KİŞİSEL VERİLERİ KAYIT, SAKLAMA VE İMHA PROSEDÜRÜ

Versiyon : 2

Düzenleme Tarihi : 01.08.2023

1. GİRİŞ

1.1. Amaç

Kişisel Verileri Kayıt, Saklama ve İmha Prosedürü ("**Prosedür**"), Iveco Araç Sanayi ve Ticaret Anonim Şirketi ("**Şirket**") tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Kişisel verilerin kaydı, saklanması ve imhasına ilişkin iş ve işlemler, Şirket tarafından bu doğrultuda hazırlanmış olan işbu Prosedüre uygun olarak gerçekleştirilir.

1.2. Kapsam

Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, tedarikçiler, müşteriler, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler, işbu Prosedür kapsamında olup; Şirket'in sahip olduğu ya da Şirketçe yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde işbu Prosedür uygulanır.

1.3 Kısaltmalar ve Tanımlar

Alıcı Grubu:	Veri sorumlusu Şirket 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:	Şirket 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:	Şirket 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:	Kanun'da 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.
Prosedür:	İşbu Kişisel Verileri Kayıt, Saklama ve İmha Prosedürü.
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 Şirket'i.
Veri Sorumluları Sicil Bilgi Sistemi:	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kişisel Verileri Koruma Kurumu tarafından oluşturulan ve yönetilen bilişim sistemi.
VERBİS:	Veri Sorumluları Sicil Bilgi Sistemi.
Yönetmelik:	28.10.2017 tarihli Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Şirket'in tüm birimleri ve çalışanları, sorumlu birimlerce Prosedür 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.

Tablo 1: Sorumlu personel ve görev dağımı

GÖREVLİ	SORUMLULUK
KVK Komitesi sorumlusu	Her bir departmanın iş süreçlerinin saklama ve periyodik imha sürelerine uygun gerçekleşip gerçekleşmediğinin gözetimi
İrtibat Kişisi	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
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 Teknolojileri 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
Finans ve Finansal Servisler 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
Kanal Yönetimi 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
Lojistik ve Ticari Lojistik 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
Parça ve Servisler 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
Pazarlama 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
Satış 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
Kurumsal İlişkiler ve Ürün Yönetimi Departmanı 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
Iveco Otobüs Departmanı 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

3. KAYIT ORTAMLARI

Kişisel veriler, Şirket 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 paylaşım, vb.) ▪ Yazılımlar (ofis yazılımları ve Şirketçe kullanılan diğer yazılımlar) ▪ Bilgi güvenliği cihazları (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, başvuru formları vb.) ▪ Yazılı, basılı, görsel ortamlar

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; çalışanlar, çalışan adayları, ziyaretçiler, tedarikçiler, müşteriler, hizmet sağlayıcıları, diğer üçüncü kişiler, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanun'a uygun olarak saklanır ve imha edilir. Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

4.1. Saklamaya İlişkin Açıklamalar

Kanun'un 3. maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4. 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. maddelerinde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, Şirket faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarına uygun süre kadar saklanır.

4.1.1. Kişisel Sağlık Verileri

Şirket tarafından toplanan ve saklanan çalışanlara ilişkin sağlık verileri, yalnızca Şirket bünyesinde görev alan işyeri hekimi tarafından işlenebilecek ve işyeri hekimine ait özel odada ve kilitli dolaplarda saklanabilecektir.

Zorunlu hallerde, söz konusu sağlık verilerinin bulunduğu dolaba erişim, yalnızca İrtibat Kişisi tarafından sağlanabilecek, başkaca hiçbir çalışan veya yetkilinin söz konusu verilere erişimi söz konusu olmayacak ve verilerin kullanılması ile ilgili yapılması gereken işin sona ermesi ile birlikte, söz konusu veriler aynı yere kaldırılacak ve aynı şekilde kilitli olarak muhafaza edilecektir.

4.1.2. Diğer Özel Nitelikli Kişisel Veriler

Gerek Şirket çalışanları gerekse 3. Kişilere ait olan özel nitelikli kişisel veriler, işlenme sebebine bakılmaksızın, yalnızca İrtibat Kişisinin erişebileceği ve sadece bu verilerin yer aldığı belge, kayıt vb. ortamları saklamak üzere özel olarak ayrılmış kilitli dolaplarda muhafaza edilecektir.

4.1.3. Saklamayı Gerektiren Hukuki Sebepler

Şirket'in faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar Şirket nezdinde muhafaza edilir.

Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 213 sayılı Vergi Usul Kanunu ve ilgili diğer vergi mevzuatı,
- 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,
- 4857 sayılı İş Kanunu,
- 6102 sayılı Türk Ticaret 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.

4.1.4. Saklamayı Gerektiren İşleme Amaçları

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

- İnsan kaynakları süreçlerini yürütmek,
- İş sağlığı ve güvenliği süreçlerini yürütmek,
- Bilgi teknolojileri süreçlerini yürütmek,
- Sistem erişimini ve güvenliğini sağlamak,
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve edimleri ifa edebilmek,
- Müşteri raporlamalarını yapabilmek,
- Satış ve pazarlama süreçlerini yerine getirmek,
- Kurumsal iletişim faaliyetlerini yerine getirmek,
- Müşteri ilişkileri ve memnuniyeti süreçlerini yürütmek,
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak,
- Şirket ile iş ilişkisinde bulunan gerçek/tüzel kişilerle irtibat sağlamak,
- Yasal raporlamalar yapmak,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü yerine getirmek,
- Mevzuatın öngördüğü zorunlu saklama sürelerine uymak.

4.2. İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması ya da mevzuatın gerekli kıldığı sürenin sona ermesi,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanun'un 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- Şirket'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 cevap vermemesi hallerinde; Kurul'a 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, Şirket tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

4.3. İmhanın Tutanak Altına Alınması

Her bir imha sürecinin sonunda ilgili imha işlemi, bir tutanak ile imha sürecini gerçekleştiren departman sorumlusu ve İrtibat Kişisi tarafından kayıt altına alınır. Söz konusu tutanak 5 yıl süreyle Şirket bünyesinde saklanır.

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 Kanun'un 12. maddesiyle 6. maddesinin dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde ve Şirket tarafından ihdas edilen Özel Nitelikli Kişisel Veri İşleme Prosedürü kapsamında, tarafından teknik ve idari tedbirler alınır.

5.1. Teknik Tedbirler

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

- Sızma (Penetrasyon) testleri ile Şirket 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 sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Şirket'in 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 erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) 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.
- Şirket içerisinde erişim prosedürleri 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.
- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.

- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Şirket internet sayfasına erişimde güvenli protokol (https) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı bir prosedür belirlenmiştir.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yaptırılmakta ve test sonuçları kayıt altına alınmaktadır.
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

5.2 İdari Tedbirler

Şirket 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 ve ilgili diğer mevzuat hakkında belli aralıklarla eğitimler verilmektedir.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Şirket tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik ve kişisel verilerin korunması taahhütnameleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanmak üzere gerekli hükümler Disiplin Yönetmeliğine eklenmiştir.
- Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kişisel verilerin işlenmesine ilişkin genel politika ve bu konuya ilişkin prosedürler hazırlanarak yayımlanmıştır.
- Şirket içi periyodik ve rastgele denetimler yapılmaktadır.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı bir prosedür belirlenmiştir.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Şirket 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 Şirket tarafından 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 süresi 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 süresi 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 süresi sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir, arşivde kilitli dolaplarda saklanır ve bu dolapların kilitleri yalnızca evrak arşivinden sorumlu birim yöneticisinde bulunur.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süresi sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.2. Kişisel Verilerin Yok Edilmesi

Kişisel veriler, Şirket 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 süresi sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik/Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süresi sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak

	yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

6.3. 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 getirilmesi bakımından, Iveco global şirket rehberlerinin hükümleri tatbik olacaktır.

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

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

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri işleme süreçleri bazında saklama süreleri Kişisel Veri İşleme Envanterinde,
- Veri kategorileri bazında saklama süreleri VERBİS kaydında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Şirket tarafından güncellemeler yapılır. Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi işbu Prosedür'ün 2. maddesinde belirtilen sorumlular tarafından yerine getirilir.

8. PERİYODİK İMHA SÜRESİ

Yönetmelik'in 11. maddesi gereğince Şirket, periyodik imha süresini altı (6) ay olarak belirlemiştir. Buna göre, Şirket nezdinde her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

9. PROSEDÜR'ÜN YAYINLANMASI VE SAKLANMASI

Prosedür, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da Şirket nezdinde dosyasında saklanır.

10. PROSEDÜR'ÜN GÜNCELLENME PERİYODU

Prosedür, mevzuat değişikliklerinde ve ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

11. PROSEDÜR'ÜN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Prosedür, 01.08.2023 tarihi itibariyle yürürlüğe girmiştir.

Yürürlükten kaldırılmasına karar verilmesi halinde, Prosedür'ün ıslak imzalı eski nüshaları Şirket yetkili organlarınca iptal edilir ve en az beş (5) yıl süre ile Şirketçe dosyasında saklanır.