RASYOTEK İNSAN KAYNAKLARI BİLİŞİM A.Ş

SAKLAMA VE İMHA POLİTİKASI

AĞUSTOS 2019

SÜRÜM 1.0

İçindekiler

ÖNSÖZ

RASYOTEK İnsan Kaynakları ve Bilişim A.Ş. (“RASYOTEK” veya “Şirket”), teknolojik altyapısı ve geliştirdiği yazılımları ile **“Teknolojik İnsan Kaynakları”** kurgusunda **“**Bütünleşik Teknolojik” dijital dönüşüm sürecinde piyasaya sunmaktadır.

İşletmelerin ana faaliyet konuları, yani varlık sebepleri dışında kalan tüm iş süreçlerinde, teknolojik verimlilik esasıyla asiste hizmetler sunan Rasyotek; bu sayede günümüz iş dünyasında, farklı uzmanlık alanlarını işletmeler adına üstlenerek, müşterilerinin asıl işlerine olan konsantrasyonuna imkan tanımaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu’nun (“Kanun”) 16. Maddesi kapsamında Veri Sorumluları Sicili’ne (“VERBİS”) kayıt yükümlülüğü bulunan veri sorumluları, hazırlamış oldukları kişisel veri işleme envanterlerine uygun olarak, işlenen verilerin saklanması ve imhasına ilişkin sürecin belirlenmesi adına saklama ve imha politikası oluşturmakla yükümlü kılınmıştır. RASYOTEK, Kanun’a uyum sürecinde VERBİS’e kayıt yükümlülüğünü yerine getirmiş olmakla birlikte Kanun’dan doğan diğer yükümlülüklerini de eksiksiz yerine getirmek suretiyle kişisel veri işleme faaliyetlerinin tümünü hukuka uygun olarak yerine getirmeyi ve kişisel verilerin güvenliğini en yüksek düzeyde sağlamayı hedeflemektedir. İşbu Kişisel Verileri Saklama ve İmha Politikası (“Politika”) Kanun ve 28.10.2017 tarihli 30224 sayılı Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (“Yönetmelik”) hükümleri doğrultusunda hazırlanmış olup Şirket içerisinde fiilen uygulanmakta olan mevcut yöntemlerde veya mevzuat düzenlemelerinde değişiklik olması halinde Politika üzerinde ilgili güncellemeler yapılmaktadır.

I. AMAÇ, KAPSAM VE KULLANICILAR

RASYOTEK, hukuki ve sosyal sorumluluğunun bir parçası olarak öncelikle Kanun'dan doğan yükümlülüklerini yerine getirmek amacıyla gerekli tüm çalışmaları yapmakta ve veri işleme faaliyetlerini mevzuat hükümleri çerçevesinde gerçekleştirmektedir. Bu doğrultuda Yönetmelik'in 5 inci ve 6 ncı maddeleri kapsamında kişisel verilerin saklanması ve imhasına ilişkin yükümlülüklerin ve Yönetmelik'te belirtilen sair yükümlülüklerin yerine getirilmesi ve kişisel veri koruma, işleme ve imha düzenlemelerine ilişkin bu mevzuata dayanılarak çıkarılan Yönetmelik/Tebliğlere uymayı da taahhüt etmektedir.

İşbu Politika, yürürlükteki mevzuat çerçevesinde kişisel veri korumasının sağlanması ve Kanun ile diğer ilgili mevzuat kapsamında kişisel verilerin ve özel nitelikli kişisel verilerin saklanma sürelerine riayet edilerek muhafaza edilmesi ve gerekli veri imha çalışmalarının yapılması için uygulanmakta olan çerçeve koşulları içermekte olup RASYOTEK tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Politika, RASYOTEK nezdinde tutulan, Kanun ile tanımlanan kişisel verileri ve özel nitelikli kişisel verileri, tüm RASYOTEK çalışanlarını, yöneticilerini ve kişisel veri paylaşımı söz konusu olan tüm durumlarda hizmetlerin yürütülmesi amacıyla RASYOTEK'in iş ortaklarını, tedarikçilerini, hissedarlarını, çalışan adaylarını, ürün ve hizmet alan kişileri, ziyaretçileri ve RASYOTEK'in sair hukuki ilişkiye girdiği gerçek ve tüzel kişileri kapsamaktadır.

Politika Kanun'da belirtildiği şekilde, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla verilerin işlendiği sistemlerde yer alan kişisel verileri ve özel nitelikli kişisel verileri kapsamaktadır.

İstatistiki değerlendirmeler, anket çalışmaları veya çalışmalar için elde edilen veriler gibi anonim hale gelmiş ve tanımlanamayan veri ve tüzel kişilere ilişkin veriler, Kanun'un 28

inci maddesi kapsamında kişisel veri olarak kabul edilmemektedir ve işbu Politika'ya tabi değildir.

İşbu Politika Kanun ve ilgili düzenlemeler doğrultusunda ve RASYOTEK prosedürleri gereğince güncellenmekte olup, yapılan değişiklikler güncellemenin www.rasyotek.com.tr adresinde paylaşılması ile yürürlüğe girecektir.

II. TANIMLAR

4857 sayılı Kanun	: 4857 sayılı İş Kanunu
5502 sayılı Kanun	: 5502 sayılı Sosyal Güvenlik Kanunu
5510 sayılı Kanun	: 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
5651 sayılı Kanun	:5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
6331 sayılı Kanun	: 6331 sayılı İş Sağlığı ve Güvenliği Kanunu
6698 sayılı Kanun	: 6698 sayılı Kişisel Verilerin Korunması Kanunu
Açık Rıza	: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Alıcı Grubu	: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi
Anayasa	: 9 Kasım 1982 tarihli ve 17863 sayılı Resmî Gazete' de yayımlanan 7 Kasım 1982 tarihli ve 2709 sayılı Türkiye Cumhuriyeti Anayasası
Anonim Hale Getirme	: Kişisel verilerin, başka verilerle eşleştirilerek ve/veya birleştirilerek dahi hiçbir suretle kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemi.
Çalışan	: RASYOTEK İnsan Kaynakları Bilişim A.Ş. personeli.
Elektronik Ortam	:Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ve tüm bu

	işlemlerin gerçekleştirilmesi için farklı yetkilendirmelerin uygulandığı ortamlar.
Elektronik Olmayan Ortam	: Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
İmha	: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kayıt Ortamı	: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olamayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
Kişisel Veri	: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kişisel Veri İşleme Envanteri	: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter
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 ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem
Kişisel Verilerin Silinmesi	: Kişisel verilerin hiçbir surette tekrar erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi.

Kişisel Verilerin Yok Edilmesi	: Kişisel verilerin hardware ve software (yani fiziki ve elektronik ortamda) hiçbir kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi. (Örneğin; bir CD veya flash diskin imha edilmesi, parçalanması veya yakılması, personel özlük dosyasının yakılması, yeniden kâğıt haline getirilmesi vs.)
KVKK/Kanun	: 7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu
Kurul	: Kişisel Verileri Koruma Kurulu
Kurum	: Kişisel Verileri Koruma Kurumu
Özel Nitelikli Kişisel Veri	: Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı,ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.
Periyodik İmha	: Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda tekrar eden aralıklarla re' sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Politika	: Kişisel Verileri Saklama ve İmha Politikası
RASYOTEK	: RASYOTEK İnsan Kaynakları Bilişim A.Ş
RASYOTEK KVK Kurulu	: RASYOTEK nezdinde kurulmuş olan ve işbu Politika'nın yürütülmesinden ve takibinden sorumlu olan Kurul
RASYOTEK SUPER PORTAL	: RASYOTEK' ten hizmet alan tüzel kişiliklerin verilerine dair raporlamaların ve taleplerin yönetildiği dijital platform
Sicil/VERBİS	: Veri Sorumluları Sicili
Veri İşleyen	: Veri sorumlusunun vermiş olduğu yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişi
Veri İşleyen	: Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.

Veri Kayıt Sistemi	: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri Sahibi/İlgili Kişi/İlgili Kişiler	: Kişisel verisi işlenen gerçek kişi
Veri Sorumlusu	: Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
Yönetmelik	: 28 Ekim 2017 tarihli 30224 sayılı Resmî Gazete' de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

III. SORUMLULUK VE GÖREV DAĞILIMLARI

Kanun, Yönetmelik ve Politika ile belirtilen verinin imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar, danışmanlar, iş ortakları ve sair surette RASYOTEK nezdinde kişisel veri saklayan ve işleyen herkes bu gerekleri yerine getirmekten sorumludur.

Her iş birimi kendi iş süreçlerinde ürettiği veriyi saklamak ve korumakla yükümlüdür; ancak üretilen verinin iş biriminin kontrolü ve yetkisi dışında sadece bilgi güvenliği sisteminde bulunması durumunda, söz konusu veri bilgi güvenliği sistemlerinden sorumlu birimler tarafından saklanacaktır. İş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar doğmasına neden olacak periyodik imhalar, ilgili kişisel verinin türü, içinde yer aldığı sistemler ve veri sahibi iş birimi dikkate alınarak kural olarak bilgi güvenliği sistemleri bölümlerince yapılacaktır.

Verilerin fiziksel ortamlarda tutulması durumunda Şirket içerisinde ilgili departman tarafından periyodik imha sürelerine veya ilgili kişinin talebi dahilinde iletilecek veri imha süreçlerine bağlı kalınarak kişisel verilerin imhası sağlanacaktır. Şirket, her departman özelinde veri imha süreçleri ve işbu Politika' da belirtilen usul ve esaslar hakkında tüm çalışanlarını, iş ortaklarını ve sair RASYOTEK nezdinde kişisel veri saklayan kişileri bilgilendirdiğini taahhüt etmektedir.

Tablo 1: Saklama ve imha süreçleri görev dağılımı

Personel	Unvan	Birim	Görev Tanımı
Erdem GÖNENÇ	Siber Güvenlik, Veri Koruma ve Teknoloji Birim Müdürü	IT, KVKK, SİBER GÜVENLİK	Şirketin ve şirket alt yapısının siber güvenlik bakımından doğru bir kurguda yapılanmasının sağlanması
Selçuk USTA	Yazılım Geliştirme Müdürü	YAZILIM	Yazılım geliştirme ve süreç yönetiminin sağlanması
Kemal UZUN	Kıdemli Veri Tabanı Yöneticisi	YAZILIM	Veri tabanı yönetiminin sağlanması

IV. DOKÜMAN İÇERİĞİ

1. Kayıt Ortamları

Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam, kayıt ortamı kapsamına girmektedir. Bu kapsamda kişisel veriler, RASYOTEK tarafından aşağıda sıralanan ortamlarda hukuka uygun olarak saklanmaktadır.

Tablo 2: Verilerin muhafaza edildiği kayıt ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Personel Bilgisayarları	Kağıt ortamları
Sunucu Sistemleri	Manuel veri kayıt sistemleri (Başvuru formları, ziyaretçi kayıt defteri)
Kamera Kayıt Sistemleri	Özlük dosyaları
PDKS Sistemleri	Kilitli birim dolapları
	Arşiv (İnsan Kaynakları, Muhasebe, …)

2. Kişisel Verilerin Saklanması

2.1. Saklamaya İlişkin Açıklamalar

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. RASYOTEK tarafından işlenmekte olan kişisel veriler, Kanun kapsamında oluşturulan envanter ve Kişisel Veri İşleme Politikası'nda detayları belirtildiği üzere çeşitli hukuki sebepler ile ve kanuni yükümlülükler gereğince belirlenen süreler kadar Şirket nezdinde saklanmaktadır.

2.2.Saklamayı Gerektiren Hukuki Sebepler

RASYOTEK nezdinde gerçekleştirilen faaliyetler kapsamında işlenen kişisel veriler aşağıda yer alan mevzuatlarda öngörülen süreler kadar yukarıda açıklanan kayıt ortamlarında muhafaza edilmektedir.

- 4857 sayılı İş Kanunu
- 5502 sayılı Sosyal Güvenlik Kanunu

- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu
- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6102 sayılı Türk Ticaret Kanunu
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 193 sayılı Gelir Vergisi Kanunu,
- 4447 sayılı İşsizlik Sigortası Kanunu,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Aktif İşgücü Hizmetleri Yönetmeliği

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır

2.3.Saklamayı Gerektiren Veri İşleme Amaçları

RASYOTEK tarafından işlenmekte olan kişisel veriler; aşağıda sayılan amaçlar dahilinde mevzuatlarda öngörülen süreler ile Şirket nezdinde saklanmaktadır.

- Ürün veya hizmet alıcısına ileri zamanlı teklif yapılabilmesi,
- Avans takiplerinin yapılması,
- Çalışan ve ziyaretçi kayıtlarının oluşturulması
- Avans takiplerinin yapılması
- Geriye dönük teşviklerin sisteme girilmesi sürecinin yürütülmesi,
- Güncel/geçmiş dönem teşvik hesaplaması raporlamalarının SGK ile teyit edilmesi,
- Faaliyetlerinin hukuka uygun olarak yürütülmesi,
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde hukuki yükümlülüklerin yerine getirilmesi,
- İnsan kaynakları süreçlerinin yürütülmesi, iş başvurularının değerlendirilmesi
- İletişim faaliyetlerinin yürütülmesi,

- Potansiyel müşterilerin tespiti ve iletişim sağlanması,
- Müşteri/Tedarikçi cari kayıtlarının takibi
- Pilot çalışmaların tamamlanması
- Sözleşmelerin kurulması ve sözleşmeden doğan yükümlülüklerin ifası

2.4.Kişisel Verilerin Saklanma Süreleri

RASYOTEK, gerçekleştirmekte olduğu faaliyetleri kapsamında işlemekte olduğu kişisel verileri Kanun'un 4 üncü maddesinde yer alan veri işleme ilkelerine uygun olarak aşağıda belirtilen süreler kadar muhafaza etmektedir.

Tablo 3: Kişisel verilerin saklanma süreleri

Veri Kategorisi	Saklama Süresi
Kimlik	İlgili sözleşmenin sona ermesini takiben 10 yıl
İletişim	İlgili sözleşmenin sona ermesini takiben 10 yıl
Lokasyon	Yargılama ve diğer hukuki süreçlerin sona ermesini takiben 10 yıl
Özlük	İlgili sözleşmenin sona ermesini takiben 10 yıl
Hukuki İşlem	Yargılama ve diğer hukuki süreçlerin sona ermesini takiben 10 yıl
Müşteri İşlem	5 yıl
Fiziksel Mekan Güvenliği	2 yıl
Finans	İlgili sözleşmenin sona ermesini takiben 10 yıl
Mesleki Deneyim	İş sözleşmenin sona ermesini takiben 10 yıl
Görsel ve İşitsel Kayıtlar	İlgili sözleşmenin sona ermesini takiben 10 yıl
Sendika Üyeliği	İş sözleşmenin sona ermesini takiben 10 yıl
Sağlık Bilgileri	İş sözleşmenin sona ermesini takiben 10 yıl
Ceza Mahkumiyeti ve Güvenlik Tedbirleri	İş sözleşmenin sona ermesini takiben 10 yıl
Denetim ve Teftiş Bilgisi	İş sözleşmenin sona ermesini takiben 2 yıl
Sigorta Bilgisi	İş sözleşmenin sona ermesini takiben 2 yıl
Çalışan Aday Bilgisi	6 ay
Çalışan Bilgisi	İlgili sözleşmenin sona ermesini takiben 10 yıl

Araç Bilgisi	İş sözleşmenin sona ermesini takiben 2 yıl
Olay Yönetim Bilgisi	İş sözleşmenin sona ermesini takiben 2 yıl
Çalışan Performans ve Kariyer Gelişim Bilgisi	İş sözleşmenin sona ermesini takiben 2 yıl
Talep Şikayet Yönetim Bilgisi	İş sözleşmenin sona ermesini takiben 2 yıl
Aile Bireyleri ve Yakın Bilgisi	İş sözleşmenin sona ermesini takiben 2 yıl
Şirket Bilgisi	İlgili sözleşmenin sona ermesini takiben 2 yıl
Tapu Bilgileri	Yargılama ve diğer hukuki süreçlerin sona ermesini takiben 10 yıl
Yan Haklar ve Menfaatler Bilgisi	İş sözleşmenin sona ermesini takiben 2 yıl
Çalışan İşlem Bilgisi	6 ay

3. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi

Kanun'un 7 inci maddesi uyarınca, Kanun ve diğer ilgili mevzuatta yer alan düzenlemelere uygun olarak işlenmiş olmasına rağmen işlenme sebeplerinin ortadan kalkması halinde kişisel verilerin, re'sen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir. İşbu düzenleme kapsamında RASYOTEK, aşağıda açıklanacak usul ve yöntemler ile kişisel verilerin imhasını gerçekleştirmekte ve Kanun'dan doğan yükümlülüklerini yerine getirmektedir.

RASYOTEK, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemleri esnasında gerekli tüm idari ve teknik tedbirleri almaktadır.

3.1. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesini Gerektiren Sebepler

İlgili kişilerin kişisel verileri, yukarıda sayılmış olan kişisel veri işleme nedenlerinin ortadan kalkması, işlemeye esas teşkil eden mevzuatın değişmesi veya mülga hale gelmesi, Kanun'un 11 inci maddesi uyarınca ilgili kişinin kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun RASYOTEK tarafından kabul edilmesi, RASYOTEK'in, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanun'da öngörülen süre içinde cevaplamaması ihtimallerinde; ilgili kişinin

Kurul'a şikayette bulunması ve bu talebin Kurul tarafından uygun görülmesi durumlarında gerçekleştirilecek ilk periyodik imha sırasında imha edilmektedir.

3.2.Kişisel Verilerin Silinmesi Yöntemleri

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. RASYOTEK, verilerin muhafaza edildiği kayıt ortamlarına göre verilerin silinmesi için ayrı yöntemler uygulamaktadır.

Kişisel verilerin silinmesi sürecinde öncelikle silme işlemine konu edilecek kişisel veriler belirlenmekte, erişim yetki/kontrol matrisi kullanılmak suretiyle ilgili veriye erişim yetkisi bulunan kullanıcılar belirlenmekte, ilgili kullanıcıların kişisel veriler üzerindeki erişim, geri getirme, tekrar kullanma gibi yetkileri kaldırılmakta ve aşağıda yer alan yöntemler ile veriler silinmektedir.

Tablo 4: Kişisel verilerin silinmesi yöntemleri

Kayıt Ortamı	Silme Yöntemi
Bulut Çözümleri	Bulut çözümünden alınan yazılım olarak hizmet (Software as a Service – SaaS) ürünü, ilgili çözüm platformu üzerinden sonlandırılır. Bulut çözümünün taahhütü doğrultusunda verinin silindiği kabul edilir.
Merkezi Sunucular	Dijital ortamda fiziksel ve/veya sanal diskler vasıtasıyla saklanan veri, imha bölümüne (partition) alınarak fiziksel olarak silinir (delete).
Elektronik Ortamlar	Dijital ortamda fiziksel ve/veya sanal diskler vasıtasıyla saklanan veri, imha bölümüne (partition) alınarak fiziksel olarak silinir (delete).

Fiziksel Ortamlar	Kağıt ortamında bulunan veriler karartma yöntemi ile silinmekte, bu süreçte; ilgili evrak üzerindeki kişisel veriler geri dönülemeyecek ve teknolojik çözümlemelerle okunamayacak şekilde sabit mürekkep kullanılarak veya kesilerek kullanılamaz hale getirilmektedir. Arşivde bulunan kişisel veriler bakımından silme işlemi arşive erişim yetkisi bulunan kişi tarafından diğer kullanıcılar için tekrar kullanılamaz hale getirilmesi yöntemi ile uygulanmakta, kilitli birim dolaplarında bulunan kişisel veriler için de yine erişim yetkisi bulunan kullanıcı tarafından aynı yöntem uygulanmaktadır.

3.3.Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Kişisel verilerin yok edilmesi için verilerin bulunduğu ortamlar ile tüm kopyaları tespit edilmekte ve tüm veriler için aşağıda belirtilen yöntemler uygulanmak suretiyle kişisel veriler yok edilmektedir.

Tablo 5: Kişisel verilerin yok edilmesi yöntemleri

Kayıt Ortamı	Yok Etme Yöntemi
Bulut Çözümleri	DLP Sistemleri ile imha edilmektedir.
Merkezi Sunucular	DLP Sistemleri ile imha edilmektedir.
Elektronik Ortamlar	DLP Sistemleri ile imha edilmektedir.

Fiziksel Ortamlar	Kağıt ortamında bulunan veriler kağıt kırpma makinesi kullanılmak suretiyle yok edilmektedir.
Veri Tabanları	Database Administrator tarafından günlük şekilde kontrol gerçekleştirilmektedir.

3.4.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 alıcı grupları 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 gerekmektedir.

Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilmekte olup RASYOTEK tarafından kişisel verilerin anonim hale getirilmesinde aşağıda belirtilen yöntemler kullanılmakta ve veriler ilgili kişi ile ilişkilendirilemeyecek hale getirilmektedir.

Tablo 6: Kişisel verilerin anonim hale getirilmesi yöntemleri

İmha Yöntemleri	Uygulama
Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	• Değişkenleri Çıkartma • Kayıtları Çıkartma • Bölgesel Gizleme • Genelleştirme • Alt ve Üst Sınır Kodlama • Global Kodlama • Örnekleme

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	• Mikro Birleştirme • Veri Değiş Tokuşu • Gürültü Ekleme
Anonim Hale Getirmeyi Kuvvetlendirici İstatistiksel Yöntemler	• K-Anonimlik • L-Çeşitlilik • T-Yakınlık

V. PERİYODİK İMHA SİSTEMİ

Yönetmelik'in 5 inci maddesi uyarınca saklama ve imha politikası hazırlamış olan veri sorumlusunun, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri silme, yok etme veya anonim hale getirme işlemlerini yerine getirme yükümlülüğü bulunmaktadır.

RASYOTEK, ilgili mevzuat düzenlemelerinde öngörülen yükümlülüklere uygun olarak, yukarıda açıklanmış bulunan kişisel verilerin imhasını gerektiren ortaya çıkması halinde ilk periyodik imha sürecinde bu verileri silmekte, yok etmekte veya anonim hale getirmektedir.

Şirket nezdinde belirlenen periyodik imha süresi 6 ay olup periyodik imha işlemleri her yıl Haziran ve Aralık aylarında gerçekleştirilmektedir.

İmhası Gerçekleştirilen Kayıtlara Ait Bilgilerin Muhafazası

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili fiziksel ortamlarda bulunan verilere uygulanan tüm işlemler tutanak ile kayıt altına alınmakta, elektronik ortamdaki veriler için uygulanan işlemlere ilişkin log kaydı alınmakta ve söz konusu kayıtlar imha tarihinden itibaren en az üç yıl süreyle saklanmaktadır.

Talep üzerine imha edilen veriler için tüm talep bilgileri ve ilgili kişi ile gerçekleştirilen iletişim detayları (yazılı form ve Kanun'da bahsi geçen kimlik doğrulama bilgileri, RASYOTEK tarafından oluşturulmuş olan başvuru formu ve Kanun'da bahsi geçen kimlik doğrulama bilgileri, başvuru cevap formu, mail iletileri, ses kayıtları ve imha tarihi), kanunlara delil teşkil etmesi nedeniyle 3 yıl süre muhafaza edilmektedir.

Periyodik olarak gerçekleştirilen imha verileri, kanunlara delil teşkil etmesi nedeniyle 3 yıl süre ile muhafaza edilmektedir.

Veri imha kayıtlarına sadece Bilgi Güvenliği Ekibi ve İnsan Kaynakları Departmanı erişebilmektedir.

Basılı ortamda bir imha gerçekleşti ise,

- İmhası gerçekleştirilen evrakların veri kategorisi belirlenerek, birden fazla veri kategorisinin imhası gerçekleştirilmiş ise imha edilen kategoriler ardışık halde tutanakta belirtilir,
- Periyodik imha gerçekleştiriliyor ise evrakları ayırt etmeye yarayan bir numara imha tutanağında belirtilir,
- Talep üzerine imha gerçekleştiriliyorsa imha edilen evrakların bilgileri tutanağa işlenir (özlük numarası, fatura numarası vs.),
- Evrakın oluşma tarihi ya da bir sözleşmenin ifası ile imha gerçekleşiyor ise sözleşme tarihi (periyodik imha ise tarih aralığı) ile
- İmha tarihine kadar saklanmasını gerektiren sebepler (kanunlar/iş gerekçeleri) tutanağa yazılır.

Basılı ortam için gerçekleştirilen imhaların kayıtları işbu Politika'da belirtilen imha sürecinde görev alan kişilerce imza edilerek imha tutanakları Şirket merkezinde İnsan Kaynakları/Bilgi Güvenliği Ekibi nezdinde 3 yıl süre ile muhafaza edilmektedir.

Basılı ortamlar dışındaki ortamlarda yapılacak silme, yok etme veya anonim hale getirme işlemlerinde, oluşturulacak otomatik imha kayıtları içerisinde asgari olarak imha işleminin kim tarafından gerçekleştirildiği ve işlemin gerçekleştirilme tarihine ilişkin bilgileri yer alır. Ayrıca elektronik ortamlarda gerçekleştirilen veri imha işlemlerinde log kayıtları da tutulmakta ve Eventlog (Olay Görüntüleyicisi) tarafından 3 yıl süreyle muhafaza edilmektedir.

VI. TEKNİK VE İDARİ TEDBİRLER

Kanun'un 12 inci maddesi uyarınca veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı erişilmesini önlemek ve verilerin güvenli şekilde

muhafazasını sağlamak ile yükümlü kılınmıştır. Bununla birlikte veri sorumlusu nezdinde özel nitelikli kişisel verilerin işlenmesi durumunda Kurul tarafından belirlenmiş olan Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler'e uygun şekilde veri işleme faaliyetinin gerçekleştirilmesi gerekmektedir. Bu kapsamda RASYOTEK, alınması gereken tüm idari ve teknik tedbirleri almakta veri güvenliğinin sağlanması bakımından azami gayret ve özeni göstermektedir.

1. **Teknik Tedbirler**

RASYOTEK tarafından uygulanmakta olan teknik tedbirler aşağıdaki gibidir:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır,
- Anahtar yönetimi uygulanmaktadır,
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır,
- Çalışanlar için yetki matrisi oluşturulmuştur,
- Erişim logları düzenli olarak tutulmaktadır,
- Gerektiğinde veri maskeleme yöntemi kullanılmaktadır,
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır,
- Güncel anti-virüs sistemleri kullanılmaktadır,
- Güvenlik duvarları kullanılmaktadır,
- Kişisel veri güvenliğinin takibi yapılmaktadır,
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır,
- Mevcut risk ve tehditler belirlenmiştir,
- Saldırı tespit ve önleme sistemleri kullanılmaktadır,
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir
- Düzenli olarak Sızma Testleri Yapılmaktadır.
- 5651 nolu Kanuna göre LOG kayıtları tutulmaktadır.
- Server ve Kullanıcıları makinelerinin güncellemeleri her SALI kontrol edilir.
- VLAN yapılandırılması mevcuttur.
- Misafir ve İç network yapıları birbirlerinden izole şekilde konumlandırılmıştır.

- Database ve Sunucu sistemlerine erişim sağlayan her kişi için ekstra LOG kayıtları alınmaktadır.
- Database ve Sunucu sistemlerinin günlük Back-up alınmaktadır.

2. İdari Tedbirler

RASYOTEK tarafından uygulanmakta olan idari tedbirler aşağıdaki gibidir:

- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur,
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır,
- Gizlilik taahhütleri yapılmaktadır,
- Kişisel veriler mümkün olduğunca azaltılmaktadır,
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir,
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yapılmaktadır,
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

VII. GEÇERLİLİK VE DOKÜMAN YÖNETİMİ

Bu dokümanın sahibi İnsan Kaynakları ve RASYOTEK Bilgi Güvenliği Ekibi olup, Şirket içerisinde fiilen uygulanmakta olan mevcut yöntemlerde veya mevzuat düzenlemelerinde değişiklik olması halinde Politika üzerinde ilgili güncellemeler yapılmaktadır. Ancak her halükârda kişisel veri güvenliğinin azami düzeyde sağlanması bakımından Politika en az yılda bir kez kontrol edilmekte ve gerekli görülen düzenlemeler yapılmaktadır.

İşbu Politika'nın etkinliği ve yeterliliği değerlendirilirken, ayrıca periyodik imha sırasında yaşanan aksaklıklar ile hakkında hiçbir kayıt tutulmayan veya Kanun'a ve Politika'da belirtilen yöntemlere uygun şekilde imha edilmeyen dokümanların sayısı göz önünde bulundurulmaktadır.

VIII. YÜRÜRLÜK VE REVİZYON

İşbu Politika 10.08.2019 tarihinde yürürlüğe girmiştir. RASYOTEK'in Politika üzerinde değişiklik yapma hakkı saklı olup Politika'nın tamamının veya belirli maddelerinin yenilenmesi durumunda Politika'nın yürürlük tarihi güncellenecektir. Politika'nın revize edilmesi halinde yeni Politika örneği ilgili yerlerde ilan edilecektir.