

SALİHLİ KOLEJİ

KİŞİSEL VERİLERİN İŞLENMESİ, KORUNMASI,
SAKLANMASI VE İMHA POLİTİKASI

Veri Sorumlusu	SALİHLİ KOLEJİ ÖZEL EĞİTİM HİZMETLERİ SANAYİ VE TİCARET ANONİM ŞİRKETİ
Adres	Yılmaz Mahallesi Koyuncuoğlu (Yeni) Sokak, Özel Salihli İ. 6. Sitesi No: 6/1, Salihli / Manisa
VKN / MERSİS	7410375965 / 0741037596500018
Belge Kodu	KVK-POL-01
Sürüm	1.0
Yürürlük Tarihi	 / / 20.....
Sonraki Olağan Gözden Geçirme	Yürürlükten itibaren en geç 12 ay içinde
Onaylayan	Yönetim Kurulu / Yetkili Temsilci:

1. AMAÇ

Bu Politikanın amacı; Şirket tarafından işlenen kişisel verilerin hukuka uygun elde edilmesi, kullanılması, paylaşılması, korunması ve işleme şartları sona erdiğinde silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin kuralları belirlemektir. Politika özellikle çocuklara ait veriler, sağlık ve rehberlik kayıtları gibi yüksek riskli veri kümelerinde hesap verebilir, ölçülür ve izlenebilir bir yönetim sistemi kurar.

2. KAPSAM

Politika; öğrenciler, öğrenci adayları, mezunlar, veli/vasiler ve yetkilendirilmiş teslim kişileri, çalışanlar ve adaylar, stajyerler, ziyaretçiler, tedarikçiler/hizmet sağlayıcılar ve bunların personeli ile iletişim kurulan diğer gerçek kişilere ait, Şirketin sorumluluğundaki tüm fiziksel ve elektronik kayıtları kapsar.

- Eğitim, kayıt-kabul, ölçme-değerlendirme, devam, disiplin, rehberlik ve mezuniyet süreçleri.
- Okul doktoru/hemşiresi tarafından yürütülen sağlık, yaralanma, ilaç, acil durum ve alerjen süreçleri.
- Yemekhane, servis/güzergâh, öğrenci teslimi, güvenlik, kamera ve ziyaretçi süreçleri.
- İnsan kaynakları, bordro, iş sağlığı-güvenliği, muhasebe, tahsilat, sözleşme, hukuk ve tedarik süreçleri.
- Web sitesi, çerezler, elektronik iletişim, çağrı/mesaj, kurumsal yazılım, e-posta, yedek ve arşivler.

3. DAYANAK

Politika başta Türkiye Cumhuriyeti Anayasasının 20. maddesi, 6698 sayılı Kişisel Verilerin Korunması Kanunu, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik, Veri Sorumluları Sicili Hakkında Yönetmelik, 5580 sayılı Özel Öğretim Kurumları Kanunu, Millî Eğitim Bakanlığının uygulanabilir düzenlemeleri, 4857 sayılı İş Kanunu, 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, 5510 sayılı Kanun, 213 sayılı Vergi Usul Kanunu, 6102 sayılı Türk Ticaret Kanunu, 6098 sayılı Türk Borçlar Kanunu, 5651 sayılı Kanun ve ilgili ikincil mevzuata dayanır.

4. TANIMLAR

Terim	Açıklama
Açık rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Alıcı grubu	Veri sorumlusu organizasyonu dışında kişisel verilerin aktarıldığı kişi kategorisi.
Anonim hâle getirme	Verilerin başka verilerle eşleştirilse dahi hiçbir surette belirli/belirlenebilir kişiyle ilişkilendirilemeyecek hâle getirilmesi.
İlgili kişi	Kişisel verisi işlenen gerçek kişi.
İlgili kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu birim dışında, veri sorumlusu organizasyonunda veya yetki/talimatıyla veri işleyen kişi/birim.
İmha	Silme, yok etme veya anonim hâle getirme işlemlerinin tümü.
Kişisel veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Özel nitelikli kişisel veri	Kanunun 6. maddesinde sayılan; sağlık, biyometrik/genetik, ceza mahkûmiyeti ve güvenlik tedbirleri, sendika, din, ırk/etnik köken ve diğer hassas veri kategorileri.
Periyodik imha	İşleme şartları tamamen sona eren verilerin, politikada belirtilen tekrarlayan aralıklarla resen imhası.
Saklama süresi	Verinin işleme amacı ve hukuki yükümlülük için tutulduğu azami süre.
Silme	Kişisel verinin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hâle getirilmesi.
Yok etme	Kişisel verinin hiç kimse tarafından erişilemez, geri getirilemez ve tekrar

Terim	Açıklama
	kullanılamaz hâle getirilmesi.

5. KİŞİSEL VERİ İŞLEME İLKELERİ

- Hukuka ve dürüstlük kurallarına uygun olma.
- Doğru ve gerektiğinde güncel olma.
- Belirli, açık ve meşru amaçlarla işleme.
- İşleme amacıyla bağlantılı, sınırlı ve ölçülü olma.
- İlgili mevzuatta öngörülen veya işleme amacı için gerekli süre kadar muhafaza etme.
- Çocuklara ilişkin işlemlerde çocuğun üstün yararını, gelişim düzeyini ve mahremiyetini ayrıca gözetme.

“İleride gerekebilir” düşüncesi tek başına veri toplama veya saklama gerekçesi değildir. Aynı amaca daha az veriyle ulaşılabiliyorsa daha az müdahaleci yöntem seçilir.

6. İŞLEME ŞARTLARI VE HUKUKİ SEBEP YÖNETİMİ

6.1 Genel nitelikli kişisel veriler

Kişisel veriler, Kanunun 5. maddesindeki şartlardan en az birinin varlığı hâlinde işlenir: kanunda açıkça öngörülme; fiili imkânsızlık hâlinde hayat/beden bütünlüğünün korunması; sözleşmenin kurulması veya ifası; hukuki yükümlülük; ilgili kişinin alenileştirmesi ve alenileştirme iradesine uygunluk; bir hakkın tesisi, kullanılması veya korunması; temel haklara zarar vermemek kaydıyla meşru menfaat. Bu şartlardan hiçbirisi yoksa ve işlem isteğe bağlıysa açık rıza değerlendirilir.

6.2 Özel nitelikli kişisel veriler

Özel nitelikli veriler, Kanunun güncel 6. maddesindeki şartlardan uygun olanına dayanılarak ve Kurulca belirlenen yeterli önlemler alınarak işlenir. Açık rıza tek ve varsayılan hukuki sebep değildir. Kanunda açıkça öngörülme, hayat/beden bütünlüğünün korunması, kişinin alenileştirdiği veriye uygun işleme, bir hakkın tesisi/kullanılması/korunması, istihdam ve iş sağlığı-güvenliği yükümlülükleri, sır saklama yükümlülüğü altındaki kişilerce sağlık hizmetleri ve kanunda sayılan diğer şartlar somut işlem bakımından ayrı ayrı değerlendirilir.

Okul sağlık birimindeki sır saklama yükümlülüğü altındaki sağlık personelinin erişimi ile öğretmen, mutfak, servis veya idari personelin erişimi aynı değildir. Bu birimlere tanı ve ayrıntılı sağlık öyküsü değil, yalnız görev için gerekli önlem bilgisi iletilir.

6.3 Açık rıza ve aydınlatma ayrımı

Aydınlatma, veri işlemenin hukuki sebebinden bağımsız bir yükümlülüktür. Açık rıza gereken işlemlerde rıza metni aydınlatmadan ayrı sunulur; belirli, anlaşılır ve seçeneğe olur. Hizmetin sunulması için zorunlu olmayan tanıtım fotoğrafı/video, isteğe bağlı ticari ileti veya benzeri amaçlar ayrı ayrı yönetilir. Rızanın geri alınması ileriye etkili sonuç doğurur; başka bir hukuki sebebe dayanan zorunlu saklama devam edebilir.

7. VERİ KONUSU KİŞİ GRUPLARI VE VERİ KATEGORİLERİ

Öğrenci / öğrenci adayı / mezun: Kimlik, iletişim, eğitim, devam, sınav-not, disiplin, rehberlik, görsel-işitsel, sağlık/alerji/engellilik, servis ve güvenlik.

Veli, vasi ve teslim yetkilisi: Kimlik, iletişim, velayet/vesayet ve yetki belgeleri, sözleşme, mali işlem/taahhüt, talep-şikâyet, iletişim tercihleri.

Çalışan / aday / stajyer: Kimlik, iletişim, özlük, mesleki deneyim, eğitim, bordro-banka, SGK, performans, disiplin, erişim/güvenlik, sağlık ve iş sağlığı-güvenliği.

Ziyaretçi: Kimlik/iletişim (gerektiği ölçüde), giriş-çıkış, ziyaret amacı, kamera görüntüsü, araç bilgisi.

Tedarikçi / hizmet sağlayıcı: Kimlik, iletişim, imza, sözleşme, mali ve hukuki işlem, erişim/güvenlik, çalışan bilgisi.

Diğer kişiler: Hukuki uyumsuzluk, olay/şikâyet, acil durum, referans veya yetkili kamu talebi kapsamında gerekli veriler.

8. İŞLEME AMAÇLARI

- Öğrenci kayıt-kabul, eğitim-öğretim, ölçme-değerlendirme, devam, sınıf/etkinlik ve mezuniyet süreçlerini yürütmek.
- Veli/vasi ilişkisi, sözleşme, ücret/taahhüt, fatura ve iletişim süreçlerini yürütmek.
- Öğrenci sağlığını ve güvenliğini korumak; yaralanma ve acil durumlara müdahale etmek; alerjen ve özel beslenme önlemlerini uygulamak.
- Rehberlik ve psikolojik danışmanlık hizmetlerini mesleki gizlilik ve çocuk güvenliği çerçevesinde yürütmek.

- Servis güzergâhı, öğrenci teslimi, ziyaretçi ve yerleşke güvenliği süreçlerini yürütmek.
- İnsan kaynakları, işe alım, özlük, bordro, SGK, performans, disiplin, eğitim ve iş sağlığı-güvenliği süreçlerini yürütmek.
- Muhasebe, vergi, satın alma, tedarik, denetim, hukuk ve resmî bildirim yükümlülüklerini yerine getirmek.
- Bilgi sistemleri, erişim, yedekleme, olay yönetimi, iş sürekliliği ve veri güvenliğini sağlamak.
- Ayrı hukuki şartı bulunması hâlinde kurumsal tanıtım, etkinlik duyurusu ve ticari elektronik ileti süreçlerini yürütmek.

9. VERİ TOPLAMA KANALLARI

Veriler; fiziki/dijital başvuru ve kayıt formları, sözleşmeler, MEB ve diğer yetkili kamu sistemleri, okul otomasyonu, kurumsal e-posta/telefon/SMS, web sitesi ve çerezler, kamera ve erişim sistemleri, sağlık ve rehberlik görüşmeleri, sınav ve eğitim kayıtları, servis/yemekhane süreçleri, bordro-muhasebe sistemleri, olay/şikâyet formları ve yetkili üçüncü kişiler üzerinden otomatik, kısmen otomatik veya veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerle toplanabilir.

10. AKTARIM

10.1 Yurt içi aktarım

Kişisel veriler; MEB ve diğer yetkili kamu kurumları, mahkemeler/kolluk, mali müşavir-banka-ödeme hizmeti, iş sağlığı-güvenliği ve sağlık hizmeti, sigorta, servis/yemek/güvenlik hizmet sağlayıcıları, bilişim-barındırma/yedekleme sağlayıcıları ve hukuk danışmanları gibi alıcılara yalnız Kanunun 8. maddesindeki şartlar, amaçla sınırlılık ve gerekli güvenlik tedbirleri sağlanarak aktarılır. Hizmet sağlayıcı sözleşmelerinde talimata uygun işleme, gizlilik, alt işleyen, olay bildirimi, iade/imha ve denetim hükümleri yer alır.

10.2 Yurt dışı aktarım

Bulut, e-posta, çevrim içi eğitim, analiz, destek veya benzeri hizmetin veriyi yurt dışına aktarması ya da yurt dışından erişilebilir kılması hâlinde Kanunun güncel 9. maddesindeki yeterlilik kararı, uygun güvence (standart sözleşme, bağlayıcı şirket kuralları veya kanunda sayılan diğer güvence) veya arızı hâl şartlarından uygulanabilir olanı işlem başlamadan önce doğrulanır. Standart sözleşme kullanılıyorsa Kuruma bildirim dâhil ilgili yükümlülükler yerine getirilir. Geçerli mekanizma yoksa aktarım yapılmaz.

11. KAYIT ORTAMLARI

Elektronik: Okul otomasyonu/MEB sistemleri, sunucu, bilgisayar, kurumsal e-posta, bulut hizmeti, veri tabanı, ağ ve güvenlik logları, kamera kayıt cihazı, mobil cihaz, yedek ortam, web ve çerez kayıtları.

Fiziksel: Öğrenci/veli dosyası, özlük dosyası, sağlık ve rehberlik dosyası, sınav evrakı, sözleşme, muhasebe belgesi, ziyaretçi kaydı, teslim/zimmet formu ve arşiv.

Üçüncü taraf sistemi: Yetkilendirilmiş kamu sistemi, banka/ödeme, bordro, servis, yemek, sağlık/İSG veya bilişim hizmet sağlayıcı sistemleri; veri işleme sözleşmesi ve erişim kontrolü şartıyla.

12. SAKLAMA SÜRESİNİ BELİRLEME KURALLARI

- Önce uygulanabilir mevzuatta açık süre bulunup bulunmadığı belirlenir.
- Birden çok süre varsa, işleme şartı ve hukuki talep/denetim ihtiyacı bakımından geçerli olan en uzun zorunlu süre uygulanır; süresiz saklama yapılamaz.
- Mevzuatta süre yoksa amaç, veri hassasiyeti, ilgili kişinin makul beklentisi, çocukların korunması, zamanaşımı ve olası uyumsuzluk ihtiyacı dikkate alınarak azami süre belirlenir.
- Süre başlangıcı tabloda belirtilen olaydır: ilişkinin sona ermesi, belgenin düzenlenmesi, kaydın oluşması, adaylık sürecinin kapanması veya rızanın geri alınması gibi.
- Yasal saklama emri, devam eden dava/denetim veya resmî makam talebi varsa yalnız ilgili veri için imha askıya alınır; sebep ve kapsam kayıt altına alınır.
- Asıl kayıt ile geçici kopya, çalışma listesi, yerel indirme ve yedeklerin süreleri ayrıca yönetilir; geçici kopya amacın tamamlanmasıyla daha erken silinir.

13. SAKLAMAYI GEREKTİREN BAŞLICA SEBEPLER

Eğitim ve özel öğretim mevzuatı; öğrenci ve personel kayıtlarının yürütülmesi; iş, sosyal güvenlik, iş sağlığı-güvenliği, vergi ve ticaret hukuku yükümlülükleri; sözleşmenin kurulması/ifası; bir hakkın tesisi, kullanılması veya korunması; yerleşke ve çocuk güvenliği; yetkili makam talepleri; bilgi güvenliği ve meşru menfaatler. Açık rıza, yalnız rıza gerektiren belirli isteğe bağlı işlemler için saklama sebebi olabilir.

14. İMHAYI GEREKTİREN SEBEPLER

- İşleme amacının ve Kanunun 5 veya 6. maddesindeki tüm işleme şartlarının sona ermesi.

- İlgili mevzuatın değişmesi veya işleme faaliyetinin hukuka aykırı olduğunun tespiti.
- Saklama süresinin dolması ve geçerli bir hukuki saklama sebebi bulunmaması.
- Açık rızaya dayalı tek amaçta rızanın geri alınması.
- İlgili kişinin silme/yok etme talebinin haklı bulunması veya Kurul/mahkeme kararı.
- Sistem, süreç veya sözleşmenin sona ermesi nedeniyle verinin artık gerekli olmaması.

15. PERİYODİK İMHA TAKVİMİ

Şirketin periyodik imha aralığı altı aydır. Olağan periyodik imha dönemleri her yıl Haziran ve Aralık aylarının son haftasında tamamlanır. İmha yükümlülüğü doğan veri, yükümlülüğün doğduğu tarihi takip eden ilk periyodik imhada imha edilir. İlgili kişinin talebi üzerine uygulanacak süreler ve Kurul kararları saklıdır.

Kontrol	Sorumlu	Kanıt
Süre dolumu listesi	KVKK Koordinasyonu + veri sahibi birim	İmha adayı listesi
Hukuki bekletme kontrolü	Hukuk/Yetkili Yönetim	Bekletme kaydı
İmha ve doğrulama	BT + ilgili birim/arşiv	İmha tutanağı/log
Örnekleme ve kapanış	KVKK Koordinasyonu	Dönem raporu

16. İMHA YÖNTEMLERİ

16.1 Silme

- Uygulama içi silme ve erişim yetkilerinin kaldırılması; verinin ilgili kullanıcılarca erişilemez/yeniden kullanılamaz hâle getirilmesi.
- Veri tabanında güvenli silme komutu, kayıt anonimleştirme veya ilişkisel bağın kaldırılması; bütünlük kontrolü.
- Kâğıt arşivde ayırma/karartma yalnız kalan belgenin içeriği ve ispat değeri bozulmadan uygulanabiliyorsa kullanılır.

16.2 Yok etme

- Kâğıt, optik ortam ve kartların çapraz kesim, öğütme, yakma veya sertifikalı güvenli imha hizmetiyle geri döndürülemez biçimde yok edilmesi.
- Manyetik/elektronik ortamların güvenli üzerine yazma, kriptografik silme, fiziksel parçalama veya üretici standardına uygun geri döndürülemez yöntemle imhası.
- Bulut/hizmet sağlayıcı ortamında üretim, replikasyon, önbellek ve sözleşmede kararlaştırılan yedeklerden silme; sağlayıcıdan imha teyidi alınması.

16.3 Anonim hâle getirme

Anonimleştirme yalnız yeniden kimliklendirme riski kabul edilebilir düzeye indirildiğinde uygulanır. Doğrudan tanımlayıcıların silinmesi tek başına her zaman anonimlik sağlamaz. Veri kümesi, bağlam ve dış veriyle eşleştirme riski test edilir.

- Toplulaştırma ve istatistiksel raporlama.
- Alt/üst sınır kodlama, genelleştirme ve bölgesel gösterim.
- Maskeleme, veri değiş-tokuşu veya gürültü ekleme.
- K-anonimlik, L-çeşitlilik veya uygun istatistiksel gizlilik yöntemleri.

16.4 Yedekler, e-posta ve loglar

Yedeklerde tekil kayıt silme teknik olarak mümkün değilse veri üretim sisteminde kullanıma kapatılır; yedek rotasyonu sonunda yok olur ve geri yükleme hâlinde silme listesi yeniden uygulanır. Bu süre boyunca yedeğe erişim yalnız felaket kurtarma personeliyle sınırlıdır. E-posta arşivi ve loglar ayrı saklama kuralına tabidir; kişisel veri içeren eklerin gereksiz çoğaltılması önlenir.

17. İMHA İŞLEMİNİN KAYDI

Silme, yok etme ve anonimleştirme işlemleri; veri kümesi/kategori, ilgili kişi grubu, miktar veya kapsam, ortam, hukuki sebebin sona erme tarihi, yöntem, işlem tarihi, işlemi yapan/onaylayan ve doğrulama sonucu gösterilecek şekilde tutanağa bağlanır. İmha kayıtları, başka bir mevzuat daha uzun süre gerektirmedikçe işlem tarihinden itibaren en az üç yıl saklanır.

18. TEKNİK VE İDARİ TEDBİRLER

18.1 İdari tedbirler

- Kişisel veri işleme envanteri, VERBİS, aydınlatma ve rıza süreçlerinin uyumlu tutulması.
- Rol bazlı en az yetki, görev ayrılığı, erişim onayı ve periyodik yetki gözden geçirmesi.
- Çalışan eğitimleri, gizlilik taahhütleri, ihlal/olay bildirim prosedürü ve disiplin hükümleri.
- Tedarikçi risk değerlendirmesi ve veri işleme/aktarım sözleşmeleri.
- Özel nitelikli veriler için ayrı politika/prosedür, yetki listesi ve eğitim.
- Çocuk verileri için mahremiyet etki değerlendirmesi; yeni teknoloji ve süreçlerde veri koruma etki değerlendirmesi.
- Fiziksel arşiv giriş kaydı, anahtar yönetimi, temiz masa ve güvenli imha kutusu.

18.2 Teknik tedbirler

- Güçlü kimlik doğrulama, benzersiz hesap, çok faktörlü doğrulama ve parola politikası.
- Ağ ayrıştırma, güvenlik duvarı, zararlı yazılım koruması, yama ve zafiyet yönetimi.
- Erişim/log kayıtları, anomali izleme ve zaman senkronizasyonu.
- Aktarımda ve uygun sistemlerde depolamada şifreleme; anahtarların ayrı yönetimi.
- Düzenli, şifreli ve geri yükleme testi yapılmış yedekleme; çevrim dışı/ayrık kopya.
- Kamera, sağlık ve rehberlik sistemlerinde ayrı yetki grubu ve dışı aktarma kontrolü.
- Veri kaybı önleme, güvenli e-posta, cihaz yönetimi, uzaktan silme ve taşınabilir ortam kısıtı.

19. ÖZEL NİTELİKLİ VERİLERE ÖZGÜ TEDBİRLER

- İşleme süreçleri ve güvenlik önlemleri ayrı yazılı prosedürde tanımlanır.
- İşleyen personele düzenli eğitim verilir ve özel gizlilik yükümlülüğü uygulanır.
- Erişim kapsamı/süresi açıkça belirlenir, erişimler düzenli kontrol edilir; görev değişikliği veya ayrılıştan derhâl kaldırılır.
- Elektronik aktarım şifreli kurumsal kanal veya güvenli bağlantıyla; fiziksel aktarım kilitli/zarf ve teslim kaydıyla yapılır.
- Sağlık ve rehberlik dosyaları genel öğrenci/özlük dosyasından ayrıştırılır. Mutfak, servis veya öğretime yalnız gerekli önlem bilgisi verilir.
- İmha ve dışı aktarma işlemleri çift kontrol veya yetkili onayla yürütülür.

20. ÇOCUK VERİLERİNE ÖZGÜ KURALLAR

- Çocuğa yaşına ve gelişim düzeyine uygun açıklama yapılır; veli/vasi yetkisi doğrulanır. Velinin işlemi bilmesi her durumda çocuğun mahremiyetini ortadan kaldırmaz.
- Öğrenci fotoğrafı/video/sesi, sağlık, rehberlik, disiplin, adres ve konum verileri yüksek riskli kabul edilir.
- Sınıf/veli gruplarında başka öğrenciye ait not, sağlık, disiplin veya iletişim bilgisi paylaşılmaz.
- Rehberlik görüşme notu disiplin veya tanıtım amacıyla kullanılamaz; yalnız güvenlik ve eğitim desteği için gerekli sonuç aktarılır.
- Mezuniyet/ayrılıştan günlük operasyon listeleri, servis güzergâhları, alerjen çalışma listeleri ve erişimler beklenmeden temizlenir.

21. GÖREV VE SORUMLULUKLAR

Rol	Sorumluluk
Yönetim Kurulu / Yetkili Temsilci	Politikayı onaylar; kaynak, sorumluluk ve yaptırım desteğini sağlar.
KVKK Koordinasyonu	Envanter/politika uyumu, başvuru, ihlal, imha takvimi, eğitim, raporlama ve güncellemeyi koordine eder.
Birim Yöneticileri	Veri doğruluğu, saklama süresi, erişim listesi ve imha adaylarını doğrular.
Bilgi Teknolojileri	Teknik güvenlik, yedek, log, güvenli silme/yok etme ve teknik kanıtları sağlar.
Arşiv / İdari İşler	Fiziksel arşiv, giriş-çıkış ve kâğıt imha sürecini yürütür.
Sağlık ve Rehberlik Birimleri	Özel nitelikli kayıtları mesleki gizlilik, ayrıştırma ve asgari paylaşım ilkesiyle yönetir.

Rol	Sorumluluk
İnsan Kaynakları / Mali İşler	Özlük, bordro, vergi ve ticari kayıt sürelerini takip eder.
Tüm Çalışanlar	Yetki sınırına uyar, yerel kopya oluşturmaz, süre dolumu ve ihlali gecikmeden bildirir.
Hizmet Sağlayıcılar	Sözleşme ve talimata uygun saklar; hizmet sonunda iade/imha teyidi verir.

22. İLGİLİ KİŞİ TALEPLERİ

İlgili kişi, Kanunun 11. maddesi kapsamındaki haklarını kurumun başvuru formu ve ilan edilen kanallar üzerinden kullanabilir. Kimlik/yetki doğrulaması ölçülü yöntemle yapılır. Silme/yok etme talebinde tüm işleme şartları sona ermişse talep mevzuattaki süre içinde yerine getirilir; veri üçüncü kişilere aktarılmışsa gerekli bildirim yapılır. Geçerli saklama sebebi varsa talep gerekçeli yanıtlanır ve veri yalnız bu sebeple sınırlı erişime alınır.

23. VERİ İHLALİ VE İMHA SÜRECİ GÜVENLİĞİ

Yetkisiz silme de veri ihlali olabilir. Şüpheli silme, yanlış imha, kayıp dosya, yedekten geri dönmeme veya imha edilecek verinin üçüncü kişiye çıkması derhâl olay prosedürüne göre bildirilir. Çalışan kanıtı silmez; BT ve KVKK Koordinasyonu olay kapsamını belirler, zararı sınırlar ve gerekli bildirimleri değerlendirir.

24. DENETİM, GÜNCELLEME VE YAYIM

Politika en az yılda bir; ayrıca mevzuat, VERBİS, süreç, sistem, tedarikçi veya risk değişikliğinde gözden geçirilir. Değişiklikler onay ve sürüm kaydıyla yürürlüğe girer. Kamuya açık nüshada güvenlik mimarisi, erişim detayları ve ticari sırlar yayımlanmaz; çalışanlar görevlerine ilişkin iç prosedürlere erişir.

25. YÜRÜRLÜK

Politika, yetkili organın onay tarihinde yürürlüğe girer. Politikanın uygulanmasından Şirket yönetimi sorumludur. Mevzuat ile çelişen hüküm yerine güncel emredici mevzuat uygulanır ve belge gecikmeksizin güncellenir.

