıt defteri (2) Görsel-Yazılı diğer ortamlar

(8)Cep telefonları (9)Tabletler (10)Ortak Folder sistemi (11)Optik diskler. (12)Kamera kayıt sistemleri (13)Ses kayıt sistemleri (14)Yazıcılar (15)Fotokopi makinaları (16)Tarayıcılar	

6.3 KİŞİSEL VERİ İŞLEME KOŞULLARI

Kişisel verilerin bu prosedüre 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 çalışanlarımız tarafından, Kurumsal Hukuk Birimi tarafından onaylanan formlar ve aydınlatma metinleri kullanılmalıdır.

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

- Kişisel Verileri işlemenin, Veri Süjesinin de taraf olduğu bir sözleşmenin ifası ve uygulanması için ya da bir sözleşmeye girmeden önce Veri Süjesinin talebi üzerine gerekli adımları atmak için zorunlu olması halinde,
- Kişisel Verileri işlemenin bir kanuni yükümlülüğe uymak için zorunlu olması halinde,
- Kişisel Verileri işlemenin bir kamu otoritesinin ya da resmi makamın yetkileri dahilindeki bir görevin ifası için gerekli olması halinde,
- Kamuya açık olan genel bilgilerin, yoruma dayanan bilgilerin ve/veya istatistik veri ve bilgilerinin işlenmesi halinde.

6.3.1 Veri Sorumlusu Olarak Aksigorta'nın Aydınlatma Yükümlülüğü

Veri Sorumlusu olarak işbu prosedürün 6.5 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 prosedürün 6.5. maddesinde sayılmış Veri Süjesinin diğer hakları.

Aydınlatma yükümlülüğü "Kişisel Verilerin Korunması Aydınlatma Metinleri"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 "FR.HM.09.03 Tedarikçilere Veri Gizliliği Bildirim Formu" göndermesi mümkündür.

6.3.2 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.

6.3.3 Çalışanların ve Çalışan Adaylarının Kişisel Verilerinin İşlenmesinde Uyulacak Kurallar

Çalışanlara ait Özel Nitelikli Kişisel Veriler de dahil olmak üzere Kişisel Verilerin İş Kanunu ve diğer ilgili mevzuat uyarınca yahut Aksigorta tarafından belirlenen başka amaçlarla işlenebilmesi için, halihazırda Aksigorta çalışanı bulunan kişilere "FR.HM.09.04 Çalışan Veri Gizliliği Taahhütnamesi"nin imzalatılması suretiyle aydınlatma ve açık rıza temini yükümlüğünün yerine getirilmesi gerekmektedir.

Halihazırda Aksigorta çalışanı durumunda bulunmayan, işe alım süreci olumlu şekilde tamamlanacak olan kişilere ilişkin kişisel verilerin işlenebilmesinin için, ilgili kişiye imzalatılacak olan iş sözleşmesine "FR.HM.09.05 İş Sözleşmesine Eklenecek Kişisel Veri Koruma Maddesi"nin eklenmesi ve iş sözleşmesinin bu haliyle imzalanması suretiyle aydınlatma yükümlülüğünün yerine getirilmesi mümkündür.

6.3.4 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.

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

Görevlerinin bir gereği olarak ve görevleri esnasında, Aksigorta adına Kişisel Verileri işlerken, çalışanlarımızın işbu prosedürde 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.

6.3.6 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 prosedürün diğer maddeleri ve 6.3.5. maddede sözü edilen hususları

gözetmelerinin yanı sıra Veri Koruma Mevzuatı uyarınca Çalışan Veri Gizliliği Taahhütnamesi'ni imzalamaları gerekmektedir.

6.3.7 Kişisel Verilerin Transferi ve Devri Gerçekleştirirken Uyulması Gereken Kurallar

- Çalışanlarımız, Veri Koruma Mevzuatı'nın uyarınca belirlenen koşullar haricinde herhangi bir üçüncü kişiye veri transfer etmeyeceklerdir.
- Çalışanlarımız, Kişisel Verileri, İlgili Kişi'nin açık rızası bulunmadıkça, Kişisel Verileri Koruma Kurulu tarafından belirlenecek ve ilan edilecek olan 'Yeterli Korumanın Bulunduğu Ülkeler' dışında bir ülkeye transfer etmeyeceklerdir.
- 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.

6.4 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.

6.4.1 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.
- Taşınabilir bellek, CD, DVD ortamından aktarılan özel nitelikli kişisel veriler şifrelenerek aktarılmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

6.4.2 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.
- Kağıt 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.

6.5 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 Prosedürü içinde anıldığı şekilde gerçekleşmesi gerekmektedir.

6.6 GÜVENLİK KOŞULLARI

Aksigorta çalışanları, 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 alırlar;

- Kişisel Verilere erişimi sadece görevlerinin ifası esnasında bu bilgilere erişmesi zorunlu olan çalışanlarla 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.
- Kişisel Verilere yetkisiz erişim veya Kişisel Verilerin usulsüz kullanımı gibi olay ve durumlardan haberdar olduğunda bunları derhal âmirine 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 alınan güvenlik tedbirleri periyodik olarak KVKK CFT 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 ve çalışanları tarafından izlenmesi gereken adımlar Aksigorta Güvenlik Olaylarına Müdahale Prosedüründe gösterilmiştir.

6.7 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.

6.7.1 Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-2'de verilen yöntemlerle silinir.

Tablo 2: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda 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 çalışanlar (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 evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için 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.

6.7.2 Kişisel Verilerin Yok Edilmesi

Tablo 3 : 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.

6.7.3 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.

6.8 VERİ TÜRLERİNE GÖRE SAKLANMA VE İMHA SÜRELERİ

Aşağıdaki tabloda belirtilen verilerin ilgili muhafaza süreleri boyunca muhafaza edilmesinden, KVKK CFT sorumludur.

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

Tablo 4: Kişisel veri saklama ve imha süreleri

VERİ TÜRÜ	MUHAFAZA SÜRESİ	İMHA SÜRESİ
E-postalar ve şirket içi yazışmalar	**10 yıl**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmeler	**Sözleşmenin sona ermesini takip eden 10 yıl boyunca**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri Kayıtları	**Müşteri ile girilen son etkileşimi takip eden 10 yıl boyunca**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Çalışan Kayıtları	**Çalıştıkları süre boyunca**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Eski Çalışan Kayıtları	**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
Muhasebe ve Finans Kayıtları	**5 yıl**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket İçi Şikayetler ve İlgili Belgeler	**10 yıl**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuk Kayıtları	**10 yıl**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Resmi Yazışmalar	**Süresiz**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Gerçek Kişi Acente Kişisel Verileri	**İş ilişkisinin sona erme tarihinden itibaren 10 yıl**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Vergi Kayıtları	**5 yıl**	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde