ELOR HOLDİNG VE GRUP ŞİRKETLERİ

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

ELOR HOLDİNG VE GRUP ŞİRKETLERİ
KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI

İçindekiler

1.GİRİŞ

1.1 Amaç

Kişisel Verileri Saklama ve İmha Politikası ("Politika"), Elor Holding tarafından ("Holding") gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Holding; Stratejik Planda belirlenen misyon, vizyon ve temel ilkeler doğrultusunda; Holding çalışanlarına, çalışan adaylarına, stajyerlerine, hizmet sağlayıcılarına, tedarikçilerine, ziyaretçilerine, müşterilerine ve diğer üçüncü kişilere ait kişisel verilerin T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Holding tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

1.2 Kapsam

Holding çalışanlarına, çalışan adaylarına, stajyerlerine, hizmet sağlayıcılarına, tedarikçilerine, ziyaretçilerine, müşterilerine ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Holdingin sahip olduğu ya da Holdingçe yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3 Kısaltmalar ve Tanımlar

Alıcı Grubu	**:**	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık Rıza	**:**	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim Hale Getirme	**:**	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
Çalışan	**:**	Elor Holding personeli.
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.
Hizmet Sağlayıcı	**:**	Elor Holding ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
İlgili Kişi	**:**	Kişisel verisi işlenen gerçek kişi.

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 kişiler.
İmha	**:**	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun	**:**	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 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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
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	**:**	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.

Politika	**:**	Kişisel Verileri Saklama ve İmha Politikası
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 Sorumlusu	**:**	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.
Veri Sorumluları Sicil Bilgi Sistemi	**:**	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
VERBİS	**:**	Veri Sorumluları Sicil Bilgi Sistemi
Yönetmelik	**:**	28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2.SORUMLULUK VE GÖREV DAĞILIMLARI

Holdingin tüm birimleri ve çalışanları, sorumlu birimlerce 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 sorumlu birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1: Saklama ve imha süreçleri görev dağılımı

UNVAN	BİRİM	GÖREV
Kişisel Verileri Koruma Komitesi (Tüm Birim Yöneticileri)	Kişisel Verileri Koruma Komitesi	Çalışanların politikaya uygun hareket etmesinden sorumludur.
İnsan Kaynakları Birimi Yöneticisi	İnsan Kaynakları Birimi	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Bilgi Teknolojileri Birimi Yöneticisi	Bilgi Teknolojileri Birimi	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

Hukuk Birimi Yetkilisi, Elor Holding Tüm Birim Yöneticileri	Elor Holding'in Tüm Birimleri ve Çalışanları	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

3.KAYIT ORTAMLARI

Kişisel veriler, Holding tarafından Tablo 2'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 2: Kişisel veri saklama ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşımı) ✓ Yazılımlar (tüm holding yazılımları yazılımları, e-posta sistemleri) ✓ Bilgi güvenliği cihazları ve yazılımları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) ✓ Kişisel bilgisayarlar (Masaüstü, dizüstü) ✓ Mobil cihazlar (telefon, tablet vb.) ✓ Optik diskler (CD, DVD vb.) ✓ Çıkartılabilir bellekler (USB, Hafıza Kart vb.) ✓ Yazıcı, tarayıcı, fotokopi makinesi	✓ Kağıt ✓ Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) ✓ Yazılı, basılı, görsel ortamlar

4.SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Holding tarafından; çalışanları, çalışan adayları, stajyerleri, hizmet sağlayıcıları, tedarikçileri, ziyaretçileri ve müşterileri olarak ilişkide bulunulan üçüncü kişilerin, Holdingin veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

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

4.1 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.

Buna göre, Holdingi (holding) faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır. Süreç bazında saklama ve imha süreleri tablosunda veri envanterinde detaylı olarak belirlenmiştir.

4.1.1 Saklamayı Gerektiren Hukuki Sebepler

Holdingde, 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,
- 6102 sayılı Türk Ticaret 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,
- 213 Sayılı Vergi Usul Kanunu ve ilgili mevzuat
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4857 sayılı İş Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik, Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır. Veri saklama hukuki ve operasyonel nedenleri veri envanterinde detaylı olarak belirlenmiştir.

4.1.2 Saklamayı Gerektiren İşleme Amaçları

Holding, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

- Acil Durum Yönetimi Süreçlerinin Yürütülmesi
- Bilgi Güvenliği Süreçlerinin Yürütülmesi
- Çalışan Adayları ve Stajyer Başvuru Süreçlerinin Yürütülmesi
- Çalışanlar İçin İş Akdi ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- Çalışanlar İçin Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi
- Çalışan Memnuniyeti ve Bağlılığı Süreçlerinin Yürütülmesi
- Denetim / Etik Faaliyetlerinin Yürütülmesi
- Eğitim Faaliyetlerinin Yürütülmesi
- Erişim Yetkilerinin Yürütülmesi
- Faaliyetlerin Mevzuata Uygun Yürütülmesi
- Finans Ve Muhasebe İşlerinin Yürütülmesi

- Fiziksel Mekan Güvenliğinin Temini
- Hukuk İşlerinin Takibi ve Yürütülmesi
- İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
- İletişim Faaliyetlerinin Yürütülmesi
- İnsan Kaynakları Süreçlerinin Planlanması
- İş Faaliyetlerinin Yürütülmesi / Denetimi
- İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
- İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
- Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- Mal / Hizmet Satış Süreçlerinin Yürütülmesi
- Organizasyon ve Etkinlik Yönetimi
- Performans Değerlendirme Süreçlerinin Yürütülmesi
- Sözleşme Süreçlerinin Yürütülmesi
- Şirketimizin tabi olduğu Kanunlara Uyum Sağlanabilmesi
- Ücret Politikasının Yürütülmesi
- Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
- Yetkili Kişi, Kurum ve Kuruluşlara Bilgi Verilmesi
- Yabancı Personel Çalışma Ve Oturma İzni İşlemleri
- Yönetim Faaliyetlerinin Yürütülmesi

4.2 İmhayı Gerektiren Sebepler

Kişisel veriler;

İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,

- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Holding tarafından kabul edilmesi,
- Holdingin, 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,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

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

5.TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12 nci maddesiyle Kanunun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Holding tarafından teknik ve idari tedbirler alınır.

5.1 Teknik Tedbirler

Holding tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır
- Çalışanların domain şifreleri 6 ayda bir değiştirilmektedir. Ayrıca uygun yapılarda çok faktörlü kimlik doğrulama yapılmaktadır.
- Sızma (Penetrasyon) testleri ile Holdingimiz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler Bilgi Teknolojileri Birimi tarafından sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim, kullanıcıların yetkilendirilmesi ve kullanıcı hesap yönetimi, erişim ve yetki matrisi ile Holding bazında güvenlik politikaları aracılığı ile yapılmakta ve kontrol edilmektedir.
- Bulut ortamlarına, ilgili kullanıcıların erişim yetkilerinin tanımlanması suretiyle kullanıcı adı ve parola ile giriş yapabilmektedirler. Bu şekilde depolanan kişisel verilerin güvenliği sağlanmaktadır.

- Bilgi teknolojileri sistemleri tedarik, gelistirme ve bakımı kapsamında güvenlik önlemleri ilgili prosedürlere göre uygulanmaktadır.
- Fiziki evraklar kağıt öğütücüsü ile veya yakılarak şirket içerisinde veya dış hizmet alınarak imha edilmektedir.
- Holding bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan parmak izi erişim kontrol sistemi, yangın söndürme sistemi ve iklimlendirme sistemi) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, anti-virüs yazılımları) önlemler alınmaktadır**.**
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Firmamız ve bulut hizmeti aldığımız firmaların sorumluluğunda kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır

- USB port kullanımı Holding bünyesinde kapalıdır. Kullanım ihtiyacı doğması durumunda Sistem yöneticisi, talepte bulunan-kullanıcı için süreli kullanıma izin vermektedir. İhtiyacın sonlanması durumunda usb port ilgili kullanıcı için kapatılmaktadır
- Holding içerisinde erişim kontrol prosedürü oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır**,**
- Holding, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Holding tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır. Şifre politikasına uygun olmayan parolalar kabul edilmemektedir.
- 5651 sayılı Kanun'a uygun olarak log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır. Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Holding internet sayfasında SSL güvenlik sertifikası kullanılarak güvenli erişim sağlanmaktadır.

Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.

5.2 İdari Tedbirler

Holding tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri, İş Kanunu ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Holding tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Erişim, bilgi güvenliği, kullanım, kişisel veri saklama ve imha konularında kurumsal politikalar ve prosedürler hazırlanmış ve uygulamaya başlanmıştır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

- Kişisel veri işlemeye başlamadan önce Holding tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır**.**
- Kişisel veri işleme envanteri hazırlanmıştır.
- Holding içi periyodik ve periyodik olmayan plansız denetimler yapılmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Veri sorumlusu veri işleyenlerin veri güvenliği iç ve dış denetimlerini gerçekleştirmektedir.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.
- İmzalanan sözleşmeler kişisel verilerin korunmasına ilişkin hükümler içermektedir. Sözleşmeler kilitli dolaplarda muhafaza edilmektedir.
- Veri Sorumlulukları, Sicil Bilgi Sistemine (VERBİS) bildirim yapılmıştır.
- Kişisel verilerin korunması özelinde risk/tehdit değerlendirmesi yapılmıştır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.

<u>Özel nitelikli kişisel veriler için alınan teknik tedbirler:</u>
Alınan teknik tedbirlerin yanı sıra,

- Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmektedir.
- Gizlilik sözleşmeleri yapılmaktadır.
- Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamları ve süreleri net olarak tanımlanmaktadır.
- Periyodik olarak yetki kontrolleri gerçekleştirilmektedir.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri derhal kaldırılmaktadır.
- Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanter iade alınmaktadır.
- Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemleri (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunmaktadır.
- Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizlilik dereceli belgeler" formatında gönderilmektedir.

- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- Özel nitelikli kişisel veriler için güvenli şifreleme/ kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.

6.KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

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

6.1 Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-3'te verilen yöntemlerle silinir.

Tablo 3: 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, veritabanı 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 veriler şifreli olarak saklanmaktadır. Bu ortamlarda tutulan kişisel veriler uygun yazılımlar ile silinir ve ilgili kullanıcıların söz konusu silinen verilere erişim ve geri getirme yetkileri ortadan kaldırılır.

Bulut Ortamlarında Yer Alan Kişisel Veriler	Bulut ortamlarında yer alan kişisel verilere erişim şifreli olarak sağlanmaktadır. Bulut sistemindeki veriler sistem yöneticisi tarafından silme komutu ile silinir ve bu ortamlarda yer alan kişisel verilere ilgili kullanıcıların erişim ve geri getirme yetkileri ortadan kaldırılır.

6.2 Kişisel Verilerin Yok Edilmesi

Kişisel veriler, Holding tarafından Tablo-4'te verilen yöntemlerle yok edilir.

Tablo 4: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde veya yakılarak şirket içerisinde veya dış hizmet alınarak 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 üzerine yazma yöntemi ile yok edilmesi işlemi uygulanır ve eski verilerin geri getirilmesinin önüne geçilir.
Bulut ortamlarında yer alan kişisel veriler	Bulut ortamlarındaki kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan herbir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

7. SAKLAMA VE İMHA SÜRELERİ

Holding tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında

yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Kişisel Verileri Koruma Komitesi tarafından güncelleme yapılır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Bilgi Teknolojileri birimi tarafından yerine getirilir.

Tablo 5: Süreç bazında saklama ve imha süreleri tablosu

SÜREÇ	**SAKLAMA SÜRESİ**	**İMHA SÜRESİ**
Sözleşmelerin hazırlanması	Sözleşmenin sona ermesini takiben 10	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Holding İletişim Faaliyetlerinin İcrası	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıtları	Azami 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	Sisteme giriş tarihinden itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi ve Toplantı Katılımcılarının	Etkinliğin sona ermesini takiben 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuki İşlemler	Muhaberattan çıkış tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Finans İşlemleri	Ticari ilişkinin/faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kamera Kayıtları	4 Ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kişisel verilerin silinmesi veya yok edilmesinin kayıtları	Silinmesi veya imhasından itibaren 1. yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan adaylarına ve Referanslara ilişkin kayıtlar	Başvuru tarihinden sonra 1 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Finans İşlemleri	Ticari ilişkinin/Faaliyetin sonlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

8. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince Holding, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Holdingde her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

Kişisel Veri Saklama Ve İmha Politikasının uygulanmasından ve yönetiminden tüm birim yöneticileri sorumludur. Saklama ve İmha Sürecinde belirtilen faaliyetlerde meydana gelen ihlal olayı, güvenlik zayıflığı gibi uygun olmayan durumlarda Uygunsuzluk ve Düzeltici Faaliyet Prosedürü gereklilikleri uygulanır.

9. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, elektronik ortamda yayımlanır, internet sayfasında kamuya duyurulur ve doküman yönetim sisteminde bulundurulmaktadır.

10.POLİTİKA'NIN GÜNCELLENME PERİYODU

Politika, yılda 1 kez ve ihtiyaç duyuldukça gözden geçirilir değişiklik ihtiyacı bulunan bölümler güncellenir**.**

11.POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Holdingin ve ilgili grup şirketlerinin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları Yönetim Kurulu kararı ile iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile saklanır. Elektronik ortamdaki dokümanlar ise şifre kontrolü ile iptal etmeye yetkili kişiler tarafından iptal edilir.