

IVECO ARAÇ SANAYİ VE TİCARET ANONİM ŞİRKETİ

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Doküman Adı	Kişisel Veri Saklama ve İmha Politikası
Doküman Kodu	[●]
Veri Sorumlusu	Iveco Araç Sanayi ve Ticaret Anonim Şirketi
Sürüm	v1.0 Taslak inceleme nüshası 5 Ekim 2026
Tarih	[●] / [●] / 2026
Onaylayan	[●]

1. GİRİŞ

1.1. Amaç

İşbu Kişisel Veri Saklama ve İmha Politikası ("Politika"), Iveco Araç Sanayi ve Ticaret Anonim Şirketi ("Şirket") tarafından gerçekleştirilen saklama ve imha faaliyetlerine ilişkin usul ve esasları belirlemek amacıyla, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in ("Yönetmelik") 5. ve 6. maddeleri uyarınca Kişisel Veri İşleme Envanteri ("Envanter") ile uyumlu olarak hazırlanmıştır.

Şirket, kişisel verilerin işlendikleri amaç için gerekli olan süreden daha uzun süre saklanmamasını ve saklamayı gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin hukuka uygun olarak imha edilmesini esas alır. Kişisel verilerin saklanmasına ve imhasına ilişkin iş ve işlemler İşbu Politikaya uygun olarak gerçekleştirilir.

Uygulama adımları Politika'nın 13. bölümünde düzenlenmiştir.

1.2. Kapsam

Çalışanlar, çalışan adayları, stajyerler, eski çalışanlar, müşteriler, potansiyel müşteriler, bayi ve yetkili servis yetkilileri ile çalışanları, tedarikçi ve hizmet sağlayıcı yetkilileri ile çalışanları, ziyaretçiler, hissedarlar ve diğer üçüncü kişilere ait kişisel veriler İşbu Politika kapsamındadır.

Politika, Şirket'in sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamlarında ve kişisel veri işlenmesine yönelik tüm faaliyetlerde uygulanır. Kişisel verilerin Şirket adına üçüncü kişilerce işlendiği hallerde, İşbu Politikada öngörülen saklama süreleri ve imha esasları veri işleyenler nezdinde de uygulanır.

1.3. Kısaltmalar ve Tanımlar

Tablo 1: Kısaltmalar ve tanımlar

Terim	Tanım
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Alıcı Grubu	Şirket tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
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.

Terim	Tanım
Elektronik Olmayan Ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
Envanter	Şirket'in iş süreçlerine bağlı olarak gerçekleştirdiği kişisel veri işleme faaliyetlerini işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve ilgili kişi grubuyla ilişkilendirerek oluşturduğu ve azami muhafaza sürelerini, yurt dışına aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin tedbirleri detaylandırdığı kişisel veri işleme envanteri.
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, Şirket organizasyonu içerisinde veya Şirket'ten aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
İmha Koordinatörü	İmha dönemini başlatan, onaylı kapsamı ilgili birimlere ileten, sonuçları takip eden ve dönem sonucunu KVK Komitesine sunan görevli.
İrtibat Kişisi	Şirket'in Kanun ve ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak Kurum ile iletişimi sağlamak üzere Sicile kayıt esnasında bildirilen gerçek kişi.
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.
KVK Komitesi	Şirket bünyesinde kişisel verilerin korunması uyum programının yönetiminden sorumlu komite.
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	Kanun'da yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda, işbu Politikada belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Politika	İşbu Kişisel Veri Saklama ve İmha Politikası.
Sicil	Kurum tarafından tutulan Veri Sorumluları Sicili.
Uygulama adımları	İşbu Politika'nın 13. bölümündeki görev dağılımı, işlem ve takip adımları.
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi.
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 kurulmasından ve yönetilmesinden sorumlu Şirket.
Yönetmelik	28.10.2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

İşbu Politikada yer almayan tanımlar bakımından Kanun ve ilgili mevzuatta yer alan tanımlar geçerlidir.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Şirket'in tüm birimleri ve çalışanları, işbu Politikada öngörülen teknik ve idari tedbirlerin gereği gibi uygulanması, çalışanların eğitimi ve farkındalığının artırılması, kişisel verilerin hukuka aykırı olarak işlenmesinin ve kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak saklanması sağlanması amacıyla sorumlu birimlere aktif olarak destek verir.

Her birim kendi kayıtlarının saklanması ve imhasından sorumludur. İmha koordinasyonunu bu görevi yürüten çalışan veya onun yerine görevlendirilen kişi sağlar. Aşağıdaki işlevsel görevler mevcut organizasyon içinde yürütülür. Aynı kişi birden fazla görevi üstlenebilir. Görevli değişiklikleri mevcut görevlendirme kayıtlarında izlenir. Koordinasyon görevi, teknik silme yetkisi vermez.

Tablo 2: Saklama ve imha süreçlerinde görev alanlar

Görev / unvan	Birim / görev kapsamı	Görev Tanımı
KVK Komitesi üyesi	KVK Komitesi	Politikanın uygulanmasının ve güncellenmesinin gözetiminden, dönem sonuçlarının ve çözilemeyen istisnaların değerlendirilmesinden sorumludur.
İmha Koordinatörü	Şirket genelinde imha koordinasyonu	Dönemin başlatılmasından, onaylı kapsamın iletilmesinden ve sonuçların EK-2 üzerinden takibinden sorumludur. Teknik imha işlemleri yetkili birimlerin sorumluluğundadır.
Birim yöneticisi	Kişisel veri işleyen tüm birimler	Kendi biriminin kayıt kapsamının ve saklama istisnalarının onaylanmasından, sonuçların gözden geçirilmesinden sorumludur. İnsan Kaynakları, ticari ve destek birimleri bu görevi kendi kayıtları için yürütür.
Yetkili BT sorumlusu	Bilgi Teknolojileri	Yetkisi içindeki sistem ve yedek işlemlerinin yürütülmesinden, yetkisi dışındaki işlemlerin global ekip veya hizmet sağlayıcıdan talep edilmesinden ve sonucun kaydından sorumludur.
Arşiv sorumlusu	Fiziki arşivi yöneten birim	Onaylı kapsam içindeki fiziki kayıtların ayrılmasından, imhanın uygulanmasından veya dış arşiv hizmetinden işlem belgesinin temininden sorumludur.
Hukuk sorumlusu veya hukuk danışmanı	Hukuk işlevini yürüten birim veya danışmanlık	Saklama süreleri, devam eden hukuki süreçler ve hizmet sağlayıcıların rolleri hakkındaki hukuki tereddütlerin değerlendirilmesinden sorumludur.

3. KAYIT ORTAMLARI

Aşağıdaki tabloda kayıt ortamları örnek olarak gösterilmiştir. Politika, tabloda sayılanlarla sınırlı olmaksızın kişisel verilerin işlendiği tüm kayıt ortamlarına uygulanır. Süreç bazındaki kayıt ortamlarının ayrıntıları Envanterde yer alır.

Tablo 3: Kişisel verilerin saklandığı kayıt ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Sunucular (etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.) Yazılım ve uygulamalar (ofis yazılımları, ERP, CRM, bayi ve servis yönetim sistemleri ile Şirketçe kullanılan diğer yazılımlar) Bulut sistemleri (Şirketçe ve grup şirketlerince kullanılan bulut tabanlı uygulama ve depolama hizmetleri) Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme sistemleri, günlük kayıt dosyaları, antivirüs vb.) Kişisel bilgisayarlar (masaüstü, dizüstü) Mobil cihazlar (telefon, tablet vb.) Optik diskler (CD, DVD vb.) Çıkarılabilir bellekler (USB, hafıza kartı vb.) Yazıcı, tarayıcı, fotokopi makinesi Kamera kayıt sistemleri	Kağıt ortamı Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) Birim arşivleri ve genel arşiv ile dış hizmet sağlayıcı nezdinde tutulan fiziki arşiv Yazılı, basılı ve görsel ortamlar

4. SAKLAMAYA VE İMHAYA İLİŞKİN AÇIKLAMALAR

4.1. Saklamayı Gerektiren Hukuki Sebepler

Kanun'un 4. maddesi uyarınca kişisel veriler, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilir. Bir kişisel verinin saklanması için mevzuatta özel bir süre öngörülmüşse bu süreye uyulur. Mevzuatta bir süre öngörülmemişse kişisel veri, işleme amacının gerektirdiği süre boyunca saklanır ve bu sürenin sonunda işbu Politikaya uygun olarak imha edilir.

Aşağıdaki mevzuat listesi örnek niteliğindedir ve sınırlayıcı değildir. Faaliyet bazındaki hukuki sebepler ve saklama gereklilikleri Envanterde yer alır. Başlıca düzenlemeler şunlardır:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 6102 sayılı Türk Ticaret Kanunu
- 6098 sayılı Türk Borçlar Kanunu
- 213 sayılı Vergi Usul Kanunu ve ilgili diğer vergi mevzuatı
- 4857 sayılı İş Kanunu
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu ve İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik
- 6502 sayılı Tüketicinin Korunması Hakkında Kanun ve Satış Sonrası Hizmetler Yönetmeliği
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ve Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik
- 4458 sayılı Gümrük Kanunu ve Gümrük Yönetmeliği
- 3308 sayılı Mesleki Eğitim Kanunu
- Yukarıda sayılan düzenlemeler uyarınca yürürlükte olan diğer ikincil mevzuat

4.2. Saklamayı Gerektiren İşleme Amaçları

Aşağıdaki işleme amaçları örnek niteliğindedir ve sınırlayıcı değildir. Faaliyet bazındaki amaçlar ve ilgili kayıtlarla bağlantıları Envanterde yer alır:

- İnsan kaynakları ve istihdam süreçlerinin yürütülmesi
- İş sağlığı ve güvenliği süreçlerinin yürütülmesi
- Ticari araç satışı, satış sonrası hizmetler, servis, garanti ve yedek parça süreçlerinin yürütülmesi
- Bayi ve yetkili servis kanal yönetimi süreçlerinin yürütülmesi
- Satış, pazarlama ve müşteri ilişkileri süreçlerinin yürütülmesi
- Sözleşmelerin kurulması ve ifasına yönelik iş ve edimlerin yerine getirilmesi
- Finans, muhasebe ve ödeme süreçlerinin yürütülmesi
- Satın alma, tedarik, lojistik ve sevkiyat süreçlerinin yürütülmesi
- Bilgi teknolojileri, sistem erişimi ve bilgi güvenliği süreçlerinin yürütülmesi
- Şirket yerleşkelerinin ve tesislerinin fiziksel güvenliğinin sağlanması
- Yasal düzenlemelerin gerektirdiği hukuki yükümlülüklerin yerine getirilmesi ve yasal raporlamaların yapılması
- İleride doğabilecek hukuki uyumsuzluklarda delil olarak ispat yükümlülüğünün yerine getirilmesi

4.3. İmhayı Gerektiren Sebepler

Kanun ve ilgili diğer mevzuat hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler, Kanun'un 7. maddesi uyarınca resen veya ilgili kişinin talebi üzerine Şirket tarafından silinir, yok edilir veya anonim hale getirilir. Bu kapsamda kişisel verilerin imhası aşağıdaki hallerde gerekir:

- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya yürürlükten kaldırılması
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması
- Kişisel verilerin işlenmesinin dayandığı hukuki sebeplerin tamamının ortadan kalkması
- Kişisel verilerin Kanun'un 5. ve 6. maddelerindeki şartlara dayalı olarak işlenmiş olmasına rağmen, işleme faaliyetinin Kanun'un 4. maddesindeki genel ilkelere aykırılık teşkil etmesi
- Kişisel verilerin yalnızca açık rıza şartına istinaden işlendiği hallerde ilgili kişinin açık rızasını geri alması ve başkaca bir hukuki sebebin bulunmaması
- İlgili kişinin Kanun'un 11. maddesindeki hakları çerçevesinde yaptığı silme veya yok etme başvurusunun Şirket tarafından kabul edilmesi
- Şirket'in ilgili kişinin başvurusunu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde Kurula yapılan şikayetin Kurul tarafından uygun bulunması
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılabilecek herhangi bir şartın mevcut olmaması

5. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin saklanması ve imhasında Kanun'un 12. maddesi ile özel nitelikli kişisel verilere ilişkin yeterli önlemler esas alınır. BT ve ilgili birimler, aşağıdaki tedbirlerin görev alanları ölçüsünde uygulanmasından ve mevcut teknik ve idari kayıtlarla izlenmesinden sorumludur. Tespit edilen eksiklikler, sorumlusu ve hedef tarihi belirtilerek mevcut aksiyon takibine alınır.

5.1. Teknik Tedbirler

- Ağ ve uygulama güvenliği için güvenlik duvarı ile uygun saldırı tespit ve önleme kontrolleri uygulanır.
- Sistemlerin risk ve zafiyetleri uygun güvenlik testleriyle değerlendirilir, bulgular sorumlu ve giderim tarihiyle takip edilir.
- BT birimi, erişim yetkilerinin görev ve ihtiyaçla sınırlandırılmasından ve yetki listelerinin düzenli olarak gözden geçirilmesinden sorumludur.
- Güçlü parola kuralları ve uygun sistemlerde güvenli işlem kayıtları uygulanır.
- Erişimler ve yetkisiz erişim denemeleri için gerekli kayıt ve izleme kontrolleri kurulur.
- Zararlı yazılım koruması ve güvenlik yamaları güncel tutulur.
- Gerekli yedeklerin güvenliği sağlanır. Yedekleme yetkisi, saklama döngüsü ve geri yükleme işlemleri sınırlandırılır.
- Silme sonucunda ilgili kullanıcıların kayda erişmesi ve kaydı tekrar kullanması önlenir.
- Fiziki kayıtlar yetkisiz erişime ve yangın veya su baskını gibi risklere karşı korunur.
- Özel nitelikli veriler için şifreleme, anahtar güvenliği, işlem kaydı, güncelleme ve güvenlik testi tedbirleri uygulanır. Somut uygulama ilgili prosedür ve sistem kayıtlarıyla izlenir.
- Özel nitelikli veriler e-postayla aktarılacaksa şifreli kurumsal e-posta veya KEP kullanılır. Sunucular arası aktarımda VPN veya SFTP gibi güvenli yöntemler, fiziki aktarımda yetkisiz erişimi önleyen gizlilik tedbirleri uygulanır.

5.2. İdari Tedbirler

- Çalışanlara görevlerine uygun kişisel veri koruma ve güvenlik eğitimleri verilir. Eğitim ihtiyacı ve katılım kayıtları izlenir.
- Çalışanların gizlilik yükümlülükleri yazılı olarak düzenlenir ve görev sona erdikten sonra da korunur.
- İlgili birimler, kendi faaliyetlerine ilişkin Envanter bilgilerinin doğruluğundan ve güncelliğinden sorumludur.
- Kişisel veri işleme sırasında uygulanabilir aydınlatma yükümlülüğü yerine getirilir.
- Hizmet ilişkilerinde veri güvenliği, yetkiler, hizmet sonunda iade veya imha ve sonuç teyidi tarafların gerçek rollerine göre düzenlenir.
- Görev değişikliği veya ayrılık halinde erişim yetkileri ihtiyaca göre güncellenir veya kaldırılır. Hesap kapatma kayıt imhası yerine geçmez.
- Risk değerlendirmesi ve uygun iç kontroller planlanır. Eksikler, sorumlu ve takip tarihiyle mevcut aksiyon düzeninde izlenir.
- Dış fiziki arşiv hizmetinde yetkiler ve güvenlik yükümlülükleri yazılı düzenlenir. Kayıt çıkarma ve imha işlemleri doğrulanabilir şekilde belgelenir.
- Güvenlik kurallarına aykırılıkların ele alınacağı disiplin ve bildirim düzeni oluşturulur.
- Veri ihlalinin değerlendirilmesi, gerekli bildirimlerin yapılması ve olayın belgelenmesi için sorumlular ve işleyiş belirlenir.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Şirket tarafından resen veya ilgili kişinin başvurusu üzerine Yönetmelik'in 7 ila 12. maddelerine uygun olarak silinir, yok edilir veya anonim hale getirilir. Kurul tarafından aksine bir karar alınmadıkça imha yönteminin seçimi Şirket'e aittir. Şirket, yöntemi belirlerken kişisel verinin niteliğini, bulunduğu kayıt ortamını, verinin diğer kayıtlarla ilişkisini ve teknik imkanları dikkate alır. Şirket, resen gerçekleştirdiği imhada uygun yöntemi kendisi seçer. İlgili kişinin talebi üzerine gerçekleştirilen imhada ise yöntem, gerekçesi açıklanmak suretiyle seçilir.

Kişisel verilerin yurt dışındaki sunucularda veya grup şirketleri bünyesindeki sistemlerde bulunduğu hallerde, saklama süresinin sona ermesi üzerine imha işlemi bu sistemler bakımından da yürütülür. Verilerin Şirket adına veri işleyen sıfatıyla işlendiği hallerde ilgili veri işleyene imha talimatı verilir ve imhanın belgelendirilmesi temin edilir. Verilerin ayrı bir veri sorumlusuna aktarılmış olduğu hallerde ise durum ilgili veri sorumlusuna bildirilir ve nezdinde gerekli işlemlerin yapılması temin edilir.

6.1. Kişisel Verilerin Silinmesi

Silme, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir. Kişisel veriler aşağıdaki tabloda gösterilen yöntemlerle silinir.

Tablo 4: Kişisel verilerin silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda yer alan kişisel veriler	Saklanmasını gerektiren süresi sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik ortamda yer alan kişisel veriler	Saklanmasını gerektiren süresi sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel ortamda yer alan kişisel veriler	Saklanmasını gerektiren süresi sona erenler, evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca üzeri okunamayacak şekilde çizilerek, boyanarak veya silinerek karartma işlemi uygulanır.
Taşınabilir medyada bulunan kişisel veriler	Taşınabilir medyada bulunan kişisel veriler şifreli olarak saklanır, saklama süresi sona erenler ise ortama uygun silme yazılımı kullanılarak silinir.

Veri Kayıt Ortamı	Açıklama
Yedekleme ortamlarında yer alan kişisel veriler	Bilgi Teknolojileri, ilgili yedeğin saklama döngüsünü ve imha tarihini, erişim ve geri yükleme yetkilerini kayıt altına alır. Aktif sistemden silinen kayıtların yedeklerden olağan kullanım için geri alınması engellenir. Yedeklerin belirlenen süre sonunda imhası takip edilir. Geri yükleme gerekiyorsa imha kapsamındaki kayıtlar yeniden kullanıma açılmadan silme işlemi tekrarlanır. Teknik engeller sorumlusu ve çözüm tarihiyle açık iş olarak izlenir. Yedekleme süresiz saklama gerekçesi değildir.
Bulut sisteminde yer alan kişisel veriler	Yetkili sistem birimi, ilgili kullanıcıların erişim ve geri alma imkanlarını kapatacak silme işlemini uygular veya hizmet sağlayıcıdan talep eder. Sürüm, arşiv ve yedek kopyaları ayrı değerlendirilir. Şifreleme anahtarlarının imhası ancak kayıt kapsamına özgü, teknik olarak uygun ve sonucu doğrulanabilir ise seçilir. Bütün bulut kayıtları için varsayılan yöntem değildir.

6.2. Kişisel Verilerin Yok Edilmesi

Yok etme, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesidir. Kişisel veriler aşağıdaki tabloda gösterilen yöntemlerle yok edilir.

Tablo 5: Kişisel verilerin yok edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel ortamda yer alan kişisel veriler	Kağıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süresi sona erenler, kağıt kırma makinelerinde geri döndürülemeyecek şekilde yok edilir. Toplu imha işlemlerinin dış hizmet sağlayıcı aracılığıyla yapılması halinde, hizmet sağlayıcı ile Kanun'un 12. maddesi kapsamında yazılı sözleşme akdedilir ve imha belgesi temin edilir.
Optik ve manyetik medyada yer alan kişisel veriler	Saklanmasını gerektiren süresi sona erenlere eritme, yakma veya toz haline getirme gibi fiziksel yok etme işlemi uygulanır. Manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılmak suretiyle üzerindeki veriler okunamaz hale getirilir. Yeniden yazılabilir ortamlarda üzerine yazma yöntemi uygulanabilir.
Kullanım ömrü sona eren cihazlar	Bilgi Teknolojileri, cihazdaki gerekli kayıtların yetkili ortama alınmasını ve saklama gereği kalmayan kayıtların uygun yöntemle temizlenmesini sağlar. Cihazın imhası gerekiyorsa yetkili hizmet sağlayıcıya kapsamı kayıt altına alınarak teslim edilir ve sonucu gösteren belge alınır. Teslim, tamamlanmış imha sayılmaz.

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. Anonim hale getirmenin gerçekleşmiş sayılabilmesi için verilerin, Şirket veya üçüncü kişiler tarafından geri döndürme ve 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.

Anonim hale getirmede uygulanacak tekniklerin belirlenmesinde Kurum tarafından yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi esas alınır.

Şirket'in dahil olduğu grup bünyesindeki rehber ve kılavuzlar, Kanun, Yönetmelik ve Kurul kararlarına aykırı olmadığı ölçüde tamamlayıcı nitelikte uygulanabilir.

6.4. İmha İşlemlerinin Kayıt Altına Alınması

İşlem kapsamı, uygulayan kişi veya birim, tarih, yöntem ve sonucu gösteren doğrulanabilir kayıtlar saklanır. Mevcut sistem kaydı, iş emri veya hizmet sağlayıcı teyidi kullanılabilir. Aynı işlem için mükerrer tutanak düzenlenmez. Çalışan ve teknik işlem kayıtları Politika'nın 13. bölümündeki görev dağılımına göre gözden geçirilir. Komite dönem sonucunu değerlendirir. Her işlem için ayrıca komite imzası aranmaz. İmha kayıtları, diğer hukuki yükümlülükler saklı kalmak üzere işlem tarihinden itibaren 5 yıl saklanır.

Aynı kayıta birden fazla kişiye ait bilgi varsa işlem kapsam dahilindeki bölümle sınırlı tutulur. Kullanılan maskeleye veya karartma yönteminin silme şartlarını sağladığı doğrulanır. Geri döndürülebilir maskeleye anonim hale getirme sayılmaz.

7. SAKLAMA VE İMHA SÜRELERİ

Aşağıdaki tablo temel kayıt gruplarının saklama sürelerini ve imha zamanını gösterir. Faaliyet ve veri bazındaki ayrıntılar Envanterde yer alır. Politika ve Envanter birlikte uygulanır. Aralarında farklılık bulunursa ilgili birim ve Hukuk uygulanacak kuralı netleştirir.

Bir ilişkinin sürmesi bütün kayıtların saklanması gerektirmez. Saklama süresi her kayıt türü için kendi başlangıcından hesaplanır. Güncelliğini yitiren irtibat ve çalışma kopyaları ticari belge veya hak ispatı sürelerine topluca dahil edilmez. E-posta ve dosyalar içerdiği kayıt türüne göre değerlendirilir. Ayrılan çalışanın hesabı kapatılır, gerekli iş kayıtları yetkili arşive ayrılır.

Aynı kayıt için birden fazla geçerli saklama nedeni varsa yalnız gerekli kapsam bakımından en son dolan süre uygulanır. Kanuni asgari süreler kısaltılamaz. Kanunda özel süresi bulunmayan kayıtlar için tabloda belirlenen süreler, işleme amacı ve hak ispatı ihtiyacına dayanır. Devam eden hukuki süreçlerde yalnız gerekli kayıtlar korunur. Zamanaşımının başlangıcı, durması ve kesilmesi Hukuk tarafından değerlendirilir.

İspat arşivinde yalnız gerekli kayıtlar tutulur. Başvuru ekleri, özlük ve staj dosyalarındaki gereksiz çalışma kopyaları ihtiyaç sona erince ayıklanır. Rıza kanıtı metin sürümü, kapsam, kişi, tarih ve geri alma bilgisiyle sınırlıdır. Araç kullanım ömrü bütün müşteri ve sürücü verilerine uygulanmaz. Belirsiz süre Hukuk ile netleştirilir, belirsizlik süresiz saklama gerekçesi değildir.

Tablo 6: Saklama süreleri ve imha zamanı

Kayıt grubu	Saklama süresi ve başlangıcı	İmha zamanı
Ticari defter, belge ve yazışmalar. Vergi kayıtları	Ticari kayıtlar, TTK m. 82'deki ilgili olayın gerçekleştiği takvim yılının bitiminden itibaren 10 yıl. Yalnız VUK kapsamındaki kayıtlar, ilgili yılı izleyen takvim yılı başından itibaren 5 yıl. İki kapsama giren kayıta 10 yıl.	İlk dönem*
Sözleşmesel hakların ispatı için gerekli kayıtlar	İlgili alacağın muacceliyetinden başlayan uygulanabilir zamanaşımı boyunca. Genel süre 10 yıl, özel süreler saklıdır.	İlk dönem*
Pay sahipliği, karar ve temsil kayıtları	Hukuki etkileri sürdüğü. Ticari defter ve belge niteliğindeki kayıtlar ayrıca ticari kayıtlar kuralına tabidir.	İlk dönem*
Çalışan, bordro, ücret, SGK, ücrete esas PDKS ve staj kayıtları	SGK, ücret, bordro, PDKS ve staj ödeme belgeleri ilgili yılı takip eden yılbaşından itibaren 10 yıl. İzin ve fesih alacaklarına ilişkin kayıtlar alacağın doğduğu veya muaccel olduğu tarihten itibaren 5 yıl. İş sözleşmesi ve diğer özlük kayıtları hizmet ilişkisi boyunca, sonrasında yalnız gerekli hak ispatı süresince. Staj sözleşmesi ve tamamlama belgesi stajın bitiminden itibaren 5 yıl.	İlk dönem*
Aday başvuruları ve açık rızaya dayalı aday havuzu	Başvuru değerlendirmesi boyunca ve sürecin kapanmasından itibaren 6 ay. Aday havuzu, geçerli açık rızayla havuza alınma tarihinden itibaren 1 yıl. Rıza geri alınırsa havuz kullanımı durdurulur. Süre sonunda yeni geçerli rıza yoksa kayıt imha edilir. İşe alınanın yalnız gerekli belgeleri özlük dosyasına aktarılır.	İlk dönem*
Çalışan ve stajyer sağlık dosyaları. Diğer İSG kayıtları	Sağlık dosyası iş ilişkisi boyunca ve işten ayrılma tarihinden itibaren en az 15 yıl. Daha uzun özel yükümlülük ilgili kayda uygulanır. Diğer İSG kayıtları kendi belge türü ve yükümlülüğüne göre saklanır. Sağlık içeriği hekim erişiminde tutulur.	İlk dönem*
Servis, garanti ve geri çağırma kayıtları	Uygulanabildiği ölçüde servis ve garanti işlem belgeleri düzenleme tarihinden itibaren 3 yıl. Ticari belgeler ticari kayıtlar kuralına tabidir. Sınırlı teknik kayıtlar ilgili garanti ve geri çağırma yükümlülüğü boyunca.	İlk dönem*
Müşteri talep, şikâyet ve memnuniyet kayıtları	Operasyonel dosyalar kapanıştan itibaren 2 yıl. Kimlikle ilişkili anket yanıtları anketin tamamlanmasından itibaren 1 yıl sonra imha edilir veya anonimleştirilir. Anket temas listeleri çalışma sonunda silinir. Ticari belgeler ve uyuşmazlık delilleri kendi sürelerine tabidir.	İlk dönem* / çalışma sonunda

Kayıt grubu	Saklama süresi ve başlangıcı	İmha zamanı
Ticari elektronik ileti gönderim, onay ve ret kanıtları	6563 m. 11/3 kapsamındaki işlem kanıtları işlemden itibaren 10 yıl. Onay kanıtları onayın sona ermesinden, diğer ileti kanıtları kayıt tarihinden itibaren 3 yıl kuralına da tabidir. Aynı kayıta en geç dolan süre uygulanır. İspat arşivi pazarlama amacıyla kullanılamaz.	İlk dönem*
İş ilişkisi kurulmayan aday tedarikçi değerlendirmeleri	Değerlendirmenin kapanışından itibaren 1 yıl.	İlk dönem*
Uyuşmazlık, icra ve mahkeme bilgi talebi kayıtları	Somut süreç ve icra takibi boyunca gerekli deliller. Kesin karar ve ifa kanıtı, kesinleşme veya ifadan daha geç olan tarihten itibaren 10 yıl. Daha kısa özel süreler ayrıca değerlendirilir.	İlk dönem*
İnternet erişim, güvenlik ve hesap yetkisi kayıtları	İnternet toplu kullanım erişim kayıtları kayıt tarihinden itibaren 2 yıl. Diğer güvenlik ve erişim logları kayıt tarihinden itibaren 1 yıl. Hesap yetkilendirme ve kapatma kanıtı işlemden itibaren 2 yıl. Otomatik silme kendi süresinde yürütülür.	İlk dönem* / otomatik
Kamera görüntüleri	Kayıt tarihinden itibaren en fazla 45 gün.	Süre sonunda otomatik
Ziyaretçi, kart geçiş ve yalnız güvenlik amaçlı giriş çıkış kayıtları	Kayıt tarihinden itibaren 1 yıl. Ücrete esas PDKS kayıtları çalışan kayıtları kuralına tabidir.	İlk dönem*
İlgili kişi başvurusu, cevap ve tebliğ kanıtı	Başvurunun sonuçlandırılmasından itibaren 5 yıl. Devam eden şikâyet veya dava için gerekli kayıtlar süreç sonuna kadar korunur.	İlk dönem*
Açık rıza kanıtları	İşleme boyunca ve rızanın geri alınması, sona ermesi veya ilgili işlemin bitmesinden en son gerçekleşen tarihten itibaren 5 yıl. Ticari ileti onayları kendi özel kuralına tabidir.	İlk dönem*
Kişisel veri ihlali kapanış ve müdahale kanıtları	İnceleme ve ilgili resmî veya yargısal süreç boyunca gerekli kayıtlar. Kapanış raporu, bildirim ve önlem kanıtları kapanıştan itibaren 10 yıl. Ham veri kopyaları bu süreye topluca tabi değildir, delil ihtiyacı bittiğinde imha edilir.	İlk dönem* / ihtiyaç sonunda
İmha tutanakları ve işlem kayıtları	İmha işleminin gerçekleştirildiği tarihten itibaren 5 yıl.	İlk dönem*
Lojistik, sevkiyat ve gümrük kayıtları	Ticari olmayan operasyonel plan ve kopyalar işlemin tamamlanmasından itibaren 3 yıl. Gümrük belgeleri 4458 m. 13'teki işlem türüne özgü başlangıçtan itibaren 5 yıl. Ticari kayıtlarda daha uzun ticari saklama süresi korunur.	İlk dönem*
İç etkinlik ve duyuru operasyon kayıtları	Etkinlik veya duyurudan itibaren 1 yıl.	İlk dönem*
Kurumsal görsel arşivi ve tanıtım görüntü veya ses kayıtları	Hukuki sebebi bulunan kurumsal görseller çekimden itibaren en fazla 3 yıl, yıllık ihtiyaç kontrolüyle. Rızaya dayalı tanıtım içeriği kampanya veya kullanım amacı boyunca, çekimden itibaren en fazla 3 yıl. Rıza geri alınırsa kullanım durdurulur, başka geçerli neden yoksa imha edilir.	İlk dönem*

* İlk dönem, saklama süresi ve işleme şartları sona erdikten sonraki ilk periyodik imha dönemidir. Otomatik silme süreleri, ilgili kişi başvuruları ve yetkili makam kararları için bu dönem beklenmez.

8. PERİYODİK İMHA SÜRESİ

Politikanın onaylanmasıyla periyodik imha aralığı en fazla altı ay olarak uygulanır. İşlemler Haziran ve Aralık aylarında planlanır. Dönem tarihleri arasındaki aralık altı ayı aşamaz. İlk uygulamada birikmiş kayıtlar gözden geçirilir.

Kişisel veri işleyen ya da saklayan tüm departmanlar, işleme şartlarının ortadan kalkıp kalkmadığını en geç altı aylık dönemler halinde kullandıkları kayıt ortamlarında gözden geçirir. İlgili kişinin başvurusu veya bir mahkeme kararı üzerine bu gözden geçirme, periyodik döneme bakılmaksızın derhal yapılır.

9. İLGİLİ KİŞİNİN TALEBİ ÜZERİNE İMHA

İlgili kişi, Kanun'un 11. ve 13. maddelerine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep edebilir. Bu halde Şirket aşağıdaki şekilde hareket eder:

- Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa, talebe konu kişisel veriler silinir, yok edilir veya anonim hale getirilir. Talep en geç otuz gün içinde sonuçlandırılır ve ilgili kişiye bilgi verilir.
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu kişisel veriler üçüncü kişilere aktarılmışsa, bu durum üçüncü kişiye bildirilir ve üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılması temin edilir.
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa talep, Kanun'un 13. maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir. Ret cevabı en geç otuz gün içinde yazılı olarak veya elektronik ortamda ilgili kişiye bildirilir.

Başvuruların alınmasında ve yanıtlanmasında, Şirketin ilgili kişi başvuru sürecine ilişkin dokümanında belirtilen usul ve esaslar uygulanır.

10. POLİTİKANIN YAYIMLANMASI, SAKLANMASI VE GÜNCELLENMESİ

Onaylanan Politika, sürüm ve onay kaydı korunarak erişime açılır. Elektronik nüsha esas alınabilir. Kurumsal belge yönetimi gerektiriyorsa basılı nüsha da tutulur. İnternet sitesinde yayımlanacak nüshada kişilerin adları, iç görev dağılımı ve sistem güvenliğine ilişkin ayrıntılar yer almaz. İnceleme yorumları ve değişiklik işaretleri, onaylanan metnin yayımlanmasından önce kaldırılır.

Politika, mevzuat değişikliklerinde ve ihtiyaç duyuldukça, her halde asgari yılda bir kez gözden geçirilir ve gerekli bölümler güncellenir. Yapılan güncellemeler, Yönetmelik'in 6. maddesinin birinci fıkrasının (h) bendi uyarınca sürüm bilgisiyle birlikte işbu Politikanın 12. bölümünde gösterilir. Kanun, Yönetmelik ve ilgili diğer mevzuatta değişiklik yapılması halinde, Politika henüz güncellenmemiş olsa dahi mevzuattaki değişiklikler derhal uygulanır.

11. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Şirket'in yetkili organı tarafından onaylanmasını takiben [●] tarihinde yürürlüğe girecektir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politikanın eski sürümü kullanımdan çekilir, sürüm ve onay geçmişi korunur ve en az beş (5) yıl süreyle Şirketçe dosyasında saklanır.

12. REVİZYON GEÇMİŞİ

Bu bölüm, Yönetmelik'in 6. maddesinin birinci fıkrasının (h) bendi uyarınca Politika üzerinde yapılan güncellemeleri gösterir.

Tablo 7: Revizyon geçmişi

Sürüm	Tarih	Değişikliğin Özeti	Hazırlayan / Onaylayan
1.0	[●]	İlk sürüm. Uygulama adımları Politika içinde düzenlenmiştir.	[●]

13. UYGULAMA ADIMLARI

13.1. Dönemin Başlatılması ve Kapsamın Onaylanması

İmha Koordinatörü Haziran ve Aralık dönemlerini ilgili birimlere bildirimle başlatır ve işlem takvimini bildirir. Birim yöneticisi, Envanter ve Politikanın 7. bölümündeki süreler ile başlangıç tarihlerini dikkate alarak imha kapsamını onaylar. Aynı ölçüte tabi kayıtlar topluca tanımlanabilir. Mevcut e-posta veya liste onayı yeterlidir.

Devam eden sözleşme, garanti, uyumsuzluk, denetim veya resmi süreç için gerekli kayıtlar, gerekçesi ve yeniden değerlendirme tarihiyle kapsamdan ayrılır. İlgisiz kayıtlar bu nedenle saklanmaz. Hukuki tereddütler Hukuk ile çözülür. Koordinatör onaylı kapsamı ilgili çalışanlara ve işlem sorumlularına iletir. Çalışan, kendisine bildirilen onaylı imha kapsamını esas alır. Saklama sürelerine ilişkin tereddütler, bu Politikadaki görev dağılımı çerçevesinde giderilir.

Otomatik silme kendi süresinde devam eder. İlgili kişi başvuruları ve yetkili makam kararları kendilerine uygulanacak sürelerde ele alınır, periyodik dönem beklenmez.

13.2. Çalışanın İşlemi ve Teyidi

Çalışan, bildirilen kapsamı yalnız fiilen kullandığı ve kontrol etmeye yetkili olduğu alanlarda kontrol eder. EK-1'deki ortam hatırlatmaları örnektir ve kontrolü kolaylaştırır. E-posta, kişiye tahsisli dosya alanları, bilgisayar, kurumsal telefon ve fiziki evrak bu kapsamda değerlendirilebilir. Yetkisi dahilindeki dijital kayıtları siler, silinmiş öğelerde ve geri dönüşüm kutularında erişebildiği ilgili kopyalarını da temizler. Kağıt belgeleri uygun kırpmak makinesinde yeniden birleştirilemeyecek şekilde imha eder. Uygun imha imkânının bulunmadığı hallerde belgeleri, imha işlemini gerçekleştirmek üzere yetkili birime teslim eder. Taşınabilir ortamlardaki kapsam içi kayıtlar için BT'den işlem ister veya ortamı teslim eder. Ortak alanlarda işlemi yetkili görevli uygular. Kullanılmayan ortamlar için işlem veya açıklama istenmez.

Çalışan, işlem sonucunu EK-1 veya aynı bilgileri içeren kurumsal e-posta ile bir kez bildirir. EK-1, çalışanın kendi alanındaki kontrol ve işlem sonucunu teyit etmesi amacıyla kullanılır. Kontrol edilen ortam, onaylı kapsam referansı, yapılan işlem veya sonuç ve tarih belirtilir. Aynı işlem, sonuç ve tarihe sahip alanlar tek satırda gösterilebilir. Kayıt bulunmadığında kontrol edilen alanlar ve bu sonuç belirtilir. Tamamlanamayan veya ilgili birime iletilen işler, kısa neden ve bildirim bilgisiyle ayrı gösterilir. Çalışanın kimliği ve tarih belli ise ayrıca form veya ıslak imza aranmaz. Çalışan yalnız kendi yetkisindeki işlemi teyit eder. Bu teyit, sistemler, yedekler veya hizmet sağlayıcılar nezdindeki teknik imhanın kanıtı yerine geçmez.

Kayıtlar kişisel cihaz veya hesaplara aktarılamaz. İmhadan kaçınmak amacıyla başka ortamlara taşınamaz veya yeniden yedeklenemez. Saklanması gereken bilgilerle birlikte bulunan kayıtlar, yalnız imha kapsamındaki bölümleri bakımından işleme alınır.

13.3. BT İşlemleri ve Yedekler

BT, onaylı kapsamda kendi yetkisindeki işlemleri uygular. Kullanıcı yönetimi ile kayıt silme yetkilerini ayrı değerlendirir. Yetkisi dışındaki işlemi ilgili global ekipten veya hizmet sağlayıcıdan talep eder. Hesap kapatma tek başına kayıt imhası sayılmaz. Teknik işlem kaydında sistem veya ortama, kapsama, kullanılan yöntem ve gerektiğinde araca, fiili işlem tarihine, uygulayan kişi veya birime ve sonuç kontrolüne yer verilir. Cihaz veya ortam imhasında gerektiği ölçüde cihaz kimliği de belirtilir. Mevcut sistem kaydı, iş emri veya hizmet sağlayıcı belgesi bu bilgileri içeriyorsa ayrıca form düzenlenmez.

Aktif kayıtlar, sürümler, arşivler ve yedekler ayrı kontrol edilir. Yedeklerin saklama döngüsü, imha tarihi, erişim ve geri yükleme yetkileri teknik kayıta gösterilir. İmha kapsamındaki kayıtlar, olağan kullanım amacıyla yedeklerden geri alınamaz. Zorunlu geri yüklemede, yeniden kullanıma açılmadan silme işlemi tekrarlanır. Teknik engel nedeniyle tamamlanamayan kısımlar gerekçesi, sorumlusu ve hedef tarihiyle açık tutulur. Yedekleme süresiz saklama gerekçesi değildir.

13.4. Global Ekip ve Hizmet Sağlayıcılara Talepler

İlgili birim veya yetkili BT sorumlusu talebi mevcut e-posta veya hizmet talep sistemiyle iletir. Talepte şirket, muhatap, sistem veya ortam, kayıt türü ve dönemi, süre başlangıcı, kapsam onayı ve istenen işlem gösterilir. İşlemin gerçekleştirilmesi ve sonucunun bildirilmesi için öngörülen tarihler ayrı ayrı belirtilir. Gereksiz kişisel veri içeriği eklenmez. Veri işleyene sözleşme kapsamındaki talimat verilir. Bağımsız veri sorumlusundan kendi yükümlülükleri çerçevesinde değerlendirme ve sonuç istenir. Rol veya yetki belirsizse Hukuk görüşü alınır.

Veri işleyene kısa örnek: “[Onaylı kapsam] içindeki kayıtların sözleşmemiz kapsamındaki talimatımız doğrultusunda [silinmesini / yok edilmesini / anonim hale getirilmesini] [işlem tarihi] tarihine kadar rica ederiz. Kapsamı, yöntemi, fiili işlem tarihini ve uygulayan birimi, açık kalan kayıtlar varsa gerekçesini, erişim kısıtını ve öngörülen tamamlanma tarihini [bildirim tarihi] tarihine kadar bildirmenizi rica ederiz.”

13.5. Fiziki Arşiv ve Kamera Kayıtları

Arşiv sorumlusu onaylı kapsam içindeki dosya ve kutuları ayırır. Dış arşiv veya imha hizmeti kullanılıyorsa işlemin sonucunu gösteren belge alınır. Hekimin kontrolündeki sağlık dosyaları, çalışanların bu bölüm kapsamındaki imha işlemlerine dahil edilmez.

Kamera kayıtlarının otomatik silme döngüsünü BT kontrol eder. Canlı izleme, geçmiş kayda erişim ve dışa aktarma yetkileri ayrı belirlenir. Görüntü paylaşımı hukuki sebep, sınırlı kapsam ve yetkili onayıyla yürütülür. Olay nedeniyle ayrılan kesitler ve dışa aktarılan kopyalar, delil ihtiyacı sona erdiğinde ayrıca imha edilir. Otomatik döngünün dönem kontrol kaydı yeterlidir. Her üzerine yazma için ayrı kayıt oluşturulmaz.

13.6. Sonucun Takibi ve Kapanış

Koordinatör çalışan teyitlerini ve BT, global ekip, hizmet sağlayıcı, arşiv ve kamera işlemlerinin sonuçlarını EK-2’de izler. Mevcut tutanak, e-posta, iş emri veya teknik kayıtlara referans verilmesi yeterlidir. Bu belgelerin içeriğinin takip tablosunda tekrarlanması gerekmez. Çalışan alanındaki işlem ile sistem veya yedek işlemi farklı kapsamdaysa ayrı izlenir. Koordinatör teknik imhayı kendisi doğrulamak yerine yetkili birimin sonuç kontrolünü gösteren kaydı takip eder.

Talebin iletilmesi veya ortamın teslim edilmesi, imha işleminin tamamlandığı anlamına gelmez. Açık kalemlerde gerekçe, sorumlu ve sonraki takip tarihi belirtilir. Talebi açan birim sonuç teyidini takip eder. İlgili kapsam için doğrulanabilir sonuç kaydı geldiğinde kalem kapatılır. Teknik işlem bekleyen kalemler, yalnızca çalışan teyidine dayanılarak kapatılamaz. Otomatik silmede işlem veya dönem kontrol kaydı kullanılır, aynı işlem için çalışanlardan ayrıca form alınmaz. Diğer kalemler açık kalır ve sonraki periyodik dönem beklenmeden takip edilir. Hukuki süreyi etkileyen engeller gecikmeden Hukuk ve komiteye bildirilir.

Birim yöneticisi sonuçları gözden geçirir. Koordinatör dönem sonucunu ve çözilemeyen istisnaları komiteye sunar. Her işlem için ayrıca koordinatör, şahit veya komite imzası aranmaz. Şirketlerin kapsam ve onayları ayrı tutulur. İK ve sağlık kayıtlarının içeriği genel tabloya kopyalanmaz, erişimi kontrollü referans kullanılır. İşlem kayıtları diğer hukuki yükümlülükler saklı kalmak üzere işlem tarihinden itibaren 5 yıl saklanır.