KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

İLGİLİ FORMLAR

•

REFERANS DOKÜMANLAR

- **6698 Sayılı Kişisel Verilerin Korunması Kanunu**
- **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik**
- **Veri Sorumluları Sicili Hakkında Yönetmelik**
- **5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**

1. AMAÇ

İşbu imha politikası **RGN İLETİŞİM HİZMETLERİ A.Ş.**(Bundan sonra "Şirket" olarak anlılacaktır) olarak veri sorumlusu sıfatıyla elimizde bulundurduğumuz kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuatı uyarınca kişisel verilerin silinmesi, yok edilmesine ilişkin Şirket tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika; Şirket Paydaşları, Şirket Yetkilileri, İş Ortağı/Tedarikçiler, iştirakçılar, Çalışan, Çalışan Adayları'mız, Ziyaretçiler'imiz, Şirket ve Grup Şirket Müşterileri, Potansiyel Müşterilerin kişisel verilerinin işlendiği tüm kayıt ortamlarını ve kişisel veri işlenmesine yönelik faaliyetleri kapsar.

3. TANIMLAR

Elektronik Ortam	**:**	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
Elektronik Olmayan Ortam	**:**	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar
İlgili kişi	**:**	Kişisel verisi işlenen gerçek kişiyi,
İmha	**:**	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

Kanun	**:**	07.04.2016 tarih ve 29677 sayılı Resmi Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanununu,
Yönetmelik	**:**	28.10.2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğini
Kurul	**:**	Kişisel Verileri Koruma Kurulunu
Politika	**:**	Kişisel Verileri Saklama ve İmha Politikası
Kayıt ortamı	**:**	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı
Bilgi Güvenliği ve KVK Komitesi	**:**	Politikanın yürütülmesi, yayınlanması ve güncellenmesinden sorumlu birim
Kişisel Verilerin İşlenmesi ve Korunması Politikası	**:**	Şirket elinde bulunan kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen politikayı,
Kişisel Veri	**:**	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Özel Nitelikli Kişisel Veri	**:**	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf yada sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.
Periyodik İmha	**:**	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Kişisel Veri Sahibi	**:**	Kişisel verisi işlenen gerçek kişi.
Açık Rıza	**:**	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Veri Sorumlusu	**:**	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi,
Veri İşleyen	**:**	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.
Kişisel Verilerin İşlenmesi	**:**	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi,

		depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması yada kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem

4. SORUMLULUK

Bu politikanın güncellenmesinin sağlanmasından Bilgi Güvenliği ve KVK Komitesi, uygulanmasından süreç sahipleri, taraflar ve tüm çalışanlar sorumludur ve politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında Bilgi Güvenliği Komitesine aktif olarak destek verirler.

Kişisel verilerin korunması uygulamasının yönetilmesi kapsamında Bilgi Güvenliği Komitesinin sorumlulukları;

• Kişisel verilerin işlenmesi ve korunması ile ilgili temel politikaları ve mevzuatla uyum sağlanması için yapılması gerekenleri belirlemek,
- ihtiyaç duyulan teknik çözümlerin sunulması

- Çalışanların politikaya uygun hareket etmesini sağlamak

• Belirlenen temel politika ve aksiyon adımlarını üst yönetimin onayına sunmak; uygulamasını gözetmek ve koordinasyonunu sağlamak,

• Kişisel verilerin işlenmesi ve korunmasına ilişkin politikaların ne şekilde uygulanacağına ve denetimin ne şekilde yapılacağına karar vermek, üst yönetimin onayını aldıktan sonra gerekli görevlendirmelerde bulunmak,

• Süreç sahipleri, süreçleri kapsamında kişisel veri işleme faaliyetlerinde oluşabilecek riskleri tespit ederek gerekli önlemlerin alınmasını temin etmek; iyileştirme önerilerini üst yönetimin onayına sunmak,

• Çalışanların kişisel verilerin korunması ve şirket politikaları konusunda eğitimlerini sağlamak,

• Kişisel veri sahiplerinin başvurularını en üst düzeyde karara bağlamak,

• Kişisel verilerin korunması konusundaki gelişmeleri takip etmek; bu gelişmeler kapsamında yapılması gerekenler konusunda ilgili taraflara tavsiyelerde bulunmak,

5. KAYIT ORTAMLARI VE GÜVENLİK TEDBİRLERİ

Rgn nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur.
Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibariyle matbu ortamlar, yerel dijital ortamlar ortamlardır.

Matbu ortamlar	**:**	1. Verilerin kağıt ya da mikrofilmler üzerine basılarak tutulduğu, 2. Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri)

		3. Yazılı,basılı,görsel ortamlardır.
Yerel dijital ortamlar	**:**	1. Şirket bünyesinde yer alan sunucular, sabit ya da taşınabilir diskler, optik diskler, 2. Yazılımlar (ofis yazılımları, İK, muhasebe yazılımları e posta sistemleri) 3. Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) 4. Kişisel bilgisayarlar (Masaüstü, dizüstü) 5. Mobil cihazlar (telefon, tablet vb.) 6. Çıkartılabilir bellekler (USB, Hafıza Kart vb.) 7. Yazıcı, tarayıcı, fotokopi makinesi sair dijital ortamlardır.

Kanun'un 12'nci maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası hükümlerinin uygulanmasına ilişkin şirket içi denetimler yapmaktadır.
Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilir.

RGN, kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır.

İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi kapsamında ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düştüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsar.

5.1.1Teknik Tedbirler

RGN, kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki teknik tedbirleri almaktadır:

- Kişisel verilerin tutulduğu ortamlarda yalnızca teknolojik gelişmelere uygun güncel ve güvenli sistemler kullanılmaktadır.
- Kişisel verilerin tutulduğu ortamlara yönelik güvenlik sistemleri kullanılmaktadır.
- Bilişim sistemleri üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri ve araştırmaları yapılmakta, yapılan test ve araştırmaların sonucunda tespit edilen mevcut ya da muhtemel risk teşkil eden hususlar giderilmektedir.
- Kişisel verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmekte ve tüm erişimler kayıt altına alınmaktadır.
- Şirket bünyesinde kişisel verilerin tutulduğu ortamların güvenliğini sağlamak üzere yeterli teknik personel bulundurmaktadır.
- Çevresel tehditlere karşı bilgi teknolojileri sistemleri güvenliğinin sağlanması için, donanımsal ve yazılımsal önlemler alınmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.

5.1.2 İdari Tedbirler

RGN, kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki idari tedbirleri almaktadır:

- Kişisel verilere erişimi olan tüm Şirket çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapılmaktadır.
- Bilgi güvenliği, özel hayatın gizliliği ve kişisel verilerin korunması alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alınmaktadır.
- Kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalanmakta, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özen gösterilmektedir.
- Kurum tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce Kurum tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kurum içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi Güvenliği ve KVK eğitimleri verilmektedir.
- Bilgi güvenliği analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.

5.1.3. Şirket İçi Denetim

Şirket, Kanun'un 12'nci maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası hükümlerinin uygulanmasına ilişkin şirket içi denetimler yapmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilir.

Denetim sırasında ya da sair bir şekilde Şirket sorumluluğunda bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması hâlinde, Şirket bu durumu en kısa sürede ilgilisine ve Kurula bildirir.**Veri İhlali Müdahale Planı** hükümlerince süreç yönetilir.

6. KİŞİSEL VERİLERİN İMHASI

6.1 SAKLAMA VE İMHA NEDENLERİ

6.1.1 Saklama Nedenleri

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü 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 ve 6 ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, Şirketimiz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

6.1.2.Saklamayı Gerektiren Hukuki Sebepler

RGN'de, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

• 6698 sayılı Kişisel Verilerin Korunması Kanunu,
• 6098 sayılı Türk Borçlar Kanunu,

- 4734 sayılı Kamu İhale 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,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

6.1.3 İmha Nedenleri

RGN bünyesinde bulunan kişisel veriler ilgili kişinin talebi halinde ya da Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenlerin ortadan kalkması halinde resen işbu imha politikası uyarınca silinir, yok edilir. Kişisel Veriler;

a) İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
b) İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
c) Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
d) Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,
e) RGN'nin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
f) Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

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

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

6.2 İMHA YÖNTEMLERİ

Şirket, Kanuna ve sair mevzuata uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re'sen siler yok eder.

Şirket tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

6.2.1 Silme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri		
Karartma	**:**	Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin karartılması ile yapılır.

Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri		
Yazılımdan güvenli olarak silme	**:**	Yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz.

6.2.2 Yok Etme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri		
Fiziksel yok etme	**:**	Matbu ortamda tutulan belgeler evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok edilir.
Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri		
Fiziksel yok etme	**:**	Kişisel veri barındıran optik ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.

6.2.3.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.

7. SAKLAMA VE İMHA SÜRELERİ

Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir. Veri saklama ve imha süreleri envanterde belirtilmiştir.

7.1 Saklama Süreleri

KİŞİSEL VERİ KATEGORİZASYONU	AZAMİ SAKLAMA SÜRELERİ

Özlük Bilgisi; **Kimlik** **İletişim** **Lokasyon** **Hukuki işlem** **Mesleki deneyim** **Irk ve etnik köken** **Ceza mahkumiyeti ve güvenlik tedbirleri** **Felsefi inanç, din, mezhep ve diğer inançlar**	Çalışma süresi boyunca ve çalışanın işten ayrılma tarihinden itibaren 15 yıl süreyle saklanır.
Çalışanların Kişisel Sağlık Dosyaları	Çalışma süresi ve Çalışanın işten ayrılma tarihinden itibaren İSG evrakları 15 yıl süreyle saklanır.
Çalışan Adayı Bilgileri	Aday bilgisi en fazla 10 yıl olmak üzere özgeçmişin güncelliğini kaybedeceği süre kadar, ses kaydı 1 yıl süre ile saklanır.
Müşteri Bilgileri	Tüzel kişi müşterinin gerçek kişi temsilcisine ait bilgiler, Türk Ticaret Kanunu md.82 uyarınca ticari defter ve kayıtlara dayanak teşkil eden faturaların düzenlenmesine esas bilgiler anılan kanun maddesi gereği 10 yıl süre ile saklanır.
Ziyaretçi Bilgileri	Etkinliğin sona ermesinden İtibaren 2 yıl süre ile saklanır.
İş Ortağı/Çözüm Ortağı/Danışman Bilgileri	İş Ortağı/Çözüm Ortağı/Danışmanın, Şirket ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 uyarınca 10 yıl süre ile saklanır.
Şirket'in İşbirliği İçinde Olduğu Kurum/Firmalar Tarafından Şirket ile Paylaşılan Kişisel Veriler	Şirketin İşbirliği İçinde Olduğu Kurum/Firmaların Şirketin ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 uyarınca 10 yıl süre ile saklanır.
İnternet Sitesi Ziyaretçisi	İnternet Sitesi Ziyaretçisine ait ad, soyad,E- Posta, telefon, IP adres ve CV, gezinme hareket bilgileri 5 yıl süre ile saklanır.
Stajyer(öğrenci) **Stajyer'e ait staj dosyasında yer alan bilgiler**	Staj ilişkisi süresince ve bitimininden itibaren 15 yıl süreyle saklanmaktadır.

Görsel kayıtlar; Kamera kayıtları	CCTV kameraları uyarınca güvenlik amaçlı olarak işlenen kişisel veriler 3 ay, sözleşmede ayrıca süre belirlenmişse maximum 1 yıl süre ile saklanır.
Muhasebe ve Finansal İşlemlere İlişkin tüm kayıtlar	Çalışma Süresi + iş ilişkisinin sona ermesinden itibaren 10 yıl süreyle muhafaza edilir.
Risk Yönetimi	Ticari, teknik, idari risklerin yönetilmesi için işlenen bilgilerin 5 yıl süre ile saklanır.
Çağrı Kayıtları (Müşteri Temsilcisi Görüşmeleri)	Hizmet verilen müşterilere sözleşmelerden kaynaklanan yükümlülükler ve bilgi güvenliği ve hizmete ilişkin kayıt ve bilgilerin talep üzerine temin edilmesi yükümlülüklerimiz ile hizmet kalitesine ilişkin taahhütlerimizin ifası nedeniyle en fazla Projenin sona ermesini takiben 5 yıl süre ile saklanabilir.
Personele Ait Log Kayıtları	Çalışma süresi boyunca ve çalışanın işten ayrılma tarihinden itibaren 15 yıl süreyle saklanır.

* Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.

7.2 İmha Süreleri

RGN, Kanun, ilgili mevzuat işbu Kişisel Verileri Saklama ve İmha Politikası uyarınca sorumlu olduğu kişisel verileri silme, yok etme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder.
İlgili kişi, Kanunun 13'ncü maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder. Şirket'in talebi almış sayılması için ilgili kişinin talebini mevzuata ve **KVKK Başvuru Formu**na uygun olarak yapmış olması gerekir. Şirket, her halde yapılan işlemle ilgili kişiye bilgi verir.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından Kanunun 13'ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

8. PERİYODİK İMHA

Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda; Şirket işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek bir işlemle siler, yok eder. Periyodik imha süreçleri ilk kez 30.06.2018 tarihinde başlar ve her 6 (altı) ayda bir tekrar eder.

9. İMHA İŞLEMİNİN HUKUKA UYGUNLUĞUNUN DENETİMİ

RGN, gerek talep üzerine gerekse periyodik imha süreçlerinde re'sen gerçekleştirdiği imha işlemlerini Kanuna, sair mevzuata, işbu Kişisel Veri Saklama ve İmha Politikasına uygun olarak yapar.
Şirket, imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla bir takım idari ve teknik tedbirler almaktadır.

9.1 Teknik Tedbirler

- Şirket, işbu politikada yer alan imha yöntemine uygun teknik araç ve ekipman bulundurur.
- Şirket, imha işlemlerinin yapıldığı yerin güvenliğini sağlar.
- Şirket, imha işlemini yapan kişilerin erişim kayıtlarını tutar.
- Şirket, imha işlemini yapacak yetkin ve tecrübeli elemanlar istihdam eder ya da gerektiğinde yetkin üçüncü kişilerden hizmet alır.

9.2 İdari Tedbirler

- RGN, imha işlemini yapacak çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapar.
- RGN, bilgi güvenliği, özel hayatın gizliliği, kişisel verilerin korunması ve güvenli imha teknikleri alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alır.
- RGN, teknik ya da hukuki gereklilikler nedeniyle imha işlemini üçüncü kişilere yaptırdığı durumlarda ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalar, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.
- RGN, imha işlemlerinin hukuka ve işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen şart ve yükümlülüklere uygun olarak yapılıp yapılmadığını düzenli olarak denetler, gereken aksiyonları alır.
- RGN, kişisel verilerin silinmesi, yok edilmesi ilgili yapılan bütün işlemleri kayıt altına alır ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklar.

10.KİŞİSEL VERİ KOMİTESİ

Şirket bünyesinde Kişisel Veri Komitesi "Bilgi Güvenliği ve KVK Komitesi" üyelerinden oluşmaktadır. Kişisel Veri Komitesi, ilgili kişilerin verilerinin hukuka ve Kişisel Veri Saklama ve İmha Politikasına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir.

Kişisel Veri Komitesi bir yönetici (Başkan), idari ve teknik üyelerden oluşur. Üyeler CEO, CTO, CFO, COO, CHRO, Teknoloji Hizmetleri Direktörü, İç Denetim Müdürü ve Üye Sekreterdir.

Kişisel Veri Komitesinde görevli Şirket çalışanlarının unvanları ve görev tanımları aşağıda belirtilmiştir:

Unvan		Görev Tanımı
Kişisel Veri Komitesi Yöneticisi(Başkan)	**:**	Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; Kanun ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür.
KVK Uzmanı (Üye) (Teknik ve İdari)	**:**	İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Komitesi Yöneticisine raporlanmasından; Kişisel Veri Komitesi Yöneticisi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Komitesi Yöneticisinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Komitesi Yöneticisine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur.

11.GÜNCELLEME VE UYUM

Şirket, Kanunda yapılan değişiklikler nedeniyle, Kurum kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında değişiklik yapma hakkını saklı tutar.
İşbu Kişisel Veri Saklama ve İmha Politikasında yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar politikanın sonunda açıklanır.

12. POLİTİKANIN YAYINLANMASI VE SAKLANMASI

Politika, web sitesinde ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır.

13. DEĞİŞİKLİK NOTLARI

04.04.2018	**:**	Kişisel Veri Saklama ve İmha Politikası yayınlanmıştır.
19.07.2019	**:**	Gözden geçirilerek güncelleme yapılmıştır
10.07.2020	**:**	Gözden geçirilerek güncelleme yapılmıştır
19.10.2021	**:**	Gözden geçirilerek güncelleme yapılmıştır
27.06.2022	**:**	Gözden geçirilerek 6 ve 7.1 maddesi güncellenmiştir.

Daha eski tarihli bir değişiklik bulunmamaktadır.

HR Sisteminden ve mailden okuduğum bu belgeyi kabul, beyan ve taahhüt ederim.