KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

1.GİRİŞ

1.1 Amaç

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

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

1.2 Kapsam

Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Şirketin sahip olduğu ya da Şirketçe yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3. Tanımlar

Bu Politika'da kullanılan, aşağıdaki terimler, Politika içinde ayrıca farklı şekilde tanımlanmadıkları sürece, aşağıdaki tabloda gösterilen anlamları ifade edeceklerdir.

TERİM	TANIM
Alıcı grubu:	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini ifade eder.
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.
Anonim hale getirme	Kişisel Verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder.
İkincil Mevzuat	Kanun uyarınca, Kişisel Verileri Koruma Kurumu tarafından çıkarılan ya da alınan herhangi bir yönetmelik, genelge, tebliğ, ilke kararı veya benzeri bir idari karar ya da genel görüş anlamına gelir.

İlgili Kullanıcılar	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri ifade eder.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini ifade eder.
Kanun	6698 Sayılı Kişisel Verilen Korunması Kanunu'nu ifade eder.
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 ortamı ifade eder.
Kişisel Veri İşleme Envanteri	Şirketimizin veri sorumlusu sıfatıyla iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdığı işbu Politika'nın ekinde yeralan envanteri ifade eder.
Kişisel Veri/ler	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.
Kişisel Verilerin işlenmesi	Kişisel Veriler'in tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder.
Kurul	Kişisel Verileri Koruma Kurulu'nu ifade eder.
Kurum	Kişisel Verileri Koruma Kurumu'nu ifade eder.
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 mahkûmiyetive güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir.
Periyodik İmha	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda işbu Politika'da belirtilen ve tekrar eden aralıklarla kendiliginden gerçekleştirilecek silme, yok etme veya anonim hale getirme şlemini ifade eder.
Sicil	Veri sorumlularının kayıt olmak zorundaoldukları ve veri işleme faaliyetleri ile ilgili bilgileri beyan ettikleri bir kayıt sistemi olan VeriSorumluları Sicili'ni ifade eder.
Silme	Kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesini ifade eder.
Saklama ve İmha Politikası	Şirket'in, Kişisel Verilerin Silinmesi, YokEdilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik çerçevesinde hazırladığı,silme ve imhaya ilişkin usul ve esasları düzenleyen politikayı ifade eder.
Şirket	İlab Holding A.Ş.
Veri İşleyen	Veri Sorumlusu'nun verdiği yetkiye dayanarak onun adına Kişisel Veriler'i işleyen gerçek veya tüzel kişiyi ifade eder.
Veri Koruma Komisyonu	Şirket'in Kişisel Verilerin Korunması Komisyonu'nu ifade eder. Altuğ İnan, Şimal Konanç, Ezgi Kızmaz ve Samet Uzun'dan oluşmaktadır.
Veri Sahibi	Kanunda "İlgili Kişi" olarak tanımlanan Veri Sahibi, Kişisel Verisi işlenen gerçek kişiyi ifade eder. Veri Sahipleri, müşterileri, internet kullanıcılarını, iletişim, elektronik posta ve pazarlama veri tabanı listelerindeki bireyleri, çalışanları, sözleşme taraflarını ve tedarikçileri de kapsar.
Veri Sorumlusu	Kişisel Verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumluolan gerçek veya tüzel kişiyi ifade eder.
Veri Sorumluları Sicili Hakkında Yönetmelik	1 Ocak 2018 tarihinde yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmelik'i ifade eder.
Yok Etme	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesini ifade eder.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Şirketin tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım aşağıda gösterilmiştir.

Tablo : 1

UNVAN	BİRİM	GÖREV
Yönetim Kurulu Başkanı	Yönetim	Çalışanların politikaya uygun Hareket etmesinin sağlanmasından sorumludur.
Veri Koruma Komisyonu	Yönetim	Kişisel veri işlenen süreçlerde politikaya uyumun takibi ve süreçlerdeki değişikliklerde ilgili birimlere danışmanlık verilmesinden sorumludur.
CFO	Yönetim	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Teknoloji Hizmetleri Müdürü	IT	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
IK, Muhasebe, Denetim, Ürün tasarım, Reklam Satış, Dijital Pazarlama, Veri Analitiği	Diğer Bölümler	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

3. KAYIT ORTAMLARI

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

Tablo :2

Elektronik Ortamlar	Fiziki Ortamlar
Sunucular (yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) Yazılımlar (ofis yazılımları, iş gereği kullanılan diğer yazılımlar) Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespitve engelleme, günlük kayıt dosyası, antivirüs vb.) Kişisel bilgisayarlar (Masaüstü, dizüstü) Mobil cihazlar (telefon, tablet vb.) Optik diskler (CD, DVD vb.) Çıkartılabilir bellekler (USB, Hafıza Kart vb.)Yazıcı, tarayıcı, fotokopi makinesi	Kağıt (Dosya ve klasörler) Yazılı, basılı, görsel ortamlar

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; çalışanlar, çalışan adayları, müşteriler, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir. Bu kapsamda saklama ve imhaya ilişkin açıklamalar aşağıdadır:

4.1 Saklama

Şirket, faaliyetleri çerçevesinde edindiği kişisel verileri, Kişisel Verileri Koruma Kanunu ve ikincil mevzuatında düzenlendiği şekilde, bağlı olunan mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklar.

İşleme ve saklama konusunda, Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi, 4 üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesive 5 ve 6 ncı maddelerdeki, kişisel verilerin işleme şartlarına ilişkin kurallara uyulur.

4.1.1 Saklamayı Gerektiren Hukuki Sebepler

Yürürlükteki İş Kanunu, Mali Mevzuat, ISG Kanunu ve iş ve işlemlerin yürütülmesi gereğitabi olunan diğer mevzuat ve ikincil düzenlemeleri

4.1.2 İşleme Amaçları

- İnsan kaynakları süreçlerinin yürütülmesi,
- Kurumsal iletişimin sağlanması,
- Fiziksel güvenliğin sağlanması,
- İmzalanan sözleşmelerden doğan yükümlülüklerin yerine getirilmesi (İş sözleşmesi,hizmet sözleşmesi vs)

- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlanması (mali mevzuat, iş kanunu vs)
- Şirketle ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlanması
- Yasal raporlamalar yapılması
- Kamu otoritelerince talep edilen bilginin sağlanması
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

4.1.3 İmhayı gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya kaldırılması, İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi
- Şirketin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, şirketçe verilen cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

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

5. TEKNİK VE İDARİ TEDBİRLER

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

5.1 Teknik Tedbirler

Şirket tarafından, kişisel verilerin korunmasına ilişkin alınan tedbirler aşağıdaki gibidir.

- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturulmuştur
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir.
- Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmaktadır

5.2 İdari Tedbirler

Şirket tarafından, işlenen kişisel verilerle ilgili olarak aşağıdaki idari tedbirler alınmaktadır.

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, KVK kanunu ve ilgili diğer mevzuat hakkında eğitimler planlanmış ve yürütülmektedir.
- Şirket işleyişine ilişkin olarak, çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Şirket Etik Kod'unda, Güvenlik politika ve prosedürlerine uyuma ilişkin hükümler bulunmaktadır.
- Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kurum içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir
- Veri İhlal Müdahale Planı hazırlanmıştır.

6. İMHA YÖNTEMLERİ

İmhası gereken verilerle ilgili aşağıdaki işlemler yapılır.

6.1. Kişisel verilerin Silinmesi

Verinin Kaydedildiği Ortam	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda bulunan Kişisel Veriler Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, CFO onayı ile Denetim Müdürü dışında, diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanabilir.

Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.2 Yok etme

Verinin Kaydedildiği Ortam	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

6.3. Anonim Hale Getirme

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.
İstatistiki amaçlarla ihtiyaç duyulabileceği düşünülen veriler, herhangi bir kişi ya da yöntemle geri döndürülemez bir şekilde, bu şekilde, belirli bir kişiyi tanımlayamaz hale getirilir.

7. SAKLAMA VE İMHA SÜRELERİ

Şirketin faaliyetleri kapsamında işlediği kişisel verilere ilişkin saklama süreleri, VERBIS'te veri kategorisi bazında gösterilmektedir. Ayrıca, veri envanterinde her bir veri kategorisi bazında saklama süreleri de yer almaktadır.

8. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince şirkette periyodik imha süresi 6 ay olarak belirlenmiştir.Saklama süresi dolan verilen imhası, mart ve eylül aylarında yapılır.

9. YÜRÜRLÜK VE GEÇERLİK

Bu Politika, 01.10.2020 tarihinde yürürlüğe girer. Yılda bir defa ya da 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve bağlı mevzuatta değişikliği olması durumunda gözden geçirilir ve gerekirse güncellenir.

EK:1

1-KimlikKişisel Veri	Yıl15 Yıl
2-İletişimKişisel Veri	Yıl15 Yıl
3-LokasyonKişisel Veri	Yıl1 Yıl
4-ÖzlükKişisel Veri	Diğer İş ilişkisinin bitiminin ardından 10 yıl
5-Hukuki İşlem Kişisel Veri	Yıl10 Yıl
7-Fiziksel Mekan Güvenliği Kişisel Veri	Diğer 15 gün
8-İşlem Güvenliği Kişisel Veri	Diğer 42 gün
10-FinansKişisel Veri	Diğer Ortakların verileri süresiz saklanmaktadır.
11-Mesleki Deneyim Kişisel Veri	Diğer İş ilişkisinin bitiminin ardından 10 yıl
13-Görsel Ve İşitsel Kayıtlar Kişisel Veri	Diğer 15 gün
21-Sağlık Bilgileri Özel Nitelikli Kişisel Veri	Diğer İş ilişkisinin bitiminden sonra 10 yıl süreyle
23-Ceza Mahkûmiyeti ve Güvenlik Tedbirleri Özel Nitelikli Kişisel Veri	Diğer İş ilişkisinin bitiminden sonra 10 yıl süreyle
24-Biyometrik Veri Özel Nitelikli Kişisel Veri	Diğer İş ilişkisinin bitiminden sonra 1 gün içerisinde