

IRON MOUNTAIN ARŞİVLEME HİZMETLERİ A.Ş

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI**İÇİNDEKİLER**

1. GİRİŞ VE POLİTİKA’NIN HAZIRLANMA AMACI	3
2. TERİMLER	3
3. TEMEL İLKELER	5
4. SAKLAMA VE İMHAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR	6
5. SAKLAMA VE İMHA SÜRELERİ	9
6. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI USULLERİ	11
I. KAYIT ORTAMLARI	11
II. TEKNİK VE İDARİ TEDBİRLER	12
a. İdari Tedbirler:	12
b. Teknik Tedbirler	13
III. PERSONEL	13
IV. KİŞİSEL VERİLERİN İMHA USULLERİ	14
7. DİĞER HUSUSLAR	17
EK-1	18
PERSONEL UNVAN, BİRİM VE GÖREV LİSTESİ	18
EK-2	19
SAKLAMA VE İMHA SÜRELERİ TABLOSU	19
EK-3	20
GÜNCELLEME TABLOSU	20

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Doküman No : BG.PL.09
Yayın Tarihi : 30.05.2018
Revizyon No : 06
Rev. Tarihi : 21.08.2023
Sayfa : 3 / 21

1. GİRİŞ VE POLİTİKA'NIN HAZIRLANMA AMACI

İşbu Kişisel Veri Saklama ve İmha Politikası (“**Politika**”), 6698 Sayılı Kişisel Verilerin Korunması Kanunu (“**KVKK**” ya da “**Kanun**”) ve Kanun’un ikincil düzenlemesini teşkil eden 28 Ekim 2017 tarihli Resmi Gazete’de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (“**Yönetmelik**”) uyarınca yükümlülüklerimizi yerine getirmek ve veri sahiplerini kişisel verilerinizin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirmek amacıyla Iron Mountain Arşivleme Hizmetleri A.Ş. (“**Iron Mountain**” ya da “**Şirket**”) tarafından hazırlanmıştır.

2. TERİMLER

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
İlgili Kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun/KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
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 ortam.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
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 hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
Kurul	Kişisel Verileri Koruma Kurulu.
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	Kanun'da yer alan kişisel verilerin işleme 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.
Veri Sahibi/İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Yönetmelik	28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.
Kişisel Veri Envanteri	Şirket bünyesinde toplanan kişisel verilerin hangi veri sahibi gruplarına ait olduğunu süreç bazlı gösteren envanterdir.

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Şirket Politikaları	Şirketimizin bu Kişisel Verileri Saklama ve İmha Politikası ile Kişisel Verilerin Korunması ve Gizlilik Politikasıdır.
Veri Kayıt Sistemi	Kişisel verilerin Şirket bünyesinde yapılandırılarak işlenmesi için kullanılan sistemdir.

3. TEMEL İLKELER

Iron Mountain tarafından kişisel verilerin saklanması ve imhasında aşağıda yer alan temel ilkeler çerçevesinde hareket edilmektedir:

1. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinde Kanun'un 4. maddesinde sayılan ilkeler ile 12. maddesi kapsamında alınması gereken ve işbu Politikanın 6 / II. maddesinde belirtilen teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve işbu Politikaya tamamen uygun hareket edilmektedir.
2. Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Şirketimiz tarafından re'sen veya veri sahibinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir.
3. Veri sahipleri tarafından Şirketimize talep ulaşması halinde Şirketimiz tarafından;
 - Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa, Şirketimiz talebe konu kişisel verileri silmekte, yok etmekte veya anonim hale getirmektedir. Bu surette veri sahibinin talebi en geç otuz (30) gün içinde sonuçlandırılarak ve kendisine bilgi verilmektedir.
 - Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, Şirketimize yöneltilen talep, söz konusu durum hakkında gerekçeli bilgilendirme yapılarak, Kanunun 13/3. maddesi uyarınca reddedilmektedir. Böyle bir durumda ret cevabımız veri sahibine en geç otuz (30) gün içinde yazılı olarak ya da elektronik ortamda bildirilmektedir.
 - Kişisel verilerin işleme şartlarının tamamı ortadan kalkmış ve fakat veri sahibinin talebine konu olan kişisel veriler üçüncü kişilerle paylaşılmış ise, Şirketimize yöneltilen talep verilerin paylaşıldığı üçüncü kişiye bildirilmekte ve üçüncü kişi tarafından bu Politika ve mevzuat çerçevesinde gerekli işlemlerin yapılması talep edilmekte ve hatta sağlanmaktadır.
 - Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi, Kanun'un 4. maddesinde sayılan ilkeler ve 12. maddesi kapsamında alınması gereken teknik ve idari tedbirler başta olmak üzere, ilgili mevzuat hükümleri, Kurul kararları ve bu Politika ile uyumlu olarak icra edilmektedir.
4. Kanun'un 4. maddesi uyarınca; hukuka ve dürüstlük kurallarına uygunluk, doğruluk ve

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

gerektiğinde güncellik, belirlilik, açıklık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkeleri Şirketimiz için öncelik arz etmektedir.

5. Kanun'un 12. maddesine uygun olarak, Şirketimiz tarafından; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amaçlarıyla uygun güvenlik düzeyini temin etmeye yönelik bu Politika ile benimsenmiş olan teknik ve idari tedbirleri almaktadır.
6. Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler, Şirketimiz tarafından kayıt altına alınmakta ve söz konusu kayıtlar, Şirketimizin uyum göstermesi gereken diğer hukuki yükümlülükleri hariç olmak üzere, en az üç (3) yıl süreyle saklanmaktadır.
7. Kişisel Verileri Koruma Kurulu ("KVK Kurulu") tarafından aksi bir karar alınmağı müddetçe, Şirketimiz tarafından, kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı seçilmektedir. Ayrıca, veri sahibinin talebi halinde, uygun yöntem gerekçesi açıklanarak seçilecek olup, seçilen nedene olarak veri sahibine gerekli geri bilgilendirme yapılacaktır.

4. SAKLAMA VE İMHAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Veri sahiplerine ait kişisel veriler, Iron Mountain tarafından özellikle (i) ticari faaliyetlerin sürdürülebilmesi, (ii) hukuki yükümlülüklerin yerine getirilebilmesi, (iii) çalışan haklarının ve yan haklarının planlanması ve ifası ile (iv) müşteri ilişkilerinin yönetilebilmesi amacıyla yukarıda sayılan fiziki veyahut elektronik ortamlarda güvenli bir biçimde KVKK ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

Saklamayı gerektiren sebepler aşağıdaki gibidir:

- a. Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- b. Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- c. Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Iron Mountain'ın meşru menfaatleri için saklanmasının zorunlu olması,
- d. Kişisel verilerin Iron Mountain'ın herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- e. Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- f. Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

sahiplerinin açık rızasının bulunması.

- g.** Şirketimizin insan kaynakları politikalarının ve süreçlerinin planlanması ve/veya icra edilmesi,
- h.** Şirketimizin ve Şirketimizle iş ilişkisi içerisinde olan ilgili kişilerin hukuki ve teknik güvenliğinin temini faaliyetlerinin planlanması ve/veya icrası,
- i.** Şirketimiz tarafından ve/veya Şirketimiz nam ve hesabına sunulan ürün ve hizmetlerin ilgili kişilerin beğeni, kullanım alışkanlıkları ve ihtiyaçlarına göre özelleştirilerek ilgili kişilere önerilmesi ve tanıtılması için gerekli olan aktivitelerin planlanması ve/veya icrası,
- j.** Şirketimiz tarafından ve/veya Şirketimiz nam ve hesabına sunulan ürün ve/veya hizmetlerden ilgili kişileri faydalandırmak için gerekli çalışmaların yapılması ve ilgili iş süreçlerinin yürütülmesi,
- k.** Şirketimiz tarafından yürütülen ticari ve/veya operasyonel faaliyetlerin gerçekleştirilmesi için ilgili iş birimlerimiz tarafından gerekli çalışmaların yapılması ve buna bağlı iş süreçlerinin yürütülmesi,
- l.** Şirketimizin ticari ve/veya iş stratejilerinin planlanması ve/veya icrası,
- m.** Şirketimizin, ticari ortaklıklarının ve stratejilerinin doğru olarak planlanması, yürütülmesi ve yönetilmesi,
- n.** Şirketimizin kurumsal işleyişinin sağlanması, yönetim ve iletişim faaliyetlerinin planlanması ve icrası,
- o.** Şirketimizin, iş ortaklarının ve çalışanlarının hukuki, ticari ve fiziki güvenliğinin temini,
- p.** Şirketimizin ürün ve hizmetlerinden kişisel veri sahiplerinin en iyi şekilde faydalandırılması ve onların talep, ihtiyaç ve isteklerine göre özel hale getirilerek önerilmesi,
- q.** Şirketimizin hukuk işlerinin icrası/takibi,
- r.** Şirketimize talep ve şikayetlerini ileten Kişisel Veri Sahipleri ile iletişime geçmesi ve talep ve şikayet yönetiminin sağlanması,
- s.** Şirketimizin etkinlik yönetimi
- t.** Şirketimizin iş ortakları, yatırımcıları veya tedarikçileriyle olan ilişkilerinin yönetimi
- u.** Şirketimizin personel temin süreçlerinin yürütülmesi
- v.** Şirketimizin itibarının korunmasına yönelik çalışmaların gerçekleştirilmesi
- w.** Finansal raporlama ve risk yönetimi işlemlerinin icrası/takibi
- x.** Yetkili kuruluşlara mevzuattan kaynaklanan bilgilerin verilmesi.

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Kişisel verilerin işlenmesi için belirtilen şartların geçerliliği süresince kişisel veriler saklanmakta, söz konusu işleme şartları sona erdiğinde veya veri sahibinin Şirketimize başvurusu (Şirketimizin riayet etmesi gereken hukuki yükümlülükleri kontrol edildikten sonra) ve talep üzerine saklanmakta olan kişisel veriler silinmekte, imha edilmekte ve/veya anonim hale getirilmektedir. Bu kapsamda kişisel veriler:

- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması.
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- İlgili kişinin, Kanun'un 11. maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
- Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyetle bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,
- Şirket bünyesinde gerçekleştirilen periyodik imha işlemleri neticesinde,

Şirketimiz topladığı kişisel verileri silmekte, imha etmekte veya anonim hale getirmektedir.

Yukarıda belirtilen veri işlemeye (saklama) ilişkin Kanun'un 5. ve 6. maddelerinde sayılan şartlar ile Şirketimizin kişisel verileri işleme amaçları, Şirketimiz tarafından yayımlanmış olan "Iron Mountain A.Ş. Kişisel Verilerin Korunması ve Gizlilik Politikası"nda ayrıca açıklanmıştır.

5. SAKLAMA VE İMHA SÜRELERİ

Iron Mountain tarafından KVKK ve diğer ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerinizin saklama ve imha sürelerinin tespitinde aşağıda sırasıyla belirtilen ölçütlerden yararlanılmaktadır:

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

1. Mevzuatta söz konusu kişisel verinin saklanması ilişkin olarak bir süre öngörölmüş ise bu süreye riayet edilir. Anılan sürenin sona ermesi akabinde veri hakkında 2. bent kapsamında işlem yapılır.
2. Söz konusu kişisel verinin saklanması ilişkin olarak mevzuatta öngörölen sürenin sona ermesi veya ilgili mevzuatta söz konusu verinin saklanması ilişkin olarak herhangi bir süre öngörölmemiş olması durumunda sırasıyla;
 - a. Kişisel veriler, KVKK'nın 6. maddesinde yer alan tanımlama baz alınarak, kişisel veriler ve özel nitelikli kişisel veriler olarak sınıflandırmaya tabi tutulur. Özel nitelikte olduğu tespit edilen tüm kişisel veriler imha edilir. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliği ve saklanması Iron Mountain nezdindeki önem derecesine göre belirlenir.
 - b. Verinin saklanmasının KVKK'nın 4. maddesinde belirtilen ilkelere uygunluğu örneğin; verinin saklanmasında Iron Mountain'in meşru bir amacının olup olmadığı sorgulanır. Saklanmasının KVKK'nın 4. maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.
 - c. Verinin saklanmasının KVKK'nın 5. ve 6. maddelerinde öngörölmüş olan istisnalardan hangisi/hangileri kapsamında değerlendirilebileceği tespit edilir. Tespit edilen istisnalar çerçevesinde verilerin saklanması gereken makul süreler tespit edilir. Söz konusu sürelerin sona ermesi halinde veriler silinir, yok edilir ya da anonim hale getirilir.

Bu kapsamda işlenen veri kategorileri ve veri saklama süreleri aşağıda yer almaktadır.

Veri Kategorisi	Veri Saklama Süresi
1. Kimlik	İş sözleşmesi devamı süresince ve iş sözleşmesinin sona ermesinden itibaren 10 yıl
2. İletişim	İş sözleşmesi devamı süresince ve iş sözleşmesinin sona ermesinden itibaren 10 yıl
3. Özlük	İş sözleşmesi devamı süresince ve iş sözleşmesinin sona ermesinden itibaren 10 yıl
4. Hukuki İşlem	Hukuki işlemin devamı süresince ve hukuki işlemin sona ermesinden itibaren 10 yıl

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

5. Müşteri İşlem	10 yıl
6. Finans	10 yıl
7. Mesleki Deneyim	İş sözleşmesi devamı süresince ve iş sözleşmesinin sona ermesinden itibaren 10 yıl
8. Sağlık Bilgileri	İş sözleşmesi devamı süresince ve iş sözleşmesinin sona ermesinden itibaren 15 yıl
9. Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri	İş sözleşmesi devamı süresince ve iş sözleşmesinin sona ermesinden itibaren 10 yıl
10. Lokasyon	10 yıl
11. Fiziksel Mekan Güvenliği	10 yıl
12. İşlem Güvenliği	10 yıl
13. Risk Yönetimi	10 yıl
14. Görsel ve İşitsel Kayıtlar	90 gün

Iron Mountain tarafından tespit edilen ve süreç bazındaki tasniflendirme doğrultusunda hazırlanan saklama, imha ve periyodik imha sürelerine, işbu Politika'nın ekinde (Ek-2) yer alan "Saklama ve İmha Süreleri Tablosu"ndan ulaşabilirsiniz. Saklama süresi dolan kişisel veriler, işbu Politika'nın ekinde (Ek-2) yer alan imha süreleri çerçevesinde, 6 aylık periyodlarla işbu Politika'da yer verilen usullere uygun olarak imha edilir.

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

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. KİŞİSEL VERİLERİN IRON MOUNTAIN TARAFINDAN SAKLANMASI VE İMHASI USULLERİ**I. KAYIT ORTAMLARI**

Veri sahiplerine ait kişisel veriler, Iron Mountain tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

Elektronik ortamlar:

- ☐ Şirket bilgisayarları
- ☐ Muhasebe Programı
- ☐ Bordrolama Programı

Fiziksel ortamlar:

- ☐ Birim Dolapları
- ☐ ARŞİV

II. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla KVKK'nın 12. maddesindeki ilkeler çerçevesinde, Iron Mountain tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır:

a. İdari Tedbirler:

Iron Mountain idari tedbirler kapsamında;

- Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği erişmesi gerekli personel

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

ile sınırlandırır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.

- b. İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgisine ve Kurul'a bildirir.
- c. Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar.
- d. Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli kişilerle çalışır ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.
- e. Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.
- f. Şirket bünyesindeki veri işleme faaliyetlerine ilişkin tüm süreçler iş birimleri bazında analiz edilmiş olup bu kapsamda veri sahibi kategorileri ve süreç bazlı işleme esaslarına dayalı olarak "Kişisel Veri Envanteri" hazırlanmıştır. Bu envanter ile, Şirketimizin iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerimiz, kişisel verileri işleme amaçlarımız, veri kategorilerimiz, aktarılan alıcı gruplarımız, veri konusu kişi gruplarımız, veri işlemede yetkili birimlerimiz, veri işleme ortamımız, ilgili kişiler ve verilerin işlendikleri amaçlar için gerekli olan azami süreler gibi konularda tüm gerekli detaylandırmalar yapılmıştır.

b. Teknik Tedbirler:

Iron Mountain teknik tedbirler kapsamında;

- a. Kurulan sistemler kapsamında gerekli iç kontrolleri yapar.
- b. Kurulan sistemler kapsamında bilgi teknolojileri risk değerlendirmesi ve iş etki analizinin gerçekleştirilmesi süreçlerini yürütür.

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

- c. Verilerin kurum dışına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini ve ilgili matrislerin oluşturulmasını sağlar.
- d. Düzenli olarak ve ihtiyaç oluştuğunda sızma testi hizmeti olarak sistem zafiyetlerinin kontrolünü sağlar.
- e. Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlar.
- f. Kişisel verilerin yok edilmesi geri dönüştürülemeyecek ve denetim izi bırakmayacak şekilde sağlanır.
- g. Kanun'un 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli veyahut kriptografik yöntemler ile korunur.

III. PERSONEL

Kişisel veri saklama ve imha sürecinde yer alan personelin unvanlarına, birimlerine ve görev tanımlarına işbu Politika'nın **Ek-1**'nde yer alan listeden ulaşabilirsiniz.

(**Ek-1**: Personal unvan, birim ve görev listesi)

IV. KİŞİSEL VERİLERİN İMHA USULLERİ

Iron Mountain tarafından KVKK ve diğer ilgili mevzuata uygun olarak elde edilen kişisel veriler Kanun ve Yönetmelik'te sayılan kişisel veri işleme amaçlarının ortadan kalkması halinde Iron Mountain tarafından re'sen yahut İlgili Kişinin başvurusu üzerine yine Kanun ve ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen teknikler ile imha edilecektir.

a. Kişisel Verilerin Silinmesi ve Yok Edilmesi Teknikleri:

Iron Mountain tarafından kişisel verilerin silinmesi ve yok edilmesi tekniklerine ilişkin usul ve esaslar aşağıda sayılmıştır:

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Doküman No	: BG.PL.09
Yayın Tarihi	: 30.05.2018
Revizyon No	: 06
Rev. Tarihi	: 21.08.2023
Sayfa	: 14 / 21

Kişisel Verilerin Silinmesi:

Yazılımdan Güvenli Olarak Silme: Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken; İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

Bulut sisteminde ilgili verilerin silme komutu verilerek silinmesi; merkezi sunucuda bulunan dosya veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi; veya taşınabilir medyada yani flash ortamında bulunan verilerin uygun yazılımlar kullanılarak silinmesi bu kapsamda sayılabilecektir.

Ancak, kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır.

- Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması,
- Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.

Uzman Tarafından Güvenli Olarak Silme: Bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşılabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde güvenli olarak silinir.

Kağıt Ortamında Bulunan Kişisel Verilerin Karartılması: Kişisel verilerin amaca yönelik olmayan kullanımını önlemek veya silinmesi talep edilen verileri silmek için ilgili kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması veya geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi, kapatılması yöntemidir.

Kişisel Verilerin Yok Edilmesi:

De-manyetize Etme: Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir. Dikkat edilmelidir ki bu yöntemle yok etme başarılı olmaz ise ancak medyanın fiziksel olarak yok

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

edilmesi ile yok etme işlemi tamamlanmış olabilecektir.

Fiziksel Yok Etme: Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler yok edilirken kişisel verinin sonradan kullanılamayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Kağıt ve mikrofiş ortamındaki verilerin yok edilmesi de, başka bir şekilde yok edilmeleri mümkün olmadığından bu şekilde gerçekleştirilmelidir.

Üzerine Yazma: Üzerine yazma yöntemi, özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkânsızlaştıran veri yok etme yöntemidir. Yukarıda sayılan durumlar gerçekleşmesi sırasında Iron Mountain; KVKK, Yönetmelik ve ilgili diğer mevzuat hükümlerine veri güvenliğinin sağlanması amacıyla tam uyum sağlamak ve gerekli tüm idari ve teknik tedbirleri almaktadır.

b. Kişisel Verilerin Anonim Hale Getirilmesi Teknikleri:

Iron Mountain tarafından kişisel verilerin anonim hale getirilmesi tekniklerine ilişkin usul ve esaslar aşağıda sayılmıştır:

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlamayan anonim hale getirme yöntemleri, saklanmakta olan kişisel verilerde bir değişiklik veya ekleme/çıkarma yapılmaksızın; herhangi bir kişisel veri grubunun genelleme, birbiri ile yer değiştirme veya gruptan belirli bir veri veya alt veri grubunun çıkarılması ile uygulanan anonimleştirmeye yöntemleridir.

Değişken Çıkartma: Betimleyici nitelikteki verilerin çıkartılması yöntemi ile toplanılan verilerin bir araya getirilmesinden sonra oluşturulan veri setindeki değişkenlerden “yüksek dereceli betimleyici” olanlar çıkarılarak mevcut veri seti anonim hale getirilmektedir.

Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkaralar saklanan veriler anonim hale getirilmektedir. Örneğin, bir şirkette tek kıdemli müdür var ise bu kişiye ait verilerin birbirleri ile aynı kademede bulunan çalışanların kıdem, maaş ve cinsiyet verilerinin tutulduğu kayıtlardan çıkarılması ile kalan veriler anonim hale getirilebilecektir.

Bölgesel Gizleme: Bölgesel gizleme yönteminde ise tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır.

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Alt ve Üst Sınır Kodlama: Alt ve üst sınır kodlaması yöntemi ile önceden tanımlanmış kategorilerin yer aldığı bir veri grubundaki değerlerin belirli bir ölçüt belirlenerek birleştirilmesiyle anonim hale getirilmektedir.

Genelleştirme: Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örneğin; çalışanların yaşlarının tek tek göstermeksizin X yaşında Z kadar çalışan bulunduğunun ortaya konulması.

Global Kodlama: Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örneğin; doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen bölgenin belirtilmesi.

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlayan anonim hale getirme yöntemlerinde değer düzensizliği sağlamayanların aksine kişisel veri gruplarında bazı verilerin değiştirilmesi ile bozulma yaratmaktadır. Bu yöntemler kullanılırken elde edilmesi beklenen/istenen fayda doğrultusunda sapmaların dikkatli uygulanması gerekecektir. Toplam istatistiklerin bozulmaması sağlanarak veriden beklenen fayda sağlanmaya devam edilebilir.

Gürültü Ekleme: Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir. Örneğin, kilo değerlerinin olduğu bir veri grubunda (+/-) 3 kg sapması kullanılarak gerçek değerlerin görüntülenmesi engellenmiş ve veriler anonimleştirilmiş olur. Sapma her değere eşit ölçüde uygulanır.

Mikro Birleştirme: Mikro birleştirme yönteminde tüm veriler ilk olarak anlamlı bir sıraya dizilerek (büyükten küçüğe gibi) gruplara ayrılıp, grupların ortalaması alınarak elde edilen değer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleştirme sağlanmış olacaktır.

Veri Değiş Tokuşu: Veri değiş tokuşu yönteminde saklanan veriler içerisinden seçilen çiftler arasında bir değişkenin değerleri birbiri ile değiştirilir. Genel olarak kategorize edilebilen veriler için kullanılan bu yöntemde amaç veri sahiplerine ait verilerin birbirleri ile değiştirilerek veri tabanının dönüştürülmesidir.

KVKK'nın 28. maddesi uyarınca, kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi durumunda bu durum Kanun kapsamı dışında kalacak ve açık rıza temini gerekmeyecektir.

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Doküman No : BG.PL.09
Yayın Tarihi : 30.05.2018
Revizyon No : 06
Rev. Tarihi : 21.08.2023
Sayfa : 17 / 21

7. DİĞER HUSUSLAR

KVKK ve ilgili diğer mevzuat hükümleri ile işbu Politika arasında uyumsuzluk olması halinde, öncelikle KVKK ve ilgili diğer mevzuat hükümleri uygulanacaktır.

Iron Mountain tarafından hazırlanan işbu Politika ilk olarak 30.05.2018 tarihinde yürürlüğe girmiştir. Politika’da değişiklik olması durumunda, Politika’nın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir. Güncelleme tablosu Ek-3’te yer almaktadır.

Iron Mountain Arşivleme Hizmetleri A.Ş.

Ek-1: Personel Unvan, Birim ve Görev Listesi

Ek-2: Saklama ve İmha Süreleri Tablosu

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Doküman No : BG.PL.09
Yayın Tarihi : 30.05.2018
Revizyon No : 06
Rev. Tarihi : 21.08.2023
Sayfa : 18 / 21

EK-1**PERSONEL UNVAN, BİRİM VE GÖREV LİSTESİ**

PERSONEL	GÖREV	SORUMLULUK
İnsan Kaynakları Müdürü	İnsan Kaynakları Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Bilgi İşlem Müdürü	Bilgi İşlem Departmanı - Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Mali İşler Müdürü	Mali İşler Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Doküman No : BG.PL.09
Yayın Tarihi : 30.05.2018
Revizyon No : 06
Rev. Tarihi : 21.08.2023
Sayfa : 19 / 21

EK-2**SAKLAMA VE İMHA SÜRELERİ TABLOSU**

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Kurumsal İletişim Faaliyetlerinin Planlanması ve İcrası	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Genel Kurul İşlemleri	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İhale/işyeri açma/bakanlıklar-müşteşarlıklar evrak hazırlama	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel ile ilgili mahkeme/icra bilgi taleplerinin cevaplanması	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Sözleşmelerin hazırlanması	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İşe alım	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Bordrolama	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel özel sağlık ve ferdi kaza sigorta poliçelerinin hazırlanması	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışanlara araç tahsis edilmesi	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İş sağlığı ve güvenliği uygulamaları	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Active Directory	İş ilişkisinin sona ermesini müteakip	Saklama süresinin bitimini takiben 180 gün içerisinde
Log/Kayıt/Takip/Kamera Sistemleri	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Ana veri oluşturma süreçleri	İş ilişkisinin sona ermesini müteakip	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirket kredi kartı tahsisi	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Ödeme işlemleri	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
-----------------	--	---

Personel Finansman Süreçleri	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Sözleşme sürecinin bir bölümü ve sözleşmenin muhafazası	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Kaza Raporlama	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Toplantı notlarının, katılımcılar ile paylaşılması	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Doküman hazırlanması	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Eğitim kayıtlarının dosyalanması	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Acil Durum Hazırlıkları	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Doküman No : BG.PL.09
Yayın Tarihi : 30.05.2018
Revizyon No : 06
Rev. Tarihi : 21.08.2023
Sayfa : 21 / 21

EK-3**GÜNCELLEME TABLOSU**

İşbu Politika’da yapılan değişiklikler aşağıdaki tabloda yer almaktadır.

GÜNCELLEME TARİHİ	DEĞİŞİKLİK
30.05.2018	İlk yayımlanma
30.06.2019	Versiyon 2
22.06.2020	Versiyon 3
11.06.2021	Versiyon 4
03.06.2022	Versiyon 5
21.08.2023	Versiyon 6