



İNSAN KAYNAKLARI POLİTİKA VE PROSEDÜR SETİ

İK-PL-03

Çalışan Kişisel Verilerinin Korunması Politikası

Çalışan verisinin işleme amaçları, hukuki sebepleri, erişim, aktarım, saklama ve imha kuralları ile ilgili kişi hakları

POLİTİKA · v1.0 · DAHİLİ · TASLAK — Yönetim Kurulu onayına sunulacak sürüm

BELGE SAHİBİ

İK Yöneticisi (İKY)

ONAY MAKAMI

Yönetim Kurulu

KAPSANAN ALT SÜREÇLER

D.03 · D.04 · L.05

DOTEKS

Bu belge şirket içi kullanım içindir; çalışanlara tebliğ edilir. Aydınlatma metni ve açık rıza formları bu politikanın uygulama belgeleridir.

BELGE KONTROL BİLGİLERİ

Belge Kimliği

Kod · sürüm · sahiplik · kapsam · gözden geçirme döngüsü

BELGE KODU İK-PL-03	BELGE TÜRÜ POLİTİKA	SÜRÜM · DURUM v1.0 · TASLAK — Yönetim Kurulu onayına sunulacak sürüm
BELGE SAHİBİ İK Yöneticisi (İKY)	HAZIRLAYAN İK Yöneticisi	KONTROL EDEN Hukuk Müşavirliği · Bilgi Teknolojileri · Genel Müdür
ONAY MAKAMI Yönetim Kurulu	GİZLİLİK SINIFI DAHİLİ	YÜRÜRLÜK TARİHİ [YK karar tarihi]
KAPSANAN ALT SÜREÇLER D.03 · D.04 · L.05	İLGİLİ BELGELER İK-PL-01 · İK-PL-02 · İK-PL-04 · İK-PR-06 · İK-PR-07 · İK-PR-08 · İK-PR-12 · İK-PR-16	EKLER Şekil 1–23 · Form eki yok (İK-FR-18 ve arşiv formları prosedürlerde tanımlıdır)

GÖZDEN GEÇİRME DÖNGÜSÜ

Yıllık — her yılın Mart ayında veri envanteri güncellemesiyle birlikte; mevzuat, Kurul kararı veya veri ihlali hâlinde derhal

İK-PL-03 · v1.0

Şekil 1 Belge kimliği — kod, sürüm, sahiplik ve kapsam

Revizyon Çizgisi

Sürüm · tarih · değişiklik özeti · hazırlayan → onaylayan



Şekil 2 Revizyon çizgisi

İÇİNDEKİLER

1	Amaç
2	Kapsam
3	Dayanak
4	Tanımlar
5	İlkeler
5.1	Veri koruma ilkeleri
V-01	Hukuka ve dürüstlük kurallarına uygunluk
V-02	Doğru ve güncel
V-03	Belirli, açık ve meşru amaç
V-04	Amaçla bağlantılı, sınırlı ve ölçülü
V-05	Süre ile sınırlı saklama
V-06	Görev gereği erişim
V-07	Özel nitelikli veri ayrı
V-08	Aydınlatma ve şeffaflık
V-09	Veri işleyen sorumluluğu
V-10	İhlal müdahalesi ve bildirim
5.2	Alt süreç ilkeleri
6	Roller ve sorumluluklar
7	Uygulama esasları
7.1	Veri sınıflandırması
7.2	Veri envanteri ve hukuki sebepler
7.3	Veri yaşam döngüsü
7.4	Erişim ve yetki yönetimi
7.5	Aktarım ve veri işleyenler
7.6	İlgili kişi hakları
7.7	Veri ihlali müdahalesi
7.8	Yıllık takvim, kontrol noktaları ve göstergeler
8	İstisna ve sapma
9	İhlal ve yaptırım
10	Gözden geçirme
11	İlgili belgeler
12	Revizyon ve onay

Şekiller

- Şekil 1** Kapsam haritası — politikanın düzenlediği alanlar ve kapsam dışı konuların düzenleyen belgeleri
- Şekil 2** Dayanak sütunları — mevzuat, standart ve çerçeve, kurumsal belgeler
- Şekil 3** Terim kartları — tanımlar
- Şekil 4** Veri koruma ilkeleri I — V-01...V-05: hüküm, gerekçe ve kaynak
- Şekil 5** Veri koruma ilkeleri II — V-06...V-10: hüküm, gerekçe ve kaynak
- Şekil 6** Alt süreç ilkeleri — üç alt süreç, altı ilke
- Şekil 7** Yönetişim haritası — üç katman, dokuz rol ve işleme yetkisinin akışı
- Şekil 8** RACI matrisi — düzenlenen alt süreçler, ihlal müdahalesi, ilgili kişi başvurusu ve aktarım
- Şekil 9** Veri sınıflandırma katmanları — dört sınıf, erişim ilkesi ve kural
- Şekil 10** Çalışan veri envanteri — sekiz kategori, hukuki sebep, saklama süresi ve erişim sınıfı
- Şekil 11** Çalışan verisi yaşam döngüsü — sekiz adım, sorumlu ve kontrol noktası
- Şekil 12** Erişim matrisi — veri kategorisi × rol, erişim düzeyi
- Şekil 13** İlgili kişi hakları ve yanıt süreleri — sekiz hak, kanal ve sorumlu
- Şekil 14** Veri ihlali müdahale akışı — yedi adım, 72 saat Kurul bildirimi
- Şekil 15** Yıllık veri koruma takvimi — ay bazında sabit olaylar ve sorumlular
- Şekil 16** Güvence haritası — dört kontrol noktası ve iki gösterge
- Şekil 17** İstisna merdiveni — üç kademe: makam, kapsam, azami süre ve kayıt
- Şekil 18** Yaptırım merdiveni ve bildirim kanalı — dört kademe, karar makamı ve koruma esasları
- Şekil 19** Gözden geçirme ve revizyon döngüsü — yıllık plan ve plansız tetikleyiciler
- Şekil 20** Belge ağı — üst çerçeve, ilgili politikalar, veri işleyen prosedürler ve kurumsal belgeler
- Şekil 21** Onay yolu — hazırlayan, kontrol edenler, onaylayan, tebliğ ve aydınlatma

1 Amaç

Bu politika, Şirketin veri sorumlusu sıfatıyla çalışan adayı, çalışan, eski çalışan, stajyer ve çalışan yakınlarına ait kişisel verileri hangi amaçlarla, hangi hukuki sebeplere dayanarak, hangi erişim, aktarım, saklama ve imha kurallarıyla işleyeceğini ve ilgili kişilerin haklarını nasıl kullanacağını belirler. Politika, İK-PL-01 İnsan Kaynakları Politikası'nın üst çerçevesi altında ve Şirketin kurumsal KVKK politikasıyla uyumlu olarak çalışan verisi özelinde bağlayıcı kuralları koyar.

Politikanın amacı, çalışan verisinin işlenmesini kişisel takdirden çıkararak yazılı bir envantere (kategori, amaç, hukuki sebep, süre), yazılı bir erişim düzenine (rol–yetki matrisi ve ayrıcalıklı erişim listesi), yazılı bir saklama–imha takvimine ve yazılı bir ihlal müdahale akışına bağlamaktır. Bu yapı, Kanunun öngördüğü idari ve cezai yaptırım riskini yönetir; çalışanın verisi üzerindeki güvenini ve Şirketin itibarını korur.

Politika, İK-OD Best Practice Evreni'nin D ailesi (Çalışan Ana Verisi, Sistemler ve Analitik) altındaki D.03 Erişim ve yetki yönetimi ve D.04 Kişisel veri koruma alt süreçleri ile L ailesi altındaki L.05 Arşivleme, saklama ve alumni ilişkisi alt sürecini doğrudan düzenler; bu alt süreçlere bağlı KN-20, KN-21, KN-22 ve KN-62 kontrol noktalarını ve KPI-15 ve KPI-50 göstergelerini işletir. Veri sahipliği ve ana veri değişiklik yönetimi (D.01, D.02) İK-PR-07'de, arşiv operasyonu İK-PR-08'de düzenlenir ve bu politikanın ilkelerine tabidir.

2 Kapsam

Bu politika, Şirketin tüm işyerlerinde, tüm sistemlerinde (İK bilgi sistemi, bordro, PDKS, e-posta, kamera, arşiv) ve tüm kayıt ortamlarında (elektronik, fiziksel, hizmet sağlayıcı ortamı) çalışan verisi işleyen herkes bakımından bağlayıcıdır: yöneticiler, İK, Finans, BT, iş yeri hekimi, hizmet sağlayıcılar ve verinin öznesi olarak çalışanlar. Politika aşağıdaki unsurları kapsar:

- Çalışan adayı, çalışan, eski çalışan (alumni), stajyer ve çalışan yakınlarına ait kişisel verilerin tüm işleme faaliyetleri;
- Veri koruma ilkeleri, işleme amaçları ve hukuki sebeplerin veri kategorisi bazında belirlenmesi (veri envanteri);
- Veri sınıflandırması, görev gereği erişim, rol–yetki matrisi ve ayrıcalıklı erişimlerin yönetimi;
- Özel nitelikli verilerin (sağlık, sendika, ceza mahkûmiyeti, biyometrik) ayrı ortamda ve kısıtlı erişimle işlenmesi;
- Yurt içi ve yurt dışı aktarım, veri işleyen (hizmet sağlayıcı) sözleşmeleri ve grup içi paylaşım kuralları;
- Saklama süresi tablosu, arşivleme, imha ve alumni ilişkisinin rıza esası;
- Aydınlatma, açık rıza, ilgili kişi başvuruları ve yanıt süreleri;
- Veri ihlali müdahale akışı, Kurul ve ilgili kişi bildirimleri, kontrol noktaları ve göstergeler.

Kapsam Haritası

Sol: bu politikanın düzenlediği alanlar · Sağ: kapsam dışı konular ve düzenleyen belge

KAPSAM İÇİ	KAPSAM DIŞI → DÜZENLEYEN BELGE
1 Çalışan adayı, çalışan, eski çalışan (alumni), stajyer ve çalışan yakınlarına ait kişisel verilerin tüm işleme faaliyetleri	Müşteri, tedarikçi ve ziyaretçi verilerinin işlenmesi Kurumsal KVKK Politikası ve Veri Saklama–İmha Politikası (Şirket geneli)
2 Veri koruma ilkeleri, işleme amaçları ve hukuki sebeplerin veri kategorisi bazında belirlenmesi (veri envanteri)	Ana veri sahipliği, mutabakat ve değişiklik yönetimi (D.01, D.02) İK-PR-07 Çalışan Ana Verisi Yönetimi Prosedürü
3 Veri sınıflandırması, görev gereği erişim, rol–yetki matrisi ve ayrıcalıklı erişimlerin yönetimi	Arşiv operasyonu, fiziksel ve elektronik saklama ortamları, imha tutanağı adımları İK-PR-08 Arşiv ve Saklama Prosedürü
4 Özel nitelikli verilerin (sağlık, sendika, ceza mahkûmiyeti, biyometrik) ayrı ortamda ve kısıtlı erişimle işlenmesi	Bilgi güvenliği altyapısı, ağ, uç nokta ve şifreleme standartları Bilgi Güvenliği Politikası (BT) · ISO/IEC 27001 kontrol seti
5 Yurt içi ve yurt dışı aktarım, veri işleyen (hizmet sağlayıcı) sözleşmeleri ve grup içi paylaşım kuralları	Bordro hizmet sağlayıcısıyla veri paketi iletimi ve kullanıcı kuruluş kontrolleri İK-PR-12 Bordro Kullanıcı Kontrolleri Prosedürü
6 Saklama süresi tablosu, arşivleme, imha ve alumni ilişkisinin rıza esası	Ayrılış kontrol listesi, erişim kapatma adımları ve alumni kaydı İK-PR-16 İşten Ayrılış Prosedürü
7 Aydınlatma, açık rıza, ilgili kişi başvuruları ve yanıt süreleri	Etik bildirim kanalı ve çıkar çatışması beyanlarının işlenmesi İK-PL-04 Etik ve Davranış Kuralları
8 Veri ihlali müdahale akışı, Kurul ve ilgili kişi bildirimleri, kontrol noktaları ve göstergeler	

IK-PL-03 · v1.0 · Kapsam

Şekil 3 Kapsam haritası — politikanın düzenlediği alanlar ve kapsam dışı konuların düzenleyen belgeleri

Kapsam dışı bırakılan konular ilgili kurumsal politika ve prosedürlerde düzenlenir; çalışan verisine dokunan her prosedür bu politikanın ilkelerine tabidir. Bir işleme faaliyetinin bu politikaya mı yoksa kurumsal KVKK politikasına mı tabi olduğu konusunda tereddüt hâlinde, ilgili kişinin çalışan sıfatı belirleyicidir ve daha koruyucu hüküm uygulanır.

3 Dayanak

Politika, 6698 sayılı Kanun ve ikincil düzenlemeleri ile Kişisel Verileri Koruma Kurulunun ilke kararları üzerine kurulur; iş, sosyal güvenlik ve iş sağlığı mevzuatının saklama ve kayıt yükümlülükleri saklama sürelerinin dayanağıdır. Bilgi güvenliği standartları teknik ve idari tedbirlerin ölçüsüdür; grup içi veya yurt dışı aktarımda GDPR hükümleri referans alınır. Mevzuat ve Kurul kararları her koşulda önceliklidir.

Dayanak Sütunları

Politikanın üzerine kurulduğu mevzuat, standart ve kurumsal belge tabanı

MEVZUAT	STANDART VE ÇERÇEVE	KURUMSAL BELGELER
6698 sayılı Kişisel Verilerin Korunması Kanunu m.4, 5, 6, 7, 8, 9, 10, 11, 12, 16 İlkeler, işleme şartları, özel nitelikli veri, silme-yok etme, aktarım, aydınlatma, ilgili kişi hakları, veri güvenliği, VERBİS	ISO/IEC 27001:2022 — A.5.15–5.18, A.5.34, A.8 Erişim kontrolü, ayrıcalıklı erişim, gizlilik ve kişisel veri koruma, teknolojik kontroller	IK-PL-01 İnsan Kaynakları Politikası Üst çerçeve; IL-X-07 görev gereği erişim ilkesi; istisna ve yaptırım mekanizması
Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik Saklama ve imha politikası, periyodik imha, imha kayıtları	ISO/IEC 27701:2019 Kişisel veri yönetim sistemi; veri sorumlusu ve veri işleyen kontrolleri	Kurumsal KVKK Politikası · Veri Saklama-İmha Politikası · VERBİS kaydı Şirket geneli veri sorumlusu çerçevesi; bu politika çalışan verisi özelinde uygular
Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ Aydınlatma metninin içeriği ve zamanı	GDPR (AB) 2016/679 m.5, 9, 28, 32, 33 Grup içi veya yurt dışı aktarımda referans; ihlal bildirimi 72 saat	IK-OD Best Practice Evreni v1.2 D ailesi ve L.05: IL-D03, IL-D04, IL-L05 ilkeleri; KN-20...22, KN-62; KPI-15, KPI-50
4857 sayılı İş Kanunu m.75; 5510 sayılı Kanun; 6331 sayılı Kanun m.15 Özlük dosyası, sigortalı kayıtları, sağlık gözetimi verisinin saklanması	DAMA-DMBOK — Veri yönetimi Veri sahipliği, sınıflandırma ve kalite	
Kişisel Verileri Koruma Kurulu ilke kararları ve rehberleri Çalışan verisi, kamera, biyometrik veri ve veri ihlali bildirimi uygulamaları		

IK-PL-03 · v1.0 · Dayanak

Şekil 4 Dayanak sütunları — mevzuat, standart ve çerçeve, kurumsal belgeler

Kanun, yönetmelik veya Kurul ilke kararında çalışan verisini etkileyen bir değişiklik hâlinde politika hükümleri değişikliğin yürürlük tarihinden itibaren mevzuata uygun yorumlanır; Hukuk Müşavirliğinin yazılı görüşü geçici uygulama esasıdır ve politika en geç 60 gün içinde revize edilir. Kurulun somut bir karar veya rehberle getirdiği ek tedbir, revizyon beklenmeksizin derhal uygulanır.

4 Tanımlar

Bu politikada geçen terimler Kanundaki ve IK-OD Best Practice Evreni sözlüğündeki anlamlarıyla kullanılır; alt kademe belgeler aynı terimleri aynı anlamla kullanır. Kırmızı işaretli terimler veri koruma sisteminin taşıyıcı kavramlarıdır.

Terim Kartları

Tanımlar — politikada ve alt kademe belgelerde aynı anlama

Kişisel veri

Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; çalışan bağlamında kimlik, iletişim, özlük, ücret, performans ve dijital izler.

Veri işleyen

Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen dış taraf; bordro, sağlık, sigorta ve yazılım sağlayıcıları.

İlgili kişi

Kişisel verisi işlenen gerçek kişi; çalışan adayı, çalışan, eski çalışan, stajyer, çalışan yakını.

Görev gereği erişim

Bir veriye yalnızca o görevi yerine getirmek için gerekli olan kişilerin, gerekli kapsamda ve sürede erişebilmesi ilkesi.

Rol-yetki matrisi

Sistem ve veri kategorisi bazında hangi rolün hangi erişim düzeyine (tam, okuma, sınırlı, yok) sahip olduğunu gösteren tablo.

Aydınlatma

İşleme faaliyeti başlamadan önce ilgili kişiye amaç, hukuki sebep, aktarım ve hakları hakkında bilgi verilmesi.

Saklama süresi

Bir veri kategorisinin yasal veya kurumsal olarak tutulması gereken azami süre; süre sonunda imha zorunludur.

Veri ihlali

Kişisel verinin yetkisiz kişilerce elde edilmesi, yetkisiz erişim, kayıp veya ifşâ; Kurula 72 saat içinde bildirilir.

Özel nitelikli veri

Sağlık, sendika üyeliği, din, ceza mahkûmiyeti, biyometrik ve genetik veri gibi kanunla ayrıca korunan kişisel veri.

Veri sorumlusu

Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu tüzel kişi: Şirket.

Veri sahibi (iş sahibi)

Bir veri alanının doğruluğundan, işleme amacından ve erişim kurallarından hesap veren iç rol; çalışan verisinde İK Yöneticisi.

Veri envanteri

İşlenen çalışan verilerinin kategori bazında amaç, hukuki sebep, saklama süresi, aktarılan taraf ve erişim bilgisiyle tutulduğu kayıt.

Ayrıcalıklı erişim

Ücret, bordro, sağlık ve sistem yönetimi gibi yüksek riskli verilere isim bazında tanımlanan erişim.

Açık rıza

Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza; iş ilişkisinde yalnızca kanunî şart bulunmadığında kullanılır.

İmha

Kişisel verinin silinmesi, yok edilmesi veya anonim hâle getirilmesi; tutanakla belgelenir.

Alumni

İş ilişkisi sona ermiş eski çalışan; iletişim yalnızca ayrı ve açık rızaya dayanır.

IK-PL-03 · v1.0 · Tanımlar

Şekil 5 Terim kartları — tanımlar

5 İlkeler

Politikanın ilkeleri iki katmandan oluşur. Birinci katman, Kanunun 4. maddesindeki genel ilkeleri çalışan verisi özelinde somutlaştıran ve bunlara erişim, özel nitelikli veri, veri işleyen ve ihlal müdahalesi ilkelerini ekleyen on veri koruma ilkesidir (V-01...V-10); bu ilkeler her işleme faaliyetinin tasarım ve kontrol ölçüsüdür ve hiçbir makam bunlardan istisna veremez. İkinci katman, politikanın doğrudan düzenlediği üç alt sürece özgü ilkelerdir. IK-PL-01'in on kesişen ilkesi, özellikle IL-X-01 (tek kayıt ortamı), IL-X-05 (sorumluluk devredilmez) ve IL-X-07 (görev gereği erişim), bu politikada aynen geçerlidir.

5.1 Veri koruma ilkeleri

Veri Koruma İlkeleri I

Hüküm · gerekçe · kaynak — çalışan verisinin her işleme faaliyetine uygulanır; istisna verilmez

V-01	Hukuka ve dürüstlük kurallarına uygunluk	KVKK m.4/2-a, m.5/2 · Kurul rehberi
HÜKÜM	GEREKÇE	
Çalışan verisi yalnızca Kanunda sayılan işleme şartlarından birine dayanarak ve ilgili kişinin makul beklentisine uygun biçimde işlenir; iş ilişkisindeki güç dengesizliği nedeniyle açık rıza son çaredir.	İş ilişkisinde rıza özgür iradeyi tam yansıtmaz; işleme, sözleşmenin ifası veya kanunî yükümlülük gibi rızaya bağlı olmayan şartlara dayandırılır.	
V-02	Doğru ve güncel	KVKK m.4/2-b · IL-X-01
HÜKÜM	GEREKÇE	
Çalışan verisi doğru ve gerektiğinde güncel tutulur; kayıt sahibi sistem taktır, kopya ortamlar mutabakatla doğrulanır.	Yanlış veri yanlış bordro, yanlış bildirim ve yanlış karar üretir; tek kayıt sahibi sistem doğruluğun ön koşuludur.	
V-03	Belirli, açık ve meşru amaç	KVKK m.4/2-c · m.16
HÜKÜM	GEREKÇE	
Her veri kategorisinin işleme amacı veri envanterinde yazılıdır; amaç dışı kullanım ve amaçla bağdaşmayan yeni işleme yasaktır.	Amaç yazılı olmadan ölçülülük ve süre sınırı değerlendirilemez; envanter, amacı denetlenebilir kılar.	
V-04	Amaçla bağlantılı, sınırlı ve ölçülü	KVKK m.4/2-ç · Veri minimizasyonu
HÜKÜM	GEREKÇE	
Yalnızca amacın gerektirdiği veri, gerektirdiği kapsamda toplanır; 'ileride gerekebilir' gerekçesiyle veri toplanmaz.	Fazla veri fazla risk demektir; toplanmayan veri sızdırlamaz ve saklanmak zorunda değildir.	
V-05	Süre ile sınırlı saklama	KVKK m.4/2-d, m.7 · Yönetmelik
HÜKÜM	GEREKÇE	
Her veri kategorisi için saklama süresi tablosu yazılıdır; süre sonunda veri periyodik imha döneminde tutanakla imha edilir.	Süresi dolan verinin tutulması başlı başına ihlaldir; saklama tablosu imhayı zorunlu ve kanıtlanabilir kılar.	

IK-PL-03 · v1.0 · İlkeler I

Şekil 6 Veri koruma ilkeleri I — V-01...V-05: hüküm, gerekçe ve kaynak

Veri Koruma İlkeleri II

Hüküm · gerekçe · kaynak — çalışan verisinin her işleme faaliyetine uygulanır; istisna verilmez

V-06 Görev gereği erişim HÜKÜM Çalışan verisine erişim rol-yetki matrisiyle ve görev gereği ilkesiyle verilir; ayrıcalıklı erişimler isim bazında listelenir ve yılda bir gözden geçirilir.	GEREKÇE Yetkisiz iç erişim en sık ihlal kaynağıdır; matris ve yıllık gözden geçirme erişimi görünür ve hesap verilebilir kılar.	KVKK m.12 · ISO 27001 A.5.15 · IL-X-07
V-07 Özel nitelikli veri ayrı HÜKÜM Sağlık, sendika, ceza mahkûmiyeti ve biyometrik veriler özlük dosyasından ayrı, kilitli veya şifreli ortamda ve isim bazlı erişimle tutulur; Kurulun belirlediği ek tedbirler uygulanır.	GEREKÇE Özel nitelikli verinin ifşası kişiye telafisi güç zarar verir ve en yüksek idari yaptırıma tabidir.	KVKK m.6 · Kurul kararı 2018/10
V-08 Aydınlatma ve şeffaflık HÜKÜM İşleme faaliyeti başlamadan önce ilgili kişi aydınlatılır; aydınlatma metni işe girişte imzalı tebliğ edilir ve envanter değişikliğinde güncellenir.	GEREKÇE Aydınlatılmamış işleme hukuka aykırıdır; şeffaflık çalışan güveninin ve ilgili kişi haklarının temelidir.	KVKK m.10 · Aydınlatma Tebliği
V-09 Veri işleyen sorumluluğu HÜKÜM Çalışan verisi işleyen her hizmet sağlayıcıyla veri işleyen sözleşmesi imzalanır; sağlayıcı yalnızca talimatla işler; sorumluluk Şirkette kalır.	GEREKÇE Hizmet devredilir, sorumluluk devredilmez; sözleşme olmadan sağlayıcının işlemesi Şirketin ihlalidir.	KVKK m.12/2 · ISAE 3402 · IL-X-05
V-10 İhlal müdahalesi ve bildirim HÜKÜM Veri ihlali öğrenildiği andan itibaren kayda alınır, 72 saat içinde Kurula ve makul sürede ilgili kişilere bildirilir; kök neden analizi yapılır.	GEREKÇE Bildirim süresi kanunîdir; geç bildirim ihlalin kendisinden bağımsız yaptırım doğurur.	KVKK m.12/5 · Kurul kararı 2019/10

IK-PL-03 · v1.0 · İlkeler II

Şekil 7 Veri koruma ilkeleri II — V-06...V-10: hüküm, gerekçe ve kaynak

V-01 Hukuka ve dürüstlük kurallarına uygunluk

Hüküm. Çalışan verisi yalnızca Kanunda sayılan işleme şartlarından birine dayanarak ve ilgili kişinin makul beklentisine uygun biçimde işlenir; iş ilişkisindeki güç dengesizliği nedeniyle açık rıza son çaredir.

Gerekçe ve uygulama sonucu. İş ilişkisinde rıza özgür iradeyi tam yansıtmaz; işleme, sözleşmenin ifası veya kanunî yükümlülük gibi rızaya bağlı olmayan şartlara dayandırılır. Bu ilke KVKK m.4/2-a, m.5/2 · Kurul rehberi referansına dayanır; Bölüm 7'deki uygulama esaslarında kural, kontrol noktası veya kayıt olarak somutlaşır ve ilkeye aykırı her işleme Bölüm 8 anlamında istisna değil Bölüm 9 anlamında ihlaldir.

V-02 Doğru ve güncel

Hüküm. Çalışan verisi doğru ve gerektiğinde güncel tutulur; kayıt sahibi sistem tektir, kopya ortamlar mutabakatla doğrulanır.

Gerekçe ve uygulama sonucu. Yanlış veri yanlış bordro, yanlış bildirim ve yanlış karar üretir; tek kayıt sahibi sistem doğruluğun ön koşuludur. Bu ilke KVKK m.4/2-b · IL-X-01 referansına dayanır; Bölüm 7'deki uygulama esaslarında kural, kontrol noktası veya kayıt olarak somutlaşır ve ilkeye aykırı her işleme Bölüm 8 anlamında istisna değil Bölüm 9 anlamında ihlaldir.

V-03 Belirli, açık ve meşru amaç

Hüküm. Her veri kategorisinin işleme amacı veri envanterinde yazılıdır; amaç dışı kullanım ve amaçla bağdaşmayan yeni işleme yasaktır.

Gerekçe ve uygulama sonucu. Amaç yazılı olmadan ölçülülük ve süre sınırı değerlendirilemez; envanter, amacı denetlenebilir kılar. Bu ilke KVKK m.4/2-c · m.16 referansına dayanır; Bölüm 7'deki uygulama esaslarında kural, kontrol noktası veya kayıt olarak somutlaşır ve ilkeye aykırı her işleme Bölüm 8 anlamında istisna değil Bölüm 9 anlamında ihlaldir.

V-04 Amaçla bağlantılı, sınırlı ve ölçülü

Hüküm. Yalnızca amacın gerektirdiği veri, gerektirdiği kapsamda toplanır; 'ileride gerekebilir' gerekçesiyle veri toplanmaz.

Gerekçe ve uygulama sonucu. Fazla veri fazla risk demektir; toplanmayan veri sızdırılmaz ve saklanmak zorunda değildir. Bu ilke KVKK m.4/2-ç · Veri minimizasyonu referansına dayanır; Bölüm 7'deki uygulama esaslarında kural, kontrol noktası veya kayıt olarak somutlaşır ve ilkeye aykırı her işleme Bölüm 8 anlamında istisna değil Bölüm 9 anlamında ihlaldir.

V-05 Süre ile sınırlı saklama

Hüküm. Her veri kategorisi için saklama süresi tablosu yazılıdır; süre sonunda veri periyodik imha döneminde tutanakla imha edilir.

Gerekçe ve uygulama sonucu. Süresi dolan verinin tutulması başlı başına ihlaldir; saklama tablosu imhayı zorunlu ve kanıtlanabilir kılar. Bu ilke KVKK m.4/2-d, m.7 · Yönetmelik referansına dayanır; Bölüm 7'deki uygulama esaslarında kural, kontrol noktası veya kayıt olarak somutlaşır ve ilkeye aykırı her işleme Bölüm 8 anlamında istisna değil Bölüm 9 anlamında ihlaldir.

V-06 Görev gereği erişim

Hüküm. Çalışan verisine erişim rol–yetki matrisiyle ve görev gereği ilkesiyle verilir; ayrıcalıklı erişimler isim bazında listelenir ve yılda bir gözden geçirilir.

Gerekçe ve uygulama sonucu. Yetkisiz iç erişim en sık ihlal kaynağıdır; matris ve yıllık gözden geçirme erişimi görünür ve hesap verilebilir kılar. Bu ilke KVKK m.12 · ISO 27001 A.5.15 · IL-X-07 referansına dayanır; Bölüm 7'deki uygulama esaslarında kural, kontrol noktası veya kayıt olarak somutlaşır ve ilkeye aykırı her işleme Bölüm 8 anlamında istisna değil Bölüm 9 anlamında ihlaldir.

V-07 Özel nitelikli veri ayrı

Hüküm. Sağlık, sendika, ceza mahkûmiyeti ve biyometrik veriler özlük dosyasından ayrı, kilitli veya şifreli ortamda ve isim bazlı erişimle tutulur; Kurulun belirlediği ek tedbirler uygulanır.

Gerekçe ve uygulama sonucu. Özel nitelikli verinin ifşası kişiye telafisi güç zarar verir ve en yüksek idari yaptırıma tabidir. Bu ilke KVKK m.6 · Kurul kararı 2018/10 referansına dayanır; Bölüm 7'deki uygulama esaslarında kural, kontrol noktası veya kayıt olarak somutlaşır ve ilkeye aykırı her işleme Bölüm 8 anlamında istisna değil Bölüm 9 anlamında ihlaldir.

V-08 Aydınlatma ve şeffaflık

Hüküm. İşleme faaliyeti başlamadan önce ilgili kişi aydınlatılır; aydınlatma metni işe girişte imzalı tebliğ edilir ve envanter değişikliğinde güncellenir.

Gerekçe ve uygulama sonucu. Aydınlatılmamış işleme hukuka aykırıdır; şeffaflık çalışan güveninin ve ilgili kişi haklarının temelidir. Bu ilke KVKK m.10 · Aydınlatma Tebliği referansına dayanır; Bölüm 7'deki uygulama esaslarında kural, kontrol noktası veya kayıt olarak somutlaşır ve ilkeye aykırı her işleme Bölüm 8 anlamında istisna değil Bölüm 9 anlamında ihlaldir.

V-09 Veri işleyen sorumluluğu

Hüküm. Çalışan verisi işleyen her hizmet sağlayıcıyla veri işleyen sözleşmesi imzalanır; sağlayıcı yalnızca talimatla işler; sorumluluk Şirkette kalır.

Gerekçe ve uygulama sonucu. Hizmet devredilir, sorumluluk devredilmez; sözleşme olmadan sağlayıcının işlemesi Şirketin ihlalidir. Bu ilke KVKK m.12/2 · ISAE 3402 · IL-X-05 referansına dayanır; Bölüm 7'deki uygulama esaslarında kural, kontrol noktası veya kayıt olarak somutlaşır ve ilkeye aykırı her işleme Bölüm 8 anlamında istisna değil Bölüm 9 anlamında ihlaldir.

V-10 İhlal müdahalesi ve bildirim

Hüküm. Veri ihlali öğrenildiği andan itibaren kayda alınır, 72 saat içinde Kurula ve makul sürede ilgili kişilere bildirilir; kök neden analizi yapılır.

Gerekçe ve uygulama sonucu. Bildirim süresi kanunîdir; geç bildirim ihlalin kendisinden bağımsız yaptırım doğurur. Bu ilke KVKK m.12/5 · Kurul kararı 2019/10 referansına dayanır; Bölüm 7'deki uygulama esaslarında kural, kontrol noktası veya kayıt olarak somutlaşır ve ilkeye aykırı her işleme Bölüm 8 anlamında istisna değil Bölüm 9 anlamında ihlaldir.

5.2 Alt süreç ilkeleri

Aşağıdaki ilkeler D.03, D.04 ve L.05 alt süreçlerine özgüdür; Evren'in IL-D03, IL-D04 ve IL-L05 ilke envanteriyle birebirdir ve ilgili kontrol noktalarıyla izlenir.

Yönetişim İlkeleri

Bu politikanın düzenlediği üç alt sürece özgü ilkeler — alt süreç başına iki ilke

D.03 Erişim ve yetki yönetimi	
IL-D03-1 ISO 27001 · A.5.15-5.18 Erişimler rol-yetki matrisine göre verilir; ücret ve bordro verisine erişim isim bazında listelenir ve yılda bir gözden geçirilir.	IL-D03-2 ISO 27001 · A.5.18 Ayrılan çalışanın tüm erişimleri son çalışma gününü izleyen 1 iş günü içinde kapatılır; kapatma kaydı ayrılış kontrol listesine eklenir.
D.04 Kişisel veri koruma (çalışan verisi)	
IL-D04-1 KVKK m.16 · VERBİS Çalışan veri envanteri işleme amacı, hukuki sebep, saklama süresi ve aktarılan tarafları alan bazında gösterir; yılda bir güncellenir.	IL-D04-2 KVKK m.6 · Kurul kararları Sağlık raporu ve benzeri özel nitelikli veriler özlük dosyasından ayrı, kilitli veya şifreli ortamda ve isim bazlı erişimle tutulur.
L.05 Arşivleme, saklama ve alumni ilişkisi	
IL-L05-1 KVKK m.7 · İş K. · SGK mevzuatı Belge türü bazında saklama süresi tablosu yazılıdır; süre sonunda imha tutanakla yapılır.	IL-L05-2 KVKK m.5, m.12 Arşiv erişimi kısıtlı ve kayıtlıdır; alumni iletişimi ayrı rızaya dayanır.

IK-PL-03 · v1.0 · Yönetişim İlkeleri

Şekil 8 Alt süreç ilkeleri — üç alt süreç, altı ilke

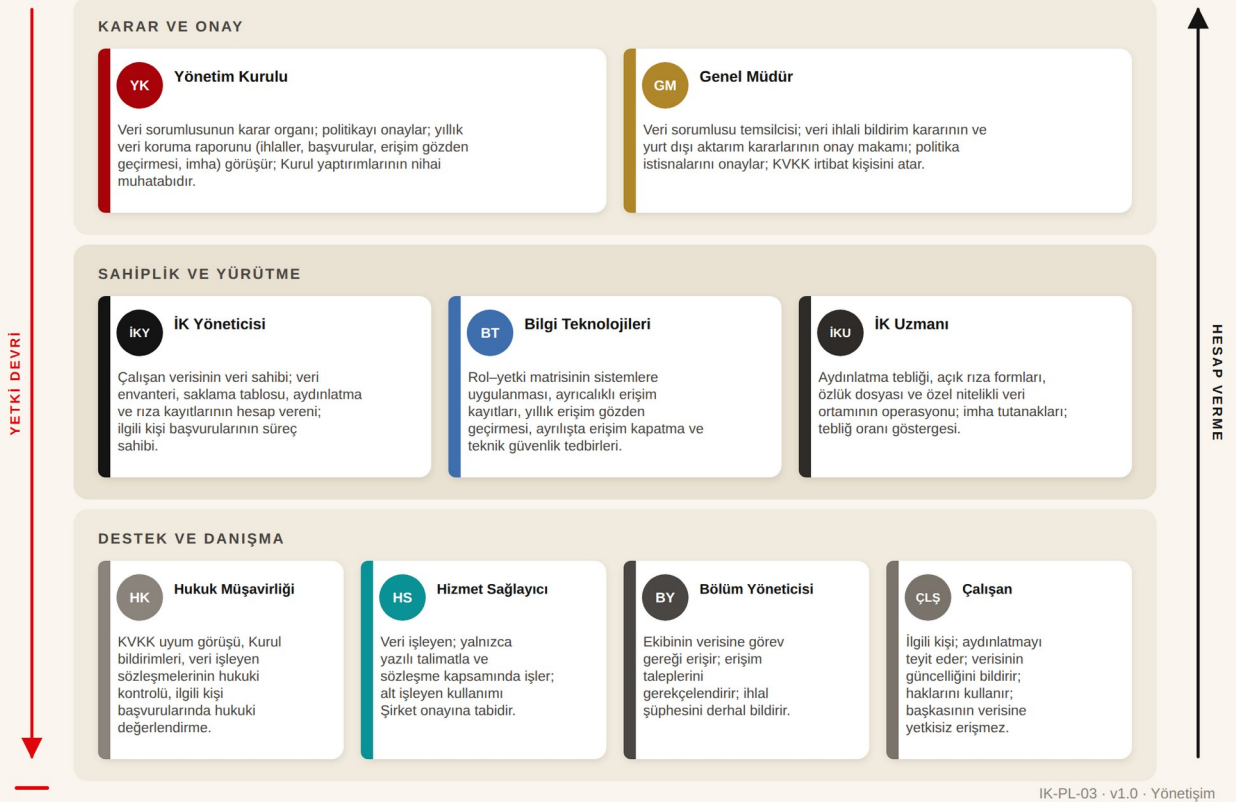
Erişim, rol-yetki matrisiyle verilir ve ayrılıştaki bir iş günü içinde kapatılır. Veri envanteri her kategorinin amacını, hukuki sebebini, süresini ve aktarılan taraflarını gösterir ve yılda bir güncellenir; özel nitelikli veri özlük dosyasından ayrı tutulur. Saklama süresi tablosu belge türü bazında yazılıdır; imha tutanaklıdır; arşiv erişimi kısıtlı ve kayıtlıdır; alumni iletişimi ayrı rızaya dayanır.

6 Roller ve sorumluluklar

Veri koruma yönetiřimi IK-PL-01'deki üç katmanlı yapıyı izler. Veri sorumlusu řirkettir; Yönetim Kurulu veri sorumlusunun karar organı, Genel Müdür veri sorumlusu temsilcisidir. Çalışan verisinin veri sahibi İK Yöneticisidir; Bilgi Teknolojileri teknik tedbirlerin ve erişim altyapısının sahibidir. Sorumluluk devredilmez; işleme yetkisi rol-yetki matrisi ve veri işleyen sözleşmeleriyle yazılı olarak devredilir.

Yönetişim Haritası

Üç katman · dokuz rol · veri sorumlusu řirkettir; sorumluluk devredilmez, işleme yetkisi yazılı devredilir



Şekil 9 Yönetişim haritası — üç katman, dokuz rol ve işleme yetkisinin akışı

Yönetim Kurulu politikayı onaylar; yıllık veri koruma raporunu (ihlaller, ilgili kişi başvuruları, erişim gözden geçirmesi, imha, denetim bulguları) görüşür; Kurul yaptırımlarının nihai muhatabıdır. Genel Müdür, veri ihlali bildirim kararının ve yurt dışı aktarım kararlarının onay makamıdır; politika istisnalarını onaylar; KVKK irtibat kişisini ve veri koruma sorumlusunu atar.

İK Yöneticisi çalışan verisinin veri sahibidir; veri envanteri, saklama tablosu, aydınlatma ve rıza kayıtları, ilgili kişi başvuruları ve ihlal kaydı İK Yöneticisinin hesap verdiği kayıtlardır. Bilgi Teknolojileri rol-yetki matrisini sistemlere uygular, ayrıcalıklı erişim kayıtlarını tutar, yıllık erişim gözden geçirmesini (KN-20) ve ayrışta erişim kapatmayı (KN-21) yürütür, teknik güvenlik tedbirlerini (şifreleme, loglama, yedekleme, uç nokta güvenliği) işletir. İK Uzmanı aydınlatma tebliğini, rıza formlarını, özlük dosyası ve özel nitelikli veri ortamını, imha tutanaklarını yürütür.

Hukuk Müşavirliği KVKK uyum görüşünü verir, Kurul bildirimlerini hazırlar, veri işleyen sözleşmelerini kontrol eder ve ilgili kişi başvurularında hukuki değerlendirmeyi yapar. Hizmet sağlayıcılar veri işleyendir; yalnızca yazılı talimatla ve sözleşme kapsamında işler; alt işleyen kullanımı řirket onayına tabidir. Bölüm Yöneticileri ekiplerinin verisine görev gereği erişir, erişim taleplerini gerekçelendirir ve ihlal şüphesini derhal bildirir. Çalışan ilgili kişidir; aydınlatmayı teyit eder, verisinin güncelliğini bildirir, haklarını kullanır ve başkasının verisine yetkisiz erişmez.

RACI Matrisi

A hesap veren · R sorumlu · C danışılan · I bilgilendirilen — her satırda tek A

	YK	GM	İKY	BT	İKU	HK	HS	BY	ÇLŞ
D.03 Erişim ve yetki yönetimi		I	A	R			C	I	
D.04 Kişisel veri koruma (çalışan verisi)		I	A	C	R	C			I
L.05 Arşivleme, saklama ve alumnı			A	C	R	C			
— Veri ihlali müdahalesi ve bildirim		I	A	R	R		C	C	
— İlgili kişi başvurusu (30 gün)			A	C	R	C			I
— Veri işleyen sözleşmesi ve yurt dışı aktarım			A	R	C		C	I	

A Hesap veren **R** Sorumlu **C** Danışılan **I** Bilgilendirilen

IK-PL-03 · v1.0 · RACI

Şekil 10 RACI matrisi — düzenlenen alt süreçler, ihlal müdahalesi, ilgili kişi başvurusu ve aktarım

RACI matrisinde her satırda tek bir hesap veren (A) bulunur. Veri ihlali müdahalesinde hesap veren Genel Müdürdür; İK Yöneticisi ve Bilgi Teknolojileri birlikte sorumludur (R). Matrisin sistem bazlı ayrıntısı BT rol–yetki matrisinde, adım bazlı ayrıntısı IK-PR-07, IK-PR-08 ve IK-PR-16'da yer alır; bu politikadaki matris yönetim düzeyinde bağlayıcıdır.

7 Uygulama esasları

Uygulama esasları sekiz alt bölümde düzenlenir: veri sınıflandırması, veri envanteri ve hukuki sebepler, veri yaşam döngüsü, erişim ve yetki yönetimi, aktarım ve veri işleyenler, ilgili kişi hakları, veri ihlali müdahalesi ile yıllık takvim, kontrol noktaları ve göstergeler. Esaslar Kanunun veri sorumlusuna yüklediği teknik ve idari tedbirlerin çalışan verisi özelindeki karşılığıdır.

7.1 Veri sınıflandırması

Veri Sınıflandırma Katmanları

Dört sınıf · en dar tepe özel nitelikli veri · sınıf yükseldikçe erişim daralır, koruma artar



İK-PL-03 · v1.0 · Veri sınıfları

Şekil 11 Veri sınıflandırma katmanları — dört sınıf, erişim ilkesi ve kural

Çalışan verisi dört sınıfta işlenir: GENEL (kurum içi rehber niteliğindeki veri), DAHİLİ (özlük, iletişim, organizasyon ve eğitim verisi), GİZLİ (ücret, banka, performans ve disiplin verisi) ve ÖZEL NİTELİKLİ (sağlık, sendika, ceza mahkûmiyeti, biyometrik veri). Sınıf yükseldikçe erişim daralır ve koruma tedbiri artar: GİZLİ veriye erişim isim bazlı ayrıcalıklı erişim listesiyle; ÖZEL NİTELİKLİ veriye erişim yalnızca İK Yöneticisi ve iş yeri hekimi ile sınırlı, ayrı ve şifreli veya kilitli ortamda, erişim kaydı tutularak sağlanır. Bir kaydın sınıfı içerdiği en yüksek sınıflı veriyle belirlenir.

7.2 Veri envanteri ve hukuki sebepler

Çalışan Veri Envanteri — Kategoriler

Kategori · hukuki sebep · saklama süresi · erişim sınıfı — ayrıntılı envanter VERBİS kaydı ve IK-PR-08 saklama tablosuyla birebirdir

K1	Kimlik ve iletişim verisi Hukuki sebep: kanunî yükümlülük (İş K., 5510) · Saklama: iş ilişkisi + 10 yıl Ad-soyad, T.C. kimlik no, doğum bilgileri, adres, telefon, acil durum kişisi; nüfus kayıt örneği yalnızca gerekli alanlarla.	DAHİLİ
K2	Özlük ve sözleşme verisi Hukuki sebep: sözleşmenin ifası, kanunî yükümlülük · Saklama: iş ilişkisi + 10 yıl İş sözleşmesi, özlük dosyası belgeleri, görev ve unvan geçmişi, eğitim ve sertifikalar, referans kayıtları.	DAHİLİ
K3	Ücret, bordro ve banka verisi Hukuki sebep: sözleşmenin ifası, kanunî yükümlülük (GVK, 5510) · Saklama: 10 yıl (VUK, 5510) Ücret, prim, yan hak, banka hesabı, icra ve nafaka kesintileri, bordro ve tahakkuk kayıtları.	GİZLİ
K4	Performans, disiplin ve şikâyet verisi Hukuki sebep: meşru menfaat, kanunî yükümlülük (İş K.) · Saklama: iş ilişkisi + 10 yıl (dava zamanasımı) Hedef kartları, değerlendirme sonuçları, gelişim planları, disiplin kararları, savunmalar, şikâyet kayıtları.	GİZLİ
K5	Sağlık verisi (özel nitelikli) Hukuki sebep: 6331 sayılı Kanun (iş yeri hekimi), açık rıza (diğer) · Saklama: 15 yıl (sağlık gözetimi) / iş ilişkisi + 10 yıl İşe giriş ve periyodik muayene raporları, istirahat raporları, engellilik, gebelik, meslek hastalığı kayıtları; yalnızca iş yeri hekimi ve İKY.	ÖZEL NİTELİKLİ
K6	Sendika, ceza mahkûmiyeti ve biyometrik veri (özel nitelikli) Hukuki sebep: kanunî yükümlülük (sendika kesintisi), açık rıza (adli sicil, biyometrik) · Saklama: amaçla sınırlı Sendika üyeliği ve aidat kesintisi; adli sicil kaydı yalnızca kanunen zorunlu pozisyonlarda; biyometrik PDKS yalnızca alternatif sunularak ve açık rızayla.	ÖZEL NİTELİKLİ
K7	Dijital izler ve görüntü verisi Hukuki sebep: meşru menfaat (güvenlik, iş sürekliliği); aydınlatma zorunlu · Saklama: kamera 30 gün, log 2 yıl (5651) Kamera kayıtları, sistem erişim logları, kurumsal e-posta ve cihaz kullanımı, araç takip; izleme ölçülü ve önceden bildirilmiş.	DAHİLİ
K8	Aday ve alumni verisi Hukuki sebep: sözleşme öncesi işlem (aday), açık rıza (havuz, alumni) · Saklama: aday 6 ay / rıza ile 2 yıl; alumni rıza süresince Özgeçmiş, mülakat notları, test sonuçları; alumni iletişim bilgileri ve etkinlik kayıtları.	DAHİLİ

IK-PL-03 · v1.0 · Veri envanteri

Şekil 12 Çalışan veri envanteri — sekiz kategori, hukuki sebep, saklama süresi ve erişim sınıfı

Veri envanteri, işlenen her çalışan veri kategorisi için amacı, hukuki sebebi, saklama süresini, aktarılan tarafları, kayıt sahibi sistemi ve erişim sınıfını gösterir; VERBİS kaydıyla ve IK-PR-08 saklama tablosuyla birebirdir ve her yıl Mart ayında güncellenir. İş ilişkisinde işleme, kural olarak sözleşmenin ifası, kanunî yükümlülük veya meşru menfaat şartlarına dayandırılır; açık rıza yalnızca bu şartların bulunmadığı işlemlerde (aday havuzu, alumni, fotoğraf, biyometrik PDKS) ve alternatifi sunularak alınır. Rızaya dayanan işlemede rızanın geri alınması işlemeyi durdurur ve çalışan için aleyhe sonuç doğurmaz.

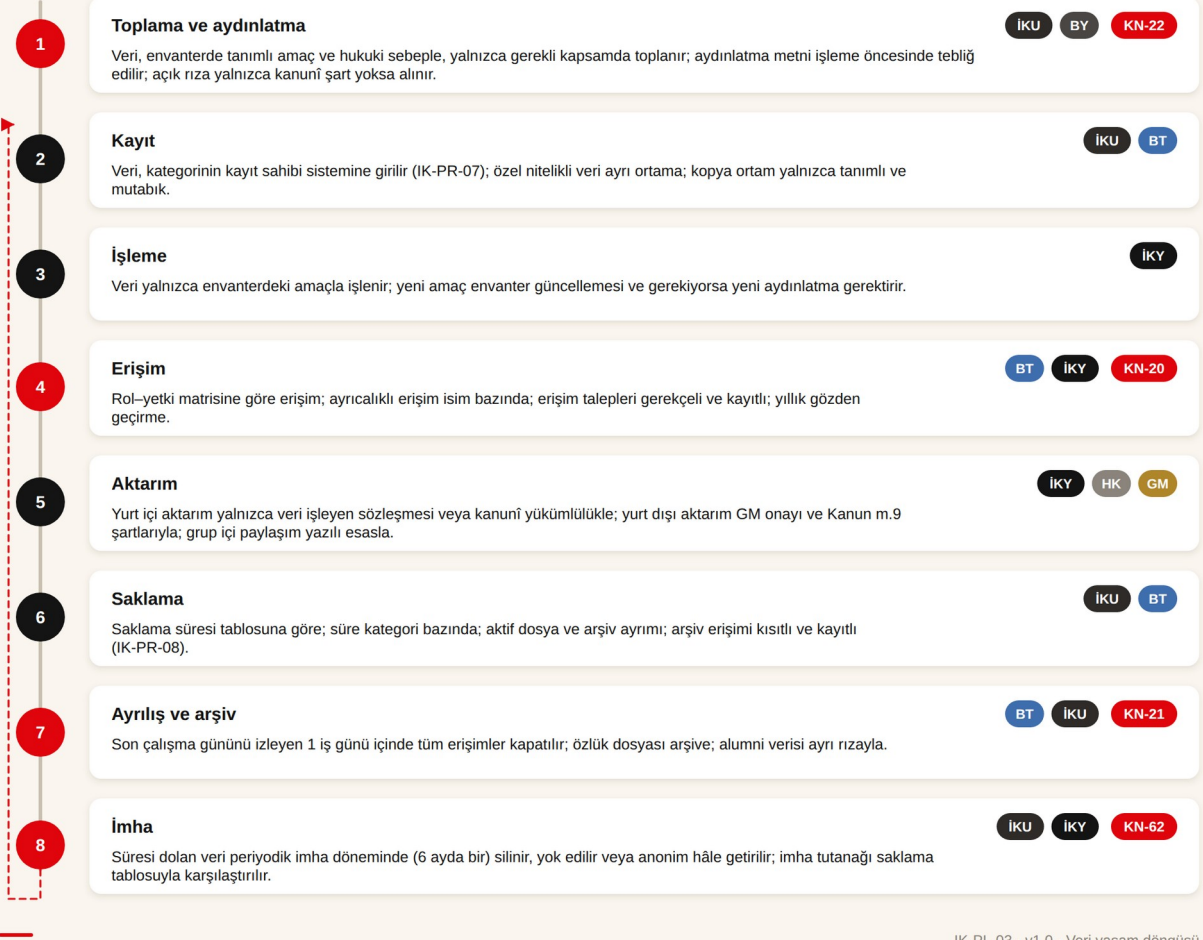
HÜKÜM

Envanterde yer almayan bir veri kategorisi işlenemez; yeni bir kategori, sistem veya izleme uygulaması ancak envanter güncellemesi, gerekiyorsa etki değerlendirmesi ve yeni aydınlatma ile işlemeye alınır. Özel nitelikli veri için Kanun m.6 şartları ve Kurulun belirlediği ek tedbirler sağlanmadan işleme başlatılmaz.

7.3 Veri yaşam döngüsü

Çalışan Verisi Yaşam Döngüsü

Sekiz adım · sorumlu · kırmızı rozet = kontrol noktası · her adımın kaydı ve dayanağı vardır



IK-PL-03 · v1.0 · Veri yaşam döngüsü

Şekil 13 Çalışan verisi yaşam döngüsü — sekiz adım, sorumlu ve kontrol noktası

Her veri kategorisi toplama, kayıt, işleme, erişim, aktarım, saklama, ayrılış–arşiv ve imha adımlarından oluşan aynı döngüden geçer; her adımın sorumlusu, kaydı ve dayanağı vardır. Toplama adımında aydınlatma metni işleme öncesinde tebliğ edilir (işe girişte IK-PR-06, adaylıkta IK-PR-05); kayıt adımında veri yalnızca kategorinin kayıt sahibi sistemine girilir ve kopya ortam yalnızca tanımlı ve mutabık olabilir (IK-PR-07). Saklama, kategori bazında saklama süresi tablosuna göre yapılır; aktif dosya ile arşiv ayrılır ve arşiv erişimi kısıtlı ve kayıtlıdır (IK-PR-08).

Ayrılışta tüm erişimler son çalışma gününü izleyen bir iş günü içinde kapatılır (KN-21, KPI-15) ve özlük dosyası arşive alınır; alumni ilişkisi yalnızca ayrı ve açık rızayla sürdürülür. Saklama süresi dolan veri altı ayda bir yürütülen periyodik imha döneminde silinir, yok edilir veya anonim hâle getirilir; imha tutanağı saklama tablosuyla karşılaştırılır (KN-62). Yasal saklama süresi dolmadan imha yapılmaz; hukuki ihtilaf, denetim veya soruşturma hâlinde saklama süresi Bölüm 8'e göre istisna kaydıyla uzatılır.

7.4 Erişim ve yetki yönetimi

Erişim Matrisi — Veri Sınıfı × Rol

T = tam (yazma) · O = okuma · S = sınırlı (yalnızca kendi ekibi / kendi verisi) · — = erişim yok · ayrıcalıklı erişimler isim bazında

VERİ KATEGORİSİ	ROL						
	İKY	İKÜ	BT	FM	BY	HS	ÇLŞ
Kimlik ve iletişim	T	T	S	O	S	O	S
Özlük ve sözleşme	T	T	—	—	S	—	S
Ücret, bordro ve banka	T	O	—	T	—	O	S
Performans ve disiplin	T	O	—	—	S	—	S
Sağlık (özel nitelikli)	O	S	—	—	—	—	S
Sendika · ceza · biyometrik	T	S	—	S	—	S	S
Dijital izler ve görüntü	S	—	T	—	—	—	S

BT sistem yöneticisi erişimi teknik yönetim amaçlıdır ve içerik erişimi loglanır; hizmet sağlayıcı (HS) erişimi veri işleyen sözleşmesi kapsamında sınırlıdır; sağlık verisinde iş yeri hekimi tam erişime sahiptir (matris dışı, 6331). Matrisin sistem bazlı ayrıntısı BT rol–yetki matrisinde tutulur ve yılda bir bu politikayla mutabık kılınır (KN-20).

İK-PL-03 · v1.0 · Erişim matrisi

Şekil 14 Erişim matrisi — veri kategorisi × rol, erişim düzeyi

Çalışan verisine erişim rol–yetki matrisiyle ve görev gereği ilkesiyle verilir: her rol, görevi için gerekli veri kategorisine, gerekli düzeyde (tam, okuma, sınırlı) ve gerekli süreyle erişir. Bölüm Yöneticisi yalnızca kendi ekibinin DAHİLİ verisine ve performans kayıtlarına erişir; ücret verisine erişimi yalnızca yıllık artış döngüsünde ve kendi ekibiyle sınırlıdır. Ücret, bordro, sağlık ve sistem yönetimi erişimleri ayrıcalıklı erişimdir; isim bazında listelenir, gerekçelidir ve yılda bir Bilgi Teknolojileri ile İK Yöneticisinin imzaladığı raporla gözden geçirilir (KN-20).

Erişim talepleri yazılı ve gerekçelidir; matris dışı erişim Bölüm 8'e göre süreli istisnadır ve BT tarafından süre sonunda otomatik kapatılır. Paylaşılan hesap kullanılmaz; her erişim kişisel hesapla ve loglanarak yapılır; GİZLİ ve ÖZEL NİTELİKLİ veriye erişim logları en az iki yıl saklanır ve olağan dışı erişim BT tarafından İK Yöneticisine raporlanır. Veri, kişisel cihaza, kişisel e-postaya veya onaysız bulut ortamına aktarılmaz; taşınabilir ortamda yalnızca şifreli taşınır.

7.5 Aktarım ve veri işleyenler

Yurt içi aktarım yalnızca kanunî yükümlülük (SGK, vergi, mahkeme, icra) veya veri işleyen sözleşmesi kapsamında yapılır. Çalışan verisi işleyen her hizmet sağlayıcıyla (bordro, sağlık, sigorta, yazılım, arşiv) Kanun m.12 ve Kurul kararlarına uygun veri işleyen sözleşmesi imzalanır; sözleşme işleme amacını, talimat esasını, gizlilik ve güvenlik tedbirlerini, alt işleyen onayını, ihlal bildirim süresini (24 saat), denetim hakkını ve sözleşme sonunda iade–imha yükümlülüğünü içerir. Sağlayıcıdan yıllık güvence raporu (ISAE 3402 veya ISO 27001 belgesi) alınır; hizmet yönetimi İK-PR-03'e tabidir.

Yurt dışı aktarım (grup şirketi, bulut hizmeti, küresel yazılım) yalnızca Kanun m.9 şartlarıyla, Hukuk Müşavirliği görüşü ve Genel Müdür onayıyla yapılır; aktarım envantere işlenir ve aydınlatma metninde belirtilir. Grup içi paylaşım yazılı esasa bağlıdır ve yalnızca gerekli alanlarla sınırlıdır (F.05 maliyet yansıtmasında kimlik ve tutar düzeyinde). Referans talepleri çalışanın yazılı rızasıyla ve yalnızca görev–unvan–tarih bilgisiyle yanıtlanır.

7.6 İlgili kişi hakları

İlgili Kişi Hakları ve Yanıt Süreleri

KVKK m.11 · başvuru İK Yöneticisine yazılı veya kayıtlı elektronik kanalla · yanıt en geç 30 gün · ücretsiz

H1	Öğrenme ve bilgi talep etme Yanıt: 30 gün · Kanal: yazılı / KEP / kurumsal e-posta Kişisel verisinin işlenip işlenmediğini öğrenme; işlenmişse amaç, kapsam ve aktarılan taraflar hakkında bilgi talep etme.	İKY
H2	Erişim ve kopya alma Yanıt: 30 gün · Kimlik doğrulaması sonrası Kendisine ait verilere erişme ve kopyasını alma; üçüncü kişi verisi içeren kayıtlar maskelenerek verilir.	İKY İKU
H3	Düzeltilme Yanıt: 30 gün · Kayıt sahibi sistemde ve kopyalarda Eksik veya yanlış işlenen verinin düzeltilmesini isteme; düzeltme aktarılan taraflara bildirilir (İK-PR-07).	İKU BT
H4	Silme ve yok etme Yanıt: 30 gün · Saklama süresi ve kanunî yükümlülük saklıdır İşleme şartlarının ortadan kalkması hâlinde silinmesini isteme; yasal saklama süresi dolmamış veri için ret gerekçeli yazılır.	İKY HK
H5	Aktarılan taraflara bildirim Yanıt: 30 gün Düzeltilme ve silme işlemlerinin verinin aktarıldığı üçüncü kişilere bildirilmesini isteme.	İKU
H6	Otomatik işlemeye itiraz Yanıt: 30 gün · İnsan müdahalesi güvencesi Münhasıran otomatik sistemlerle analiz sonucu aleyhe bir sonucun ortaya çıkmasına itiraz etme; İK kararlarında nihai karar insan tarafından verilir.	İKY
H7	Zararın giderilmesi Yanıt: 30 gün · Hukuki değerlendirme Hukuka aykırı işleme nedeniyle uğranan zararın giderilmesini talep etme; Hukuk Müşavirliği değerlendirir.	HK GM
H8	Kurula şikâyet Başvuru reddi veya 30 günde yanıtızlık hâlinde Şirkete başvurunun reddedilmesi, yetersiz bulunması veya süresinde yanıt verilmemesi hâlinde Kişisel Verileri Koruma Kuruluna şikâyet hakkı; başvuru yanıtında bu hak hatırlatılır.	—

İK-PL-03 · v1.0 · İlgili kişi hakları

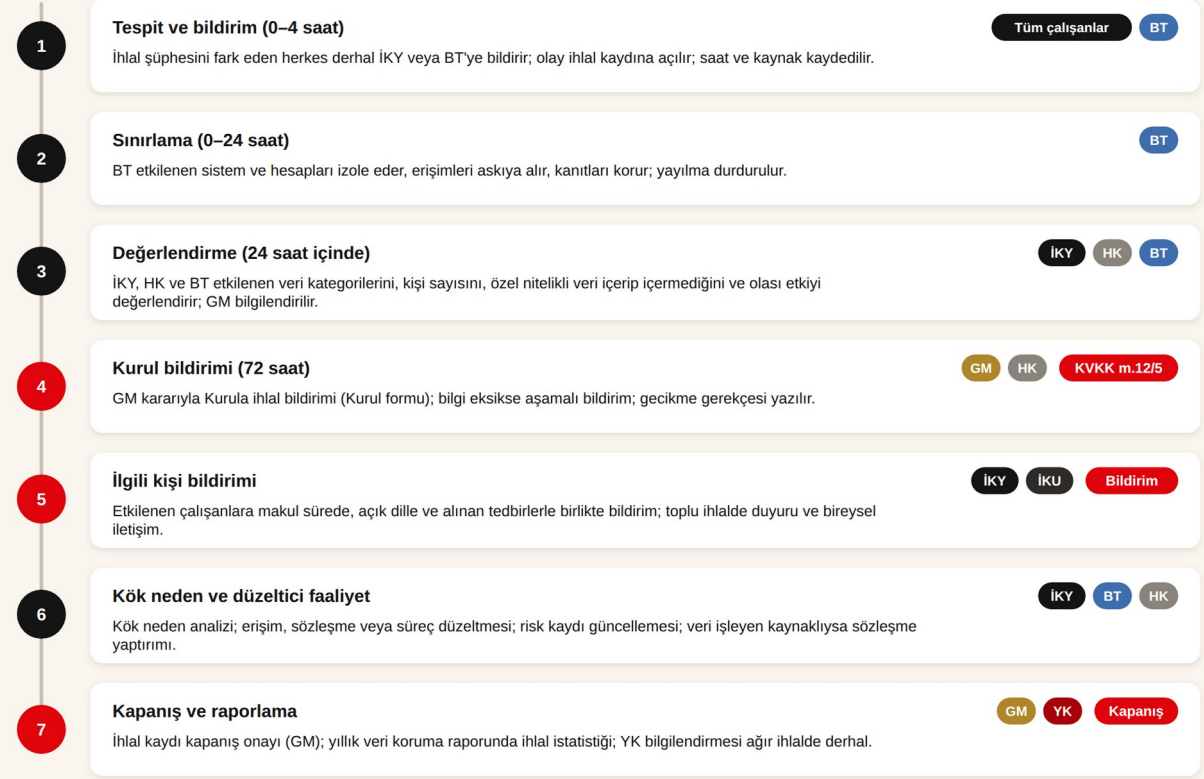
Şekil 15 İlgili kişi hakları ve yanıt süreleri — sekiz hak, kanal ve sorumlu

Çalışan, Kanun m.11'deki haklarını İK Yöneticisine yazılı olarak veya kayıtlı elektronik kanalla ücretsiz kullanır; başvuru, kimlik doğrulaması sonrasında en geç 30 gün içinde yazılı olarak yanıtlanır. Ret hâlinde gerekçe ve Kurula şikâyet hakkı yazılır. Başvuru kayıtları İK Yöneticisi tarafından tutulur; yanıt süreleri yıllık veri koruma raporunda özetlenir. Başvuru nedeniyle çalışana aleyhe işlem yapılamaz.

7.7 Veri ihlali müdahalesi

Veri İhlali Müdahale Akışı

Öğrenme anından kapanışa · 72 saat Kurul bildirim · kırmızı rozet = kontrol / bildirim noktası



İK-PL-03 · v1.0 · İhlal müdahalesi

Şekil 16 Veri ihlali müdahale akışı — yedi adım, 72 saat Kurul bildirim

Veri ihlali şüphesini fark eden herkes derhal İK Yöneticisine veya Bilgi Teknolojilerine bildirir; olay ihlal kaydına açılır. Bilgi Teknolojileri yayılmayı durdurur ve kanıtı korur; İK Yöneticisi, Hukuk Müşavirliği ve Bilgi Teknolojileri 24 saat içinde etkilenen veri kategorilerini, kişi sayısını ve olası etkiyi değerlendirir. Genel Müdür kararıyla Kurula bildirim öğrenme anından itibaren en geç 72 saat içinde yapılır; etkilenen çalışanlara makul sürede açık dille bildirimde bulunulur. Kök neden analizi, düzeltici faaliyet ve risk kaydı güncellemesi kapanış koşuludur; yılda bir ihlal tatbikatı yapılır.

7.8 Yıllık takvim, kontrol noktaları ve göstergeler

Yıllık Veri Koruma Takvimi

Ay bazında sabit olaylar · sorumlu · kırmızı = Yönetim Kurulu / Genel Müdür kararı

Oca	Periyodik imha dönemi I: saklama süresi dolan kayıtların imhası ve tutanağı (KN-62); kamera ve log saklama kontrolü	İKU · BT
Şub	Veri işleyen sözleşmeleri envanteri; alt işleyen listesi teyidi; sağlayıcı güvence raporlarının (ISAE 3402 / ISO 27001) alınması	İKY · HK · HS
Mar	Veri envanteri ve VERBİS kaydı yıllık güncellemesi; saklama tablosu güncellemesi; politika yıllık gözden geçirmesi	İKY · HK
Nis	Aydınlatma metni ve rıza formlarının güncel sürümüyle yıllık tebliğ; imza oranı %100 hedefi (KPI-50)	İKU · BY
May	Yıllık erişim gözden geçirmesi: rol-yetki matrisi ve ayrıcalıklı erişim listesi imzalı raporu (KN-20)	BT · İKY
Haz	Özel nitelikli veri ortamı denetimi: ayrı saklama, şifreleme, erişim kaydı kontrol listesi (KN-22)	İKY · BT
Tem	Periyodik imha dönemi II; arşiv erişim kayıtlarının gözden geçirilmesi	İKU · BT
Ağu	Veri koruma farkındalık eğitimi (tüm çalışanlar); İK ve BT için ileri düzey eğitim; ihlal tatbikatı	İKY · BT
Eyl	İlgili kişi başvuru kayıtları ve yanıt sürelerinin analizi; aday havuzu ve alumni rıza sürelerinin kontrolü	İKU · HK
Eki	Kamera, PDKS, log ve izleme uygulamalarının ölçülülük gözden geçirmesi; yeni sistem veya uygulama için etki değerlendirmesi	BT · İKY · HK
Kas	Yıllık veri koruma raporu Yönetim Kurulu gündemi: ihlaller, başvurular, erişim, imha, denetim bulguları; revizyon kararı	YK · GM · İKY
Ara	Yeni yıl saklama tablosu ve imha takvimi; hizmet sağlayıcı sözleşme yenilemeleri; risk kaydı güncellemesi	İKY · HK · FM

IK-PL-03 · v1.0 · Takvim

Şekil 17 Yıllık veri koruma takvimi — ay bazında sabit olaylar ve sorumlular

Güvence Haritası

Dört kontrol noktası (Evren 04_KONTROLLER) · iki gösterge (Evren 05_KPI)

KONTROL NOKTALARI

KN-20 Yıllık erişim gözden geçirmesi

Tespit edici · Sıklık: Yıllık

Kanıt: İmzalı erişim gözden geçirme raporu

BT

KN-21 Ayrılıştaki erişim kapatma (1 iş günü)

Önleyici · Sıklık: İşlem bazlı

Kanıt: Erişim kapatma kaydı (ayrılış kontrol listesi)

BT

KN-22 Özel nitelikli veri ayrı saklama kontrolü

Önleyici · Sıklık: Yıllık

Kanıt: Denetim kontrol listesi; erişim listesi

İKY

KN-62 İmha tutanağı kontrolü

Tespit edici · Sıklık: Yıllık

Kanıt: İmha tutanakları; saklama tablosu karşılaştırması

İKY

GÖSTERGELER

KPI-15

Ayrılıştaki erişim kapatma süresi (iş günü)

Son çalışma günü → erişim kapatma (ortalama)

HEDEF ≤ 1 ↓

Aylık

KPI-50

KVKK aydınlatma ve etik tebliğ imza oranı

İmzalı tebliğ / toplam çalışan

HEDEF %100 ↑

Üç aylık

İK-PL-03 · v1.0 · Güvence

Şekil 18 Güvence haritası — dört kontrol noktası ve iki gösterge

Takvim, tek yıllık İK takviminin (IL-X-08) veri koruma katmanıdır; her olayın sahibi ve kanıtı vardır. Politikanın işletildiğinin kanıtı dört kontrol noktası ve iki göstergedir; tanım, sıklık ve kanıt Evren'in 04_KONTROLLER ve 05_KPI sekmelerinden değiştirilmeden alınır. Ana veri mutabakat farkı (KPI-13) ve dayanaksız ana veri değişikliği (KPI-14) İK-PR-07 kapsamında izlenir ve bu politikanın veri doğruluğu ilkesinin (V-02) göstergeleridir. Göstergeler yıllık veri koruma raporunda hedefle birlikte sunulur; hedefin tutturulamaması gözden geçirme tetikleyicisidir.

8 İstisna ve sapma

İstisna, bu politikanın bir hükmünden tanımlı makamın yazılı onayıyla, süresi ve gerekçesi kayıtlı olarak sapılmasıdır. Veri koruma alanında istisna üç kademedede düzenlenir; kademe, sapmanın derinliğine (sürekli erişim, saklama–aktarım kararı, yapısal işleme değişikliği) ve süresine göre belirlenir. Kanunun emredici hükümleri, veri koruma ilkeleri ve özel nitelikli veri kuralı istisna konusu değildir.

İstisna Merdiveni

Sapmanın derinliği ve süresi kademeyi belirler · yazılı olmayan istisna yoktur · özel nitelikli veri kuralından istisna verilmez

KADEME 3 YK	KAPSAM Yeni özel nitelikli veri kategorisinin işlenmesi (biyometrik, genetik); izleme uygulamalarının kapsam değişikliği; veri envanterinde amaç değişikliği AZAMİ SÜRE Süresiz değil — revizyon KAYIT Politika revizyonu; etki değerlendirmesi; gerekiyorsa Kurul görüşü
KADEME 2 GM	KAPSAM Saklama süresinin uzatılması (hukuki ihtilaf, denetim, soruşturma); yurt dışı aktarım kararı; yeni veri işleyen ile sözleşme öncesi geçici işleme AZAMİ SÜRE 12 ay KAYIT İstisna kaydı; HK görüşü; gerekçe, telafi edici tedbir, bitiş tarihi; YK'ya yıllık raporlanır
KADEME 1 İKY	KAPSAM Sürelili erişim istisnası: proje, denetim veya vekâlet nedeniyle rol-yetki matrisi dışında geçici erişim; kapsam ve süre yazılı; BT uygulamalar AZAMİ SÜRE 30 gün KAYIT İstisna kaydı; erişim kapatma tarihi; BT bilgilendirilir

IK-PL-03 · v1.0 · İstisna

Şekil 19 İstisna merdiveni — üç kademe: makam, kapsam, azami süre ve kayıt

- Yazılı olmayan istisna yoktur; sözlü onayla verilen erişim yetkisiz erişimdir.
- Her istisna kaydı gerekçe, kapsam, telafi edici tedbir, sorumlu ve bitiş tarihi içerir; süresi dolan erişim istisnası BT tarafından otomatik kapatılır.
- Veri koruma ilkelerinden (V-01...V-10) ve özel nitelikli veri kuralından istisna verilmez; Kanunun emredici hükümlerine aykırı talep değerlendirmeye alınmaz.
- Saklama süresi uzatma istisnası yalnızca somut hukuki gerekçeyle ve etkilenen kayıt listesiyle verilir; genel uzatma yapılmaz.
- Açık istisnalar yıllık veri koruma raporunun sabit bölümüdür; Yönetim Kurulu açık istisnaları yılda bir görür.

HÜKÜM

Veri koruma ilkelerinden (V-01...V-10) ve özel nitelikli veri kuralından hiçbir makam istisna veremez. Sözlü onayla verilen erişim yetkisiz erişimdir; erişimi veren ve kullanan için ihlaldir.

İstisna kaydı İK Yöneticisi tarafından tutulur; sürelili erişim istisnaları BT tarafından süre sonunda otomatik kapatılır. Saklama süresi uzatma istisnası etkilenen kayıt listesini ve hukuki gerekçeyi içerir; genel uzatma yapılmaz. Açık istisnalar yıllık veri koruma raporunda Yönetim Kuruluna sunulur.

9 İhlal ve yaptırım

İhlal, politika hükmüne tanımlı bir istisna onayı bulunmaksızın aykırı davranılmasıdır; veri ihlali (Kanun anlamında) ile politika ihlali (bu bölüm anlamında) farklı kavramlardır ve bir veri ihlali her zaman bir politika ihlalden kaynaklanmayabilir. Politika ihlalinin incelenmesi, savunmanın alınması ve yaptırım kararı IK-PL-05 Disiplin Politikası ve IK-PR-15'e göre yürütülür; bu bölüm veri koruma alanına özgü ihlal türlerini kademelere bağlar. Yaptırım orantılıdır ve savunma alınmadan uygulanmaz; Kurul bildirimi ve ilgili kişi bildirimi yaptırım kararından bağımsız olarak süresinde yapılır.

Yaptırım Merdiveni ve Bildirim Kanalı

Dört kademe · orantılılık · savunma alınmadan yaptırım uygulanmaz · yetkisiz erişim ve sızdırma her koşulda ağır ihlaldir



BİLDİRİM KANALI VE KORUMA

KANAL

Veri ihlali şüphesi derhal İKY veya BT'ye; etik bildirim kanalı (IK-PL-04) yetkisiz erişim ve kötüye kullanım için; anonim bildirim kabul edilir.

KORUMA

İhlali bildiren çalışan misillemeye karşı korunur; iyi niyetli yanlış alarm yaptırım doğurmaz.

SÜRE

Şüpheli bildirim anında kayda alınır; değerlendirme 24 saat; Kurul bildirim 72 saat; ilgili kişi bildirim makul sürede; inceleme 30 gün.

KAYIT

İhlal kaydı; tarih, kaynak, etkilenen veri ve kişi sayısı, tedbirler, bildirimler, kök neden, kapanış; yıllık raporda özet.

IK-PL-03 · v1.0 · Yaptırım

Şekil 20 Yaptırım merdiveni ve bildirim kanalı — dört kademe, karar makamı ve koruma esasları

Çalışan verisinin sızdırılması veya satılması, kasıtlı yetkisiz erişim ve ifşa, kayıt tahrifi ve ihlalin gizlenmesi her koşulda ağır ihlaldir ve Hukuk Müşavirliği görüşüyle haklı nedenle fesih kademesinde değerlendirilir; Kanunun cezai hükümleri (TCK m.135–140) saklıdır. Veri işleyen kaynaklı ihlallerde sözleşme yaptırımları (cezai şart, fesih, tazminat) IK-PR-03'e göre uygulanır.

HÜKÜM

İhlali veya ihlal şüphesini bildiren çalışan misillemeye karşı korunur; iyi niyetli yanlış alarm yaptırım doğurmaz. Bildirim nedeniyle görev, ücret, değerlendirme veya çalışma koşullarında aleyhe değişiklik başlı başına ağır ihlaldir.

Yöneticiler, ekiplerinde tespit ettikleri yetkisiz erişim veya kötüye kullanımı derhal İK Yöneticisine bildirmekle yükümlüdür; bildirmeme yöneticinin kendi ihlalidir. İhlal kaydı tarih, kaynak, etkilenen veri ve kişi sayısı, tedbirler, bildirimler, kök neden ve kapanış alanlarını taşır; yıllık veri koruma raporunda ihlal istatistiği kişi bilgisi olmaksızın tür ve kademe bazında sunulur.

10 Gözden geçirme

Gözden Geçirme ve Revizyon Döngüsü

Mart: veri envanteri güncellemesiyle birlikte gözden geçirme · Kasım: Yönetim Kurulu gündemi · altı tetikleyici



IK-PL-03 · v1.0 · Gözden geçirme

Şekil 21 Gözden geçirme ve revizyon döngüsü — yıllık plan ve plansız tetikleyiciler

Politika, her yılın Mart ayında veri envanteri, VERBİS kaydı ve saklama tablosunun yıllık güncellemesiyle birlikte İK Yöneticisi tarafından gözden geçirilir; Hukuk Müşavirliği mevzuat ve Kurul kararı taramasını, Bilgi Teknolojileri teknik tedbir değerlendirmesini yapar; revizyon ihtiyacı Kasım ayında yıllık veri koruma raporuyla birlikte Yönetim Kuruluna sunulur. Gözden geçirme, değişiklik gerekmesi dahi tutanakla kayda geçer. Aşağıdaki tetikleyicilerden herhangi biri plansız gözden geçirme başlatır:

- Mevzuat ve Kurul kararı: Kanun, yönetmelik veya Kurul ilke kararında çalışan verisini etkileyen değişiklik;
- Veri ihlali: Kurula bildirilen her ihlal veya özel nitelikli veri içeren her olay;
- Yeni işleme faaliyeti: yeni sistem, izleme uygulaması, biyometrik teknoloji veya yurt dışı aktarım ihtiyacı;
- Denetim bulgusu: iç denetim, bağımsız denetim, Kurul incelemesi veya hizmet sağlayıcı güvence raporunda bulgu;
- Gösterge sapması: ayrılıştaki erişim kapatma süresinin 1 iş gününü veya tebliğ oranının %100 hedefini iki dönem üst üste tutturamaması;
- Tekrarlayan istisna: aynı hükümden bir yılda ikinci kez istisna talep edilmesi.

Veri envanteri, saklama tablosu ve rol–yetki matrisinin yıllık güncellenmesi politika revizyonu değildir; bunlar kendi sürüm düzeniyle kayda geçer. Veri koruma ilkelerinin, veri sınıflarının, aktarım kurallarının veya karar yetkilerinin değişmesi yapısal revizyondur (v2.0); metin düzeltilmesi ve hüküm eklemesi küçük revizyondur (v1.x). Her revizyon IK-PL-01 Bölüm 7.2'deki yaşam döngüsünden geçer ve aydınlatma metninin güncel sürümüyle birlikte tebliğ edilir; mevzuat kaynaklı revizyonlar 60 gün içinde tamamlanır.

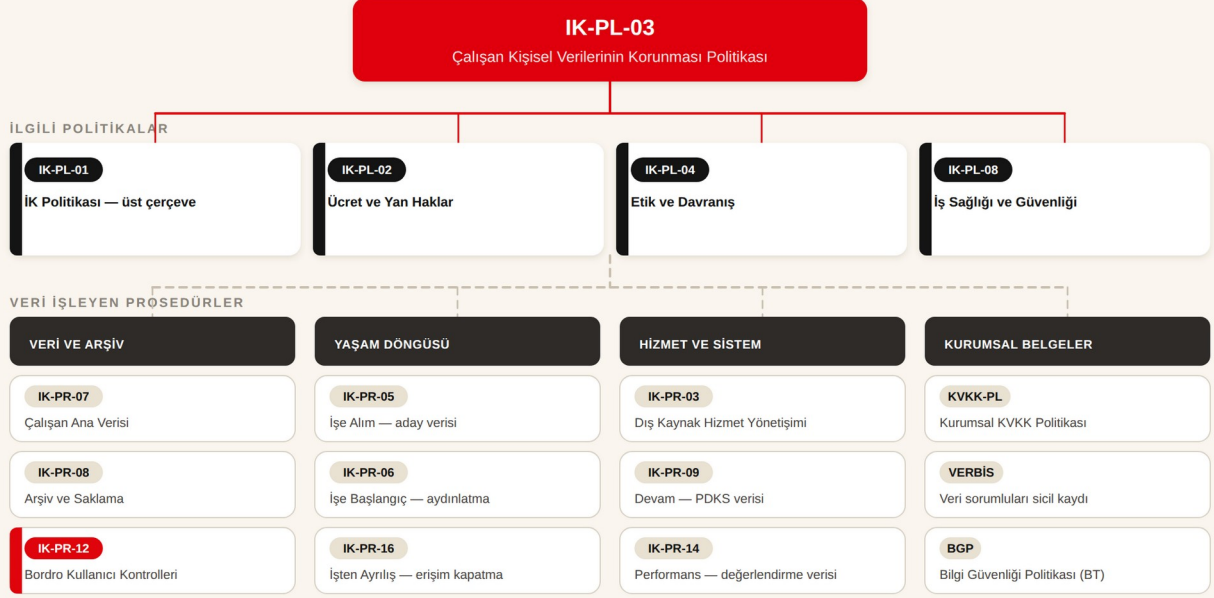
11 İlgili belgeler

Bu politika IK-PL-01 İnsan Kaynakları Politikası'nın üst çerçevesine ve Şirketin kurumsal KVKK politikasına tabidir; çalışan verisi işleyen tüm prosedürler bu politikanın ilkelerini adım düzeyinde uygular. Aydınlatma

metni, açık rıza formları, veri işleyen sözleşme şablonu ve saklama süresi tablosu bu politikanın uygulama belgeleridir ve kendi sürüm düzeniyle yönetilir.

Belge Ağı

Üst çerçeve IK-PL-01 · ilgili politikalar · veri işleyen prosedürler · çelişkide üst kademe uygulanır



IK-PL-03 · v1.0 · Belge ağı

Şekil 22 Belge ağı — üst çerçeve, ilgili politikalar, veri işleyen prosedürler ve kurumsal belgeler

Belgeler arasında çelişki hâlinde üst kademe belge uygulanır; bu politika ile kurumsal KVKK politikası arasında çalışan verisine ilişkin çelişkide daha koruyucu hüküm uygulanır ve çelişki bir sonraki gözden geçirmede giderilir. Bu politikanın form eki yoktur; IK-FR-18 Ana Veri Değişiklik Formu ve arşiv-imha formları ilgili prosedürlerle birlikte sürümlenir.

12 Revizyon ve onay

Belge kimliği ve revizyon çizgisi belge kontrol sayfasında yer alır. Politika, aşağıdaki onay yolunun tamamlanmasıyla yürürlüğe girer; yürürlük tarihi Yönetim Kurulu karar tarihidir. Politika tüm çalışanlara 30 gün içinde aydınlatma metninin güncel sürümüyle birlikte tebliğ edilir; tebliğ imza veya elektronik onayla kaydedilir ve tebliğ oranı üç ayda bir raporlanır (KPI-50).

Onay Yolu

Hazırlayan → kontrol edenler → onaylayan → tebliğ ve aydınlatma · yürürlük = Yönetim Kurulu karar tarihi



IK-PL-03 · v1.0 · Onay yolu

Şekil 23 Onay yolu — hazırlayan, kontrol edenler, onaylayan, tebliğ ve aydınlatma

İmzalı asıl nüsha İK belge yönetim alanında saklanır; elektronik kopya belge ana listesine bağlı olarak yayımlanır. Politikanın İngilizce ayna sürümü aynı sürüm numarasını taşır ve Türkçe metinle birlikte onaylanır; yorum uyumsuzluğunda Türkçe metin esastır.

HAZIRLAYAN · KONTROL EDEN · ONAYLAYAN

Bu belge, aşağıdaki imzaların tamamlanmasıyla yürürlüğe girer. İmzalı asıl nüsha İK belge yönetim alanında saklanır; yürürlükten kalkan sürüm arşivlenir.

Rol	Ad Soyad	Unvan	Tarih	İmza
Hazırlayan		İK Yöneticisi		
Kontrol eden		Hukuk Müşaviri		
Kontrol eden		Bilgi Teknolojileri Yöneticisi		
Kontrol eden		Genel Müdür		
Onaylayan		Yönetim Kurulu Başkanı		