K&P LEGAL HUKUK BÜROSU

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

K&P LEGAL HUKUK BÜROSU

Erdal Kardas - Yelda Topuz Kardas Ortaklığı

KİŞİSEL VERİLERİN İŞLENMESİ KORUNMASI VE İMHA POLİTİKASI

1. GİRİŞ

1.1. Amaç

Bu Politikanın amacı; **K&P LEGAL HUKUK BÜROSU** / Erdal Kardas - Yelda Topuz Kardas Ortaklığı'nda (bundan sonra K&P Legal olarak anılacaktır) işlenen kişisel verilerin, korunması çalışmalarının başında kişisel veri olarak çeşitli amaç ve kanallardan Hukuk Bürosu bünyesine gelen yazılı, basılı ya da elektronik ortamdaki kişisel verilerin tespiti ve uygun kontrollerin tesis edilmesi, bu verilerin saklanmasına ilişkin gereken güvenli ortamların hazırlanması ve bu verilere erişimin kısıtlı sayıda ve yetkili kişiler tarafından gerçekleştirildiğinden emin olunması ile burada işlenen kişisel verilerin, işlendikleri amaç için gerekli olan azami süreler ile silinme, yok edilme ya da anonim hale getirilme süreçlerinin belirlenmesi ve bu süreçlerde görev alacak kişilerin rol ve sorumluluklarının tanımlanması ve kişisel veri ihlal olaylarının yönetiminin belirlenmesidir.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, K&P Legal tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

1.2. Kapsam

Bu Politikanın kapsamı; Hukuk Bürosu çalışanları, çalışan adayları, müvekkiller, hizmet sağlayıcıları, müşteriler, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin gizliliği, mahremiyeti konusunda kişisel verilerin korunması amacıyla gereken güvenlik önlemlerinin alınması ve kontrollerin uygulanması, kişisel verilerin azami saklama süreleri, kişisel verilerin hukuka uygun olarak saklanması, imha edilmesi için alınmış teknik ve idari tedbirler, kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetleri oluşturmaktadır. Bu kapsamda yukarıda belirtilen kişisel veri sahipleri gruplarına, işbu Politikanın tamamı uygulanabileceği gibi, sadece birtakım hükümleri de uygulanabilecektir.

1.3. Tanımlar

Politikada kullanılan terimlere ait tanımlar aşağıda yer almaktadır.

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza.
Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.

Başkanlık	Kişisel Verileri Koruma Kurumu Başkanlığı
Çalışan	K&P Legal personeli
Hukuk Bürosu	K&P LEGAL HUKUK BÜROSU / Erdal Kardas - Yelda Topuz Kardas Ortaklığı
Elektronik Ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
Elektronik Olmayan Ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
Hizmet Sağlayıcı	K&P Legal ile belirli süreli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
İlgili Kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
KEP	Kayıtlı Elektronik Posta
Kayıtlı Elektronik Posta	Gönderici ve alıcı kimliklerinin belli olduğu, gönderi zamanının ve içeriğinin değiştirilemediği, uyuşmazlık durumunda hukuki geçerliliği olan güvenli elektronik posta hizmeti.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her tülü bilgi.
Kişisel Veri İşleme Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.
Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kurul	Kişisel Verileri Koruma Kurulu
Kanun	Kişisel Verilerin Korunması Kanunu
Kişisel Verilerin Korunması Komitesi	K&P Legal tarafından atanmış Kişisel Verilerin Korunması Kanunu ve alt düzenlemeleri kapsamında oluşturulmuş süreçlerin idari takibini yapmak üzere oluşturulan komite.
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 mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.
Periyodik İmha	Kanunda yer alan verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re 'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Politika	K&P Legal Kişisel Verileri Saklama ve İmha Politikası.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan tüzel kişi olarak K&P LEGAL HUKUK BÜROSU / Erdal Kardas - Yelda Topuz Kardas Ortaklığı
Veri Sorumluları Sicil Bilgi Sistemi	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
VERBİS	Veri Sorumluları Sicili Bilgi Sistemi
Yönetmelik	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

Bu Politika'da yer almayan tanımlar için Kanun'daki tanımlar geçerlidir.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Ortaklığın 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 aktif olarak destek verir.

3. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

K&P Legal tarafından; çalışanlar, çalışan adayları, müvekkiller, ziyaretçiler, müşteriler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

Kanunun 3'üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 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 edilmesi gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır.

Bu kapsamda, Ortaklığın faaliyetleri çerçevesinde kişisel verileri 5/1, 5/2-a, 5/2-b, 5/2-c, 5/2-ç, 5/2-e, 5/2-f ve 6/3 maddelerine istinaden işlemekte, ilgili mevzuatta öngörülen süre kadar veya işleme amaçlarına uygun süre kadar saklanmaktadır.

- 5/1 Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.
- 5/2-a Kanunlarda açıkça öngörülmesi.
- 5/2-b Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- 5/2-c Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- 5/2-ç Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- 5/2-e Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- 5/2-f İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.
- 6/3 Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

3.1. Saklamayı Gerektiren Hukuki Sebepler

K&P Legal faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 1136 Sayılı Avukatlık Kanunu
- 6098 Sayılı Türk Borçlar Kanunu
- 6102 Sayılı Türk Ticaret Kanunu
- 4721 Sayılı Türk Medeni Kanunu
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu
- 6502 Sayılı Tüketicinin Korunması Hakkında Kanunu
- 4857 Sayılı İş Kanunu
- 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu ve ilgili Yönetmelikler

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

3.2. Saklamayı Gerektiren İşleme Amaçları

- Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
- Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
- Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
- Eğitim Faaliyetlerinin Yürütülmesi

- Erişim Yetkilerinin Yürütülmesi
- Faaliyetlerin Mevzuata Uygun Yürütülmesi
- Finans ve Muhasebe İşlerinin Yürütülmesi
- Fiziksel Mekân Güvenliğinin Temini
- Hukuk İşlerinin Yürütülmesi
- İletişim Faaliyetlerinin Yürütülmesi
- İş Faaliyetlerinin Yürütülmesi / Denetimi
- İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
- İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
- Lojistik Faaliyetlerinin Yürütülmesi
- Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
- Mal / Hizmet Satış Süreçlerinin Yürütülmesi
- Mal / Hizmet Üretim ve Operasyon Süreçlerinin Yürütülmesi
- Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi
- Organizasyon ve Etkinlik Yönetimi
- Risk Yönetimi Süreçlerinin Yürütülmesi
- Sözleşme Süreçlerinin Yürütülmesi
- Yetkili Kişi, Kurum ve Kuruluşlara Bilgi Verilmesi
- Ziyaretçi Kayıtlarının Oluşturulması ve Takibi

3.3. İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- 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 K&P Legal tarafından kabul edilmesi,
- K&P Legal'ın ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği 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, K&P Legal tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

4. KİŞİSEL VERİLERİN GÜVENLİĞİNİN VE GİZLİLİĞİNİN SAĞLANMASI

K&P Legal, Kanunun 12 inci maddesine uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli teknik

ve idari tedbirleri almakta, bu kapsamda gerekli denetimleri yapmak veya yaptırmaktadır. Kişisel verilerin kanuni olmayan yollarla ifşası durumunda Kanunda öngörülen tedbirlere uygun olarak hareket edilmektedir.

4.1. İdari Tedbirler

- Ortaklık, Kişisel Verilerin Korunması hukukuna ilişkin olarak çalışanlarını eğitmekte ve bilinçlendirilmelerini sağlamaktadır.
- Çalışanlar, öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacı dışında kullanamayacağı ve bu yükümlülüğün görevden ayrılmalarından sonra da devam edeceği konusunda bilgilendirilmekte ve bu doğrultuda kendilerinden gerekli taahhütler alınmaktadır.
- Çalışanların güvenlik politikalarına uymaması durumunda disiplin süreci işletilmektedir.
- Kişisel verilerin aktarıma konu olduğu durumlarda, K&P Legal tarafından kişisel verilerin aktarıldığı kişiler ile akdedilmiş olan sözleşmelere, kişisel verilerin aktarıldığı tarafın veri güvenliğini sağlamaya yönelik yükümlülükleri yerine getireceğine ilişkin kayıtlar eklenmesi temin edilir.
- Kişisel verilerin saklanması konusunda teknik gereklilikler sebebiyle dışarıdan bir hizmet alınması durumunda, kişisel verilerin hukuka uygun olarak aktarıldığı ilgili firmalar ile akdedilen sözleşmelere; kişisel verilerin aktarıldığı kişilerin, kişisel verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlanacağına ilişkin hükümlere yer verilmektedir.
- Belirli aralıklarla tedarikçi veri işleyen denetimi uygulanmaktadır. “Tedarikçi Değerlendirme Formu” üzerinden süreç işletilmektedir.
- K&P Legal tarafından VERBİS sistemine uyumlu Kişisel Veri İşleme Envanteri çıkarılarak, burada hukuka ve amaca uygunluk denetimleri yapılmaktadır.
- K&P Legal tarafından yürütülen kişisel veri işleme faaliyetleri detaylı olarak incelenmekte ve periyodik olarak gözden geçirilerek gerektiğinde güncellenmektedir. Bu kapsamda, Kanunda öngörülen kişisel veri işleme şartlarına uygunluğun sağlanması için atılması gereken adımlar tespit edilir.
- Gözden geçirme sonucunda, ihtiyaç duyulmayan kişisel veriler, “Kişisel Veri Saklama Ve İmha Politikası” ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yönetmeliğine uygun ve güvenli bir şekilde imha edilmektedir.
- K&P Legal, Kanuna uyumun sağlanması için yerine getirilmesi gereken uygulamaları tespit ederek, “Kişisel Veri Saklama ve İmha Politikası”nı düzenler ve periyodik olarak gözden geçirerek gerektiğinde günceller. Kişisel veri ihlal olayları için ortaya çıkabilecek riskler ile güvenlik ihlallerinin nasıl yönetileceği de açıkça belirlenmektedir.

4.2. Teknik Tedbirler

- K&P Legal, kişisel verilerin saklanmasında Bilgi Güvenliği Politikalarına uyumlu hareket eder.
- K&P Legal tarafından kişisel verilerin korunmasına ilişkin olarak, teknolojinin imkân verdiği ölçüde teknik önlemler alınmakta ve alınan önlemler gelişmelere paralel olarak güncellenip, iyileştirilir.

- Teknik konularda, uzman personel istihdam edilir.
- Alınan önlemlerin uygulanmasına yönelik düzenli aralıklarla denetim yapılır.
- Güvenliği temin edecek yazılım ve sistemler kurulur.
- K&P Legal bünyesinde işlenmekte olan kişisel verilere erişim yetkisi, belirlenen işleme amacı doğrultusunda ilgili çalışanlar ile sınırlandırılır.
- Kişisel verilerin güvenli ortamlarda saklanması için teknolojik gelişmelere uygun sistemler kullanılmaktadır.
- Saklanma alanlarına yönelik teknik güvenlik sistemleri kurulmakta, alınan teknik önlemler periyodik olarak denetlenmekte, risk teşkil eden hususlar yeniden değerlendirilerek gerekli teknolojik çözüm üretilmektedir.
- Kişisel verilerin güvenli bir biçimde saklanmasını sağlamak için hukuka uygun bir biçimde tüm gerekli altyapılar kullanılmaktadır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

K&P Legal tarafından kişisel verilerin hukuka aykırı erişimini engellemek için alınan başlıca teknik tedbirler aşağıda sıralanmaktadır;

4.2.1. Siber Güvenliğin Sağlanması

- Kişisel veri içeren bilgi teknoloji sistemlerinin internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında öncelikli olarak güvenlik duvarı ve ağ geçidi tedbirleri alınmaktadır.
- Kişisel veri güvenliğinin sağlanması için farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilme durumlarında, bağlantılar SSL ile gerçekleştirilmektedir.
- Güncel Anti-virüs yazılımları kullanılmaktadır. İnternete giden veya gelen trafik virüslere karşı taranmaktadır.
- İnternet üzerinden hukuk bürosu tarafından onaylanmamış yazılımlar indirilemez ve hukuk bürosu sistemleri üzerine bu yazılımlar kurulamaz.
- Üçüncü şahısların hukuk bürosu internetini kullanmaları Bilgi Teknolojileri çalışanlarının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.
- Ağ üzerinde kullanıcının erişeceği servisler kısıtlanıp, sınırsız ağ erişimi engellenmektedir.
- Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmıştır.
- Firewall olarak kullanılan cihazlar başka bir amaç için kullanılmamaktadır.
- Firewall konfigürasyonu kritik güncellemeleri Bilgi İşlem Müdürü onaylı yapılmaktadır.

- Ağ cihazlarının güncel topolojisi tutularak, konfigürasyon bilgileri saklanmaktadır.

4.2.2. Yazılım Güncellemeleri

- Kullanılmayan yazılım ve servislerin cihazlardan kaldırılması işlemi uygulanıp, güvenlik açıklarının önüne geçilmektedir.
- Kullanılan yazılım, servis ve donanımların yama yönetimleri ve yazılım güncellemeleri düzenli olarak kontrol edilmektedir.
- Yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığı düzenli olarak kontrol edilmektedir.

4.2.3. Erişim Sınırlamaları

- Kişisel veri içeren sistemlere erişim sınırlı tutulmaktadır.
- Erişim yetki ve kontrol matrisi oluşturularak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanımlanmış olup, kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanmaktadır.
- İş tanımı değişen veya hukuk bürosundan ayrılan çalışanların erişim hakları hemen silinmektedir.

4.2.4. Parola

- Şifre oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine küçük büyük harf, rakam hem dijit hem de noktalama karakterleri, sembollerden oluşacak güçlü şifre kombinasyonları tercih edilmektedir.
- Şifreler en az 6 (altı) ayda bir değiştirilmektedir.
- Şifre giriş deneme sayısı 5 (beş) ile sınırlandırılmıştır.

4.2.5. Anti-virüs Yazılımları

- Kötü amaçlı yazılımlardan korunmak için bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden anti-virüs programı kullanılmaktadır.
- Domaine bağlı pc'ler otomatik olarak bulundukları alt ağlardaki Sunucu'dan en son versiyonları update etmektedir.
- Domaine bağlı olmayan kullanıcılar ise, anti-virüs programının farklı güncelleme kurallarıyla güncel tutulması sağlanmaktadır.
- Çıkarılabilir medyalar (cd-rom, dvd-rom, bluetooth, flash disk, external disk) daima virüslere karşı tarama yapılmaktadır.

4.2.6. Kişisel Veri Güvenliğinin Takibi

- Sunucuların anti-virüs veri tabanlarını güncellemeleri düzenli ve kontrollü olarak yapılmaktadır.
- Veri tabanı sistemlerinin kesintisiz ve güvenli şekilde işletilmesine yönelik gerekli tedbirler alınmaktadır.

- Kullanılmayan servis ve uygulamalar kapatılmaktadır.
- Sunucular fiziksel olarak korunmuş sistem odalarında bulunmaktadır.
- Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmaktadır.
- Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan olaylar, port tarama atakları, yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması ile ilgili güvenlik logları sistem yöneticisi tarafından değerlendirilerek gerekli tedbirler alınıp, veri sorumlusuna bildirmektedir.
- Tüm kullanıcıların işlem hareketleri, log kayıtları düzenli olarak tutulmaktadır.
- Yılda bir kez Zafiyet ve Sızma (Penetrasyon) testleri yaptırılmakta, bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Hukuk bürosunun bilgisayar ağında sistem açıklarının tespit etmek ve gerekli tedbirlerin alınmasını sağlamak amacıyla kendi içerisinde ya da yetkili firmalara risk analizi yaptırılmaktadır.
- Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanıp güvenli bir şekilde saklanmaktadır.

4.2.7. Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

- Kâğıt ortamında saklanan kişisel veriler ve cihazlarda bulunan kişisel verilerin çalınması veya kaybolması gibi tehditlere karşı fiziksel güvenlik önlemleri alınmaktadır.
- Kullanım ömrü sona eren ve artık ihtiyaç kalmadığı kanaatine varılan kişisel verilere ait gizli bilgiler kâğıt öğütücü, yakma vb. metotlarla yok edilir.
- Sunucu ve ağ cihazlarının imha edilmesi durumlarında, depolama cihazında bulunan kişisel verilerin bir daha okunamaması önlemleri alınarak depolama cihazı fiziksel olarak imha edilir.
- Bilgisayar başından kalkarken oturumun kapatılması veya şifre ile aktif edilebilecek ekran koruyucuların devreye girmesi önlemleri alınır.
- Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kâğıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu sistem odası ve arşiv odasında tutulmaktadır.
- Sistem odası ve arşiv odasına giriş / çıkışlar kontrol altına alınmaktadır. Yetkisiz kişilerin erişimine kapalıdır.
- Hukuk Bürosu dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili güvenlik görevlileri gözetiminde gerçekleştirilmektedir.
- Kişisel veri içeren cihazların kaybolması veya çalınması gibi durumlara karşı erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemleri kullanılmaktadır.
- Kişisel verilerin yer aldığı fiziksel ortamların (sistem odası, arşiv odası) dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunmaktadır.
- Kişisel verilerin korunması amaçlı, cihazlarda tam disk şifreleme veya cihazda kişisel veri bulunan dosya da şifreleme işlemi uygulanmaktadır.
- Bilgisayarlar ve PDA cihazlar üzerinde anti-virüs programları yüklüdür ve hiçbir nedenle devre dışı bırakılamaz.
- Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifreleme kullanılmaktadır.

- Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için sayısal imzalar veya mesaj doğrulama kodları kullanılmaktadır.
- Bir olay veya faaliyetin oluşumu veya oluşmadığının kanıtını elde etmek için kriptografik teknikler kullanılmaktadır.

4.2.8. Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı

- Yeni sistemlerin tedariği, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmaktadır.
- Arızalandığı ya da bakım süresi geldiği için üretici, satıcı, servis gibi üçüncü kurumlara gönderilen cihazlar eğer kişisel veri içermekte ise bu cihazların bakım ve onarım işlemi için gönderilmesinden önce, kişisel verilerin güvenliğinin sağlanması için cihazlardaki veri saklama ortamının sökülerek saklanması, sadece arızalı parçaların gönderilmesi işlemi uygulanır.
- Bakım ve onarım gibi amaçlarla dışarıdan personel gelmişse kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemler alınmaktadır**.**

4.2.9. Kişisel Verilerin Yedeklenmesi

- Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde yedeklenen veriler kullanarak en kısa sürede faaliyete geçirilmektedir.
- Yedeklenen kişisel verilere sadece sistem yöneticisi tarafından erişilebilmektedir.
- Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenip, yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmaktadır.
- Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilip güncellenmektedir.
- Yedekleme işlemi yedekleme programı ajanının yedeği alınmak istenen bilgisayara kurularak network üzerinden yapılacak şekilde ayarlanmaktadır.
- Yedeğin sağlıklı bir şekilde alındığının kontrolü alınan yedeklerin sağlaması yapılarak kontrol edilmektedir.
- Tüm yedeklerin fiziksel güvenliği de ayrıca sağlanmaktadır.

4.3. Kişisel Veri Güvenliği İhlal Olayları Yönetimi

K&P Legal tarafından yürütülen kişisel veri işleme faaliyeti kapsamında, işlenen kişisel verilerin idari ve teknik tüm tedbirler alınmış olmasına rağmen, kanuni olmayan yollarla üçüncü kişiler tarafından ele geçirilmesi/ifşası durumunda;

- Kişisel veri güvenliği ihlal olaylarına hızlı etkili ve düzenli şekilde cevap verebilmek için kişisel veri güvenliği ihlal olayları karşısında çalışan öncelikli ve gerçek sorumludur. Böyle bir durumda çalışan öncelikli olarak kplegal.com.tr adresine durumu bildirmekle yükümlüdür.
- Kanun çerçevesinde yayımlanmış olan yönetmeliklerde belirtilen hükümlere aykırı düşen ve kuralları ihlal eden tutum, davranış ve olayların ortaya çıkması durumunda

izlenecek süreçler ve gerekliliklerine uymayan çalışanlara karşı "İhlal Bildirim Tutanağı" tutularak "Disiplin Politikası" işletilmektedir.

- Tespiti yapılan olay ile ilgili kurum dışı birim ya da firmalardan destek alınması gereken durumlarda iletişimi kurmak ve sağlamak konusunda öncelikli sorumluluk irtibat kişisidir.
- İrtibat kişisi ihlal ve olay bildirimini ilgili kişiye ve Kurula 72 saat içinde bildirmekle yükümlüdür.
- K&P Legal söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa K&P Legal web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapmakla yükümlüdür.
- K&P Legal bildirimin 72 saat içinde yapılamaması durumunda, Kurula haklı bir gerekçe ile yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula bildirmekle yükümlüdür.
- Kurula yapılacak bildirimde Kurulun yayınlamış olduğu "Kişisel Veri İhlal Bildirim Form"u kullanılacaktır.
- Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgilerin gecikmeye mahal verilmeksizin aşamalı olarak sağlanacaktır.
- K&P Legal tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulacaktır.

4.4. Kişisel Verilerin Korunmasına İlişkin Denetim Faaliyetlerinin Yürütülmesi

K&P Legal tarafından, kişisel verilerin korunması ve güvenliğinin sağlanması kapsamında alınan teknik ve idari tedbirlerin işleyişi denetlenmekte ve işleyişin devamını sağlayacak uygulamalar yürütülmektedir. Bu kapsamda gerçekleştirilen denetim faaliyetlerinin sonuçları, K&P Legal bünyesinde KVK Komitesi'ne ve ilgili departmana raporlanmaktadır. Denetim sonuçları doğrultusunda verilerin korunmasına ilişkin alınan tedbirlerinin geliştirilmesini ve iyileştirilmesini sağlayacak faaliyetler yürütülür.

5. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, K&P Legal tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

5.1. Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-1'te verilen yöntemlerle silinir.

Tablo 1: *Kişisel Verilerin Silinmesi*

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için Bilgi İşlem Departmanı 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, Bilgi İşlem Departmanı hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu çalışan hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, Bilgi İşlem Departmanı tarafından şifrelenerek ve erişim yetkisi sadece Bilgi İşlem Müdürü'ne verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

5.2. Kişisel Verilerin Yok Edilmesi

Kişisel veriler, K&P Legal tarafından Tablo-2'te verilen yöntemlerle yok edilir.

Tablo 2: *Kişisel Verilerin Yok Edilmesi*

Veri Kayıt Ortamı	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.

5.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

6. SAKLAMA VE İMHA SÜRELERİ

K&P Legal tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi gerçekleştirilir.

7. PERİYODİK İMHA SÜRELERİ

Yönetmeliğin 11 inci maddesi gereğince K&P Legal periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Kurumda her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

8. İLGİLİ KİŞİ BAŞVURU SÜREÇLERİ

Kanunda ilgili kişi olarak tanımlanan kişisel veri sahiplerine, Kanunun 11 inci maddesinde kişisel verilerinin işlenmesine ilişkin birtakım taleplerde bulunma hakkı tanınmıştır.

Kanunun 13 üncü maddesinin birinci fıkrası uyarınca; veri sorumlusu olan K&P Legal bu haklara ilişkin olarak yapılacak başvuruların yazılı olarak veya Kurul tarafından Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ kapsamında belirlenen diğer yöntemlerle tarafımıza iletilmesi gerekmektedir.
Bu çerçevede "yazılı" olarak K&P Legal-Erdal KARDAŞ Yelda TOPUZ KARDAŞ Ortaklığı'na yapılacak başvurular, başvuru formunun çıktısı alınarak;

- Başvuru Sahibinin şahsen başvurusu ile,
- Noter vasıtasıyla,
- İadeli taahhütlü posta yoluyla kimlik doğrulamak suretiyle,
- E-mail adresi vasıtasıyla, (erdal.kardas@kplegal.com.tr)

tarafımıza iletilebilecektir.

9. GÖZDEN GEÇİRME

İşbu Politika, K&P Legal KVK Komitesi tarafından her yıl en az 1 (bir) defa gözden geçirilerek gerekli olması halinde güncellenecektir. İşbu Politika'nın yürürlüğe girmesi, değiştirilmesi, yürütülmesi ve yürürlükten kaldırılması hususlarında K&P Legal KVK Komitesi yetkili ve sorumludur.

10. YÜRÜRLÜK

Bu politika üst yönetim tarafından onaylanmış ve 01.01.2019 tarihi itibariyle yürürlüğe girmiştir.