KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. Bu politikanın amacı, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektir.

2. Bu politika; 6698 sayılı Kanunun 7. maddesinin üçüncü fıkrası ile 22. maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanmış Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Yönetmeliğine uygun olarak hazırlanmıştır.

3. Şirket; Kişisel veri işleme envanterine uygun olarak bu kişisel veri saklama ve imha politikasını hazırlamıştır.

4. Tanımlar

4.1. Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.

4.2. 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 kişileridir

4.3. İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemidir.

4.4. 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.

4.5. Kişisel veri işleme envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanterdir.

4.6. Kişisel veri saklama ve imha politikası: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikadır.

4.7. Periyodik imha: Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini ifade eder.

4.8. Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini ifade eder.

4.9. Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.

4.10. Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

4.11. Kişisel verilerin silinmesi Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

4.12. Kişisel verilerin yok edilmesi Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

4.13. 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, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

5. Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamları:

5.1. Kâğıt ortamlar

5.2. Elektronik ortamlar

6. Kişisel verilerin saklanmasını ve imhasını gerektiren hukuki, teknik ya da diğer sebeplere ilişkin açıklamalar:

6.1. Kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir.

6.2. Türk Ceza Kanunu'nun 138. maddesinde ve KVK Kanunu'nun 7. maddesinde düzenlendiği üzere ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde Şirket kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hale getirilir.

6.3. İlgili kişi, Şirkete başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde bu talebi yerine getirilmek üzere hemen değerlendirmeye alınır.

6.4. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Şirket, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.

6.5. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa Şirket bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu politika kapsamında gerekli işlemlerin yapılmasını temin eder.

6.6. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

7. Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirler

7.1. Teknik Tedbirler

7.1.1. Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

7.1.2. Ağ yoluyla veri aktarımlarında kapalı sistem ağ kullanılmaktadır.

7.1.3. Anahtar yönetimi uygulanmaktadır.

7.1.4. Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.

7.1.5. Çalışanlar için yetki matrisi oluşturulmuştur.

7.1.6. Erişim logları düzenli olarak tutulmaktadır.

7.1.7. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.

7.1.8. Gerektiğinde veri maskeleme yöntemi uygulanmaktadır.

7.1.9. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.

7.1.10. Kişisel veri güvenliğinin takibi yapılmaktadır.

7.1.11. Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.

7.1.12. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.

7.1.13. Kişisel veri içeren ortamların güvenliği sağlanmaktadır.

7.1.14. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.

7.1.15. Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.

7.1.16. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

7.1.17. Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.

7.1.18. Mevcut risk ve tehditler belirlenmiştir.

7.1.19. Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.

7.1.20. Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.

7.1.21. Saldırı tespit ve önleme sistemleri kullanılmaktadır.

7.1.22. Sızma testi uygulanmaktadır.

7.1.23. Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.

7.1.24. Şifreleme yapılmaktadır.

7.1.25. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklara denetimi sağlanmaktadır.

7.1.26. Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

7.1.27. Veri kaybı önleme yazılımları kullanılmaktadır.

7.2. İdari Tedbirler

7.2.1. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

7.2.2. Çalışanlar için veri güvenliği konusunda belirli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

7.2.3. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.

7.2.4. Gizlilik taahhütnameleri yapılmaktadır.

7.2.5. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.

7.2.6. Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.

7.2.7. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.

7.2.8. Kişisel veri içeren ortamların güvenliği sağlanmaktadır.

7.2.9. Kişisel veriler mümkün olduğunca azaltılmaktadır.

7.2.10. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

7.2.11. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler mevcuttur.

8. Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirler

8.1. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili bütün işlemler yetkili kişiler tarafından politika ve prosedürlere uygun olarak yapılır ve kayıt altına alınır.

8.2. Söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

9. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi Teknikleri

9.1. Fiziksel Olarak Yok Etme Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler silinirken/yok edilirken kişisel verinin sonradan kullanılamayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Örnek: İlgili dosyanın, belgenin parçalanarak çöpe atılması.

9.2. Yazılımdan Güvenli Olarak Silme Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; çok yüksek ihtimalle bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

9.3. Uzman Tarafından Güvenli Olarak Silme Şirket bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından bir daha kurtarılamayacak biçimde güvenli olarak silinir/yok edilir.

9.4. Kişisel Verileri Anonim Hale Getirme Teknikleri

9.4.1. Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder. Şirket, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir.

9.4.2. KVK Kanunu'nun 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler KVK Kanunu kapsamı dışındadır. Anonim hale getirilerek işlenen kişisel veriler KVK Kanunu kapsamı dışında olacağından politikanın 10. Bölümünde düzenlenen haklar bu veriler için geçerli olmayacaktır.

9.4.3. Maskeleme (Masking) Veri maskeleme, kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir. Örnek: Kişisel veri sahibinin tanımlanmasını sağlayan isim, T.C. Kimlik No, ad-soyad vb. bilginin çıkartılması yoluyla kişisel veri sahibinin tanımlanmasının imkânsız hale geldiği bir veri setine dönüştürülmesi.

9.4.4. Toplulaştırma (Aggregation) Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örnek: Müşterilerin doğum yıllarını tek tek göstermeksizin 1975 yılında doğan 100 müşteri bulunduğunun ortaya konulması.

9.4.5. Veri Türetme (Data Derivation) Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örnek: Doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen ilçenin veya şehrin belirtilmesi.

9.4.6. Veri Karma (Data Shuffling, Permutation) Veri karma yöntemi ile kişisel veri seti içindeki değerlerinin karıştırılarak değerler ile kişiler arasındaki bağın kopartılması sağlanmaktadır. Örnek: Ses kayıtlarının niteliğinin değiştirilerek sesler ile veri sahibi kişinin ilişkilendirilemeyecek veya tanınamayacak hale getirilmesi.

10. Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimleri ve görev tanımları:

10.1. Bilgi İşlem Birimi Yöneticisi; Şirketin tüm Bilgi İşlem süreçlerini yönetir.

10.2. Hukuk Birimi Yöneticisi, Şirketin tüm hukuki işlem süreçlerini yönetir.

10.3. İnsan Kaynakları Yöneticisi (Personel ile ilgili konularda), Şirketin tüm personel süreçlerini yönetir.

10.4. Satış ve Pazarlama Yöneticisi (Müşteri bilgileri ile ilgili konularda); Şirketin tüm satış pazarlama süreçlerini yönetir.

11. Saklama ve imha sürelerini gösteren tablo

VERİ KATEGORİSİ	**VERİ SAKLAMA SÜRESİ**
Kimlik	10 YIL
İletişim	10 YIL
Lokasyon	2 YIL
Özlük	10 YIL
Hukuki İşlem	10 YIL
Müşteri İşlem	10 YIL
Fiziksel Mekân Güvenliği	2 YIL
İşlem Güvenliği	10 YIL
Risk Yönetimi	10 YIL
Finans	10 YIL
Mesleki Deneyim	10 YIL
Pazarlama	10 YIL
Görsel ve İşitsel Kayıtlar	10 YIL
Sağlık Bilgileri	10 YIL
Ceza Mahkûmiyeti ve Güvenlik Tedbirleri	10 YIL

Dernek Üyeliği	10 YIL
Vakıf Üyeliği	10 YIL

12. Periyodik imha süreleri,

12.1. Şirket saklama süresi dolan kişisel verileri saklama süresinin dolduğu tarihten itibaren en geç 180 gün içerisinde imha eder.

12.2. Şirket; kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

12.3. Periyodik imhanın gerçekleştirileceği zaman aralığı veri sorumlusu tarafından kişisel veri saklama ve imha politikasına, prosedürlere ve şirketin iş akışına uygun olarak belirlenir. Bu süre her halde altı ayı geçemez.

12.4. Şirket; kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir.