Özel Nitelikli Kişisel Veri Yönetimi Politikası

1. AMAÇ

Bu Politikanın amacı; veri sorumlusu nezdinde işlenen özel nitelikli kişisel verilerin, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK"), ilgili ikincil mevzuat, Kişisel Verileri Koruma Kurulu ("Kurul") kararları ve diğer ilgili mevzuata uygun olarak işlenmesine, muhafaza edilmesine, aktarılmasına, erişimlerinin sınırlandırılmasına, güvenliğinin sağlanmasına, saklama süresi sonunda silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektir. Bu Politika ile ayrıca; özel nitelikli kişisel verilerin hukuka ve dürüstlük kurallarına uygun şekilde işlenmesi, gizlilik, bütünlük ve erişilebilirliğinin korunması, yetkisiz erişim, ifşa, kayıp, değişiklik, tahrifat ve kötüye kullanım risklerine karşı korunması, KVKK'nın 6. ve 12. maddeleri kapsamındaki yükümlülüklerin yerine getirilmesi, özel nitelikli kişisel veriler için gerekli ilave idari ve teknik tedbirlerin belirlenmesi ve uygulanması, veri işleme faaliyetlerinin ölçülülük, veri minimizasyonu ve hesap verebilirlik ilkeleri doğrultusunda yürütülmesi amaçlanmaktadır.

2. KAPSAM

Bu Politika; veri sorumlusu tarafından işlenen özel nitelikli kişisel verilere ilişkin tüm işleme faaliyetlerini kapsar. Politika; başta aşağıdaki ilgili kişi grupları olmak üzere, özel nitelikli kişisel verisi işlenen tüm gerçek kişilere ilişkin süreçlere uygulanır: çalışanlar, çalışan adayları, stajyerler, eski çalışanlar, ziyaretçiler, tedarikçi/alt işveren çalışanları, iş ortakları yetkilileri ve çalışanları, müşteriler, misafirler, danışanlar ve benzeri ilgili kişiler. Bu Politika kapsamında işlenebilecek özel nitelikli kişisel veriler; ilgili mevzuat ve faaliyet konusu çerçevesinde işlenmesi gereken sağlık verileri, ceza mahkûmiyeti ve güvenlik tedbirlerine ilişkin veriler, biyometrik veriler, sendika üyeliği verileri, din/mezhep bilgisi gibi özel nitelikli kişisel verileri kapsar. Politika; özel nitelikli kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesi ile herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesine ilişkin fiziksel, elektronik, dijital, sözlü, yazılı ve görsel tüm veri işleme ortamlarına uygulanır.

3. DAYANAK

Bu Politika başta aşağıdaki mevzuata dayanılarak hazırlanmıştır:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- Veri Sorumluları Sicili Hakkında Yönetmelik,
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik,
- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ,
- Özel nitelikli kişisel verilerin işlenmesine ve veri güvenliğine ilişkin Kurul kararları, ilke kararları, rehberler ve duyurular,
- Faaliyet alanına göre uygulanması gereken İş Kanunu, İş Sağlığı ve Güvenliği mevzuatı, Türk Ticaret Kanunu ve diğer ilgili mevzuat hükümleri.

4. TANIMLAR

Açık rıza: Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi ifade eder.

Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.

Özel nitelikli kişisel veri: KVKK'nın 6. maddesinde sayılan; 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 mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerini ifade eder.

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.

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

5. TEMEL İLKELER

Özel nitelikli kişisel verilerin işlenmesinde aşağıdaki temel ilkelere uyulur:

1. Hukuka ve dürüstlük kurallarına uygun işleme,
2. Doğru ve gerektiğinde güncel olma,
3. Belirli, açık ve meşru amaçlar için işlenme,
4. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
5. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme,
6. Gizlilik, bütünlük ve erişilebilirliğin sağlanması,
7. Erişim yetkilerinin görev ve ihtiyaç esasına göre sınırlandırılması,
8. Hesap verebilirlik ve kayıt altına alma yükümlülüğünün yerine getirilmesi.

6. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN ESASLAR

6.1. Hukuki sebep ve işleme şartı

Özel nitelikli kişisel veriler, KVKK'nın 6. maddesinde yer alan işleme şartlarına uygun olarak işlenir. Özel nitelikli kişisel verilerin işlenmesinde, veri sorumlusu tarafından öncelikle ilgili veri işleme faaliyetinin hukuki sebebi tespit edilir ve veri işleme faaliyeti bu hukuki sebep ile sınırlı

olarak yürütülür. Açık rıza, ancak ilgili veri işleme faaliyeti bakımından KVKK'da öngörülen uygun işleme şartının bulunmadığı veya açık rıza alınmasının hukuken gerekli olduğu durumlarda alınır. Açık rıza alınması halinde, açık rıza metni aydınlatma metninden ayrı düzenlenir ve açık rıza belirli bir konuya ilişkin, bilgilendirmeye dayalı ve özgür iradeyle verilmiş olmalıdır.

6.2. Aydınlatma yükümlülüğü

Özel nitelikli kişisel verilerin işlenmesi süreçlerinde ilgili kişilere, KVKK'nın 10. maddesi kapsamında gerekli aydınlatma yapılır. Aydınlatma metinlerinde, işlenen veri kategorileri, işleme amaçları, hukuki sebepler, aktarım alıcı grupları, toplama yöntemi ve ilgili kişinin haklarına açık şekilde yer verilir.

6.3. Veri minimizasyonu ve amaçla sınırlılık

Özel nitelikli kişisel veriler yalnızca açıkça belirlenmiş işleme amacı için gerekli olduğu ölçüde işlenir. İşleme amacıyla ilgisiz, gereksiz veya aşırı veri toplanamaz. Her veri işleme sürecinde veri minimizasyonu ilkesi esas alınır.

7. İDARİ TEDBİRLER

Özel nitelikli kişisel verilerin güvenliğini sağlamak amacıyla veri sorumlusu tarafından aşağıdaki idari tedbirler alınır:

1. Özel nitelikli kişisel veri işleme süreçleri belirlenir, kayıt altına alınır ve gerektiğinde güncellenir.
2. Özel nitelikli kişisel veri işleyen birimler, süreçler ve sistemler veri envanterinde açık şekilde gösterilir.
3. Görev tanımları, yetki ve sorumluluklar belirlenir; çalışanların erişim yetkileri görev ve ihtiyaç esasına göre tanımlanır.
4. Erişim yetki matrisi oluşturulur, yetkiler düzenli aralıklarla gözden geçirilir; görev değişikliği veya işten ayrılma halinde erişim yetkileri derhal revize edilir veya kaldırılır.
5. Çalışanlara genel KVKK farkındalık eğitimi verilir; İnsan Kaynakları, Bilgi Teknolojileri, İş Sağlığı ve Güvenliği, hukuk/uyum ve özel nitelikli kişisel veri işleyen diğer personele görev alanına uygun ilave eğitimler sağlanır.
6. Veri işleyenlerle imzalanan sözleşmelere, gizlilik, veri güvenliği, alt işleyen kullanımı, ihlal bildirimi, denetim ve imha yükümlülüklerine ilişkin hükümler eklenir.
7. Özel nitelikli kişisel verilerin işlendiği süreçler bakımından periyodik risk değerlendirmeleri yapılır; gerekli görülen durumlarda düzeltici ve önleyici tedbirler planlanır.
8. Özel nitelikli kişisel verilerin işlendiği süreçlerde kullanılan formlar, klasörler, arşiv alanları ve sistemler veri sınıflandırma kurallarına uygun şekilde tanımlanır.

9. İlgili kişi başvuruları, talepleri ve şikâyetleri kayıt altına alınır; mevzuattaki süreler içinde sonuçlandırılır.
10. Politika, prosedür ve talimatlar düzenli aralıklarla gözden geçirilir ve ihtiyaç halinde güncellenir.

8. TEKNİK TEDBİRLER

Özel nitelikli kişisel verilerin işlendiği elektronik/dijital ortamlarda aşağıdaki teknik tedbirler uygulanır:

1. Veriler mümkün olduğu ölçüde kriptografik yöntemlerle korunur.
2. Kriptografik anahtarlar güvenli ortamlarda saklanır ve yetkisiz erişime karşı korunur.
3. Özel nitelikli kişisel verilere erişim, görüntüleme, değiştirme, aktarma ve silme işlemleri mümkün olduğu ölçüde loglanır.
4. Log kayıtları düzenli olarak kontrol edilir, bütünlüğü korunur ve güvenli şekilde saklanır.
5. Kullanıcı hesapları kişiye özel tanımlanır; ortak kullanıcı hesabı kullanımından kaçınılır.
6. Güçlü parola politikası uygulanır; gerekli görülen sistemlerde çok faktörlü kimlik doğrulama kullanılır.
7. Uzaktan erişim gereken durumlarda, güvenli bağlantı yöntemleri (örneğin VPN), çok faktörlü kimlik doğrulama ve oturum güvenliği tedbirleri uygulanır.
8. Sistem, uygulama, sunucu, ağ cihazı ve güvenlik yazılımlarına ilişkin güncelleme ve yamalar zamanında yapılır.
9. Anti-virüs, EDR/XDR, güvenlik duvarı, saldırı tespit/önleme ve benzeri uygun güvenlik önlemleri risk seviyesine göre uygulanır.
10. Güvenlik testleri, zafiyet taramaları ve gerekli görülen diğer kontroller düzenli olarak yapılır veya yaptırılır; sonuçlar kayıt altına alınır ve iyileştirme faaliyetleri takip edilir.
11. Verilere bir yazılım aracılığıyla erişiliyorsa, uygulama bazlı yetkilendirme, erişim kontrolü ve güvenlik testleri sağlanır.
12. Yedekleme süreçlerinde özel nitelikli kişisel verilerin güvenliği ayrıca dikkate alınır; yedeklere erişim sınırlandırılır ve uygun koruma tedbirleri uygulanır.

9. FİZİKSEL GÜVENLİK TEDBİRLERİ

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği veya erişildiği fiziksel ortamlarda aşağıdaki tedbirler alınır:

1. Özel nitelikli kişisel veri içeren fiziksel dosya, arşiv, klasör, dolap ve odalara erişim yalnızca yetkili kişilerle sınırlandırılır.
2. Fiziksel arşiv alanları, dolaplar ve veri saklama alanları mümkün olduğu ölçüde kilitli, kontrollü ve izlenebilir şekilde korunur.
3. Yetkisiz kişilerin bu alanlara erişimi engellenir; gerekli görülen durumlarda refakat kuralı uygulanır.

4. Fiziksel ortamların niteliğine uygun olarak yangın, su baskını, elektrik kaçağı, hırsızlık, sabotaj ve benzeri risklere karşı uygun güvenlik tedbirleri alınır.
5. Özel nitelikli kişisel veri içeren fiziksel kayıtlar, veri sınıflandırma ve gizlilik derecelendirme kurallarına uygun şekilde işaretlenebilir ve ayrıştırılabilir.
6. Kağıt ortamındaki özel nitelikli kişisel verilerin masa üstünde, ortak kullanım alanlarında veya yetkisiz kişilerin görebileceği ortamlarda açıkta bırakılmaması sağlanır.

10. AKTARIM GÜVENLİĞİ

10.1. Genel esaslar

Özel nitelikli kişisel veriler, yalnızca işleme amacıyla bağlantılı, gerekli ve ölçülü olmak kaydıyla; KVKK, ilgili mevzuat ve veri aktarımına ilişkin güncel düzenlemelere uygun olarak aktarılır. Aktarım öncesinde verinin niteliği, aktarım amacı, alıcının sıfatı ve aktarım yöntemi değerlendirilir.

10.2. Yurt içi aktarım

Yurt içi aktarım süreçlerinde, aktarımın hukuki sebebi belirlenir; veri aktarımı güvenli iletişim kanalları, erişim kısıtları ve uygun idari/teknik tedbirler eşliğinde gerçekleştirilir.

10.3. Yurt dışı aktarım

Özel nitelikli kişisel verilerin yurt dışına aktarımı, KVKK, ilgili ikincil mevzuat, Kurul kararları ve yürürlükteki veri aktarım düzenlemelerine uygun şekilde gerçekleştirilir. Yurt dışı aktarım süreçlerinde gerekli hukuki mekanizmalar, sözleşmesel güvenceler ve teknik/idari güvenlik tedbirleri ayrıca değerlendirilir.

10.4. Aktarım yöntemleri bakımından güvenlik

1. E-posta ile aktarım gerekiyorsa mümkün olduğu ölçüde kurumsal e-posta altyapısı kullanılmalı, gerekli hallerde şifreleme ve ek güvenlik önlemleri uygulanmalıdır.
2. Taşınabilir medya ile aktarım zorunlu ise veri şifrelenmeli, medya güvenli şekilde teslim edilmeli ve gerekli kayıtlar tutulmalıdır.
3. Sunucular arası veri aktarımında güvenli iletişim protokolleri ve erişim güvenliği tedbirleri uygulanmalıdır.
4. Kağıt ortamında aktarım zorunlu ise evrakın kaybolması, çalınması veya yetkisiz kişilerce görülmesi risklerine karşı uygun idari ve fiziksel önlemler alınmalıdır.

11. SAKLAMA, İMHA VE GÜNCELLEME

1. Özel nitelikli kişisel veriler, yalnızca ilgili işleme amacı için gerekli olan süre boyunca ve ilgili mevzuatta öngörülen saklama süreleri dikkate alınarak muhafaza edilir.
2. Saklama süresi sona eren veya işlenmesini gerektiren amaç ortadan kalkan özel nitelikli kişisel veriler; KVKK, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ve veri saklama-imha politikası doğrultusunda silinir, yok edilir veya anonim hale getirilir.
3. Güncellenmesi gereken verilerin doğru ve güncel tutulması için ilgili süreç sahipleri tarafından gerekli kontroller yapılır.
4. İmha süreçleri kayıt altına alınır ve gerektiğinde ispatlanabilir şekilde muhafaza edilir.

12. ERİŞİM KONTROLLERİ VE DENETİM

1. Özel nitelikli kişisel verilere erişim yetkileri yılda en az bir kez gözden geçirilir.
2. Ayrıcalıklı kullanıcı hesapları ve kritik erişimler düzenli olarak denetlenir.
3. Politika kapsamındaki süreçler, gerektiğinde iç denetime, KVKK uyum kontrollerine, bilgi güvenliği denetimlerine ve ikinci taraf denetimlerine tabi tutulur.
4. Veri işleyen hizmet sağlayıcıları, sözleşmesel yükümlülükler ve risk durumu dikkate alınarak uygun aralıklarla denetlenebilir veya güvence mekanizmalarına tabi tutulabilir.

13. İLGİLİ KİŞİ BAŞVURULARI, ŞİKÂYETLER VE AÇIK RIZANIN GERİ ALINMASI

1. İlgili kişiler, KVKK'nın 11. maddesi kapsamındaki haklarını Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun şekilde kullanabilir.
2. Başvurular yazılı, kayıtlı elektronik posta (KEP), kurumsal e-posta, noter veya veri sorumlusu tarafından duyurulan diğer yöntemlerle alınabilir.
3. Başvurular kayıt altına alınır, değerlendirilir ve yasal süreler içinde cevaplandırılır.
4. Açık rızaya dayalı bir işleme faaliyeti söz konusu ise, ilgili kişinin açık rızasını geri alması halinde, geri alma talebinin hukuki ve fiili sonuçları değerlendirilir; açık rızaya dayanan veri işleme faaliyetleri durdurulur veya ilgili süreç mevzuata uygun şekilde yeniden yapılandırılır.
5. İlgili kişi şikâyetleri, gerekli hallerde KVKK Komitesi, ilgili birim yöneticileri, hukuk/uyum birimi, insan kaynakları veya bilgi işlem birimi ile koordineli şekilde değerlendirilir.

14. KİŞİSEL VERİ İHLALİ YÖNETİMİ

1. Özel nitelikli kişisel verilerin hukuka aykırı olarak elde edilmesi, erişilmesi, ifşa edilmesi, kaybedilmesi, silinmesi, değiştirilmesi veya benzeri güvenlik ihlali şüphesi ortaya çıktığında durum derhal yetkili iç temas noktalarına bildirilir.
2. Veri ihlali şüphesi, yetkili birimler tarafından ivedilikle değerlendirilir; ihlalin kapsamı, etkileri, ilgili kişi sayısı, veri kategorileri ve risk düzeyi tespit edilmeye çalışılır.

3. Gerekli görülen teknik, idari ve hukuki tedbirler gecikmeksizin alınır; olay kayıt altına alınır.
4. KVKK'nın 12. maddesi kapsamında Kurul'a ve ilgili kişilere yapılması gereken bildirimler mevzuata uygun şekilde yerine getirilir.
5. Veri ihlali sonrasında kök neden analizi yapılarak tekrarını önleyici tedbirler planlanır.

15. SORUMLULUKLAR

15.1. Üst Yönetim

- Bu Politikanın uygulanması için gerekli organizasyonel desteğin ve kaynakların sağlanmasından,
- politika ve ilgili süreçlerin onaylanmasından,
- gerekli görülen düzeltici/önleyici faaliyetlerin desteklenmesinden sorumludur.

15.2. KVKK Komitesi / Uyum Birimi

- Politikanın hazırlanması, gözden geçirilmesi, güncellenmesi ve uygulanmasının izlenmesinden,
- özel nitelikli kişisel veri işleme süreçlerine ilişkin uyum çalışmalarının koordine edilmesinden,
- risk, denetim, eğitim ve iyileştirme faaliyetlerinin takibinden sorumludur.

15.3. Veri Sorumlusu İrtibat Kişisi

- İlgili kişi başvurularının ve KVKK kapsamındaki iletişim süreçlerinin koordinasyonundan,
- Kurum ile yapılacak iletişim ve bildirim süreçlerinin takibinden,
- gerekli kayıtların tutulmasına destek olunmasından sorumludur.

15.4. İnsan Kaynakları Birimi

- Çalışan, çalışan adayı ve benzeri personel süreçlerinde işlenen özel nitelikli kişisel verilerin hukuka uygun şekilde toplanması, işlenmesi, muhafaza edilmesi ve gerekli durumlarda imhasına ilişkin süreçlerin yürütülmesinden,
- özlük dosyaları ve personel süreçlerinde gerekli gizlilik ve erişim tedbirlerinin uygulanmasından sorumludur.

15.5. Bilgi Teknolojileri / Bilgi İşlem Birimi

- Özel nitelikli kişisel verilerin işlendiği bilgi sistemlerinde erişim güvenliği, loglama, yedekleme, güncelleme, şifreleme, uzaktan erişim güvenliği ve diğer teknik tedbirlerin uygulanmasından,
- bilgi sistemleri kaynaklı güvenlik risklerinin izlenmesinden ve gerekli teknik önlemlerin alınmasından sorumludur.

15.6. İş Sağlığı ve Güvenliği / İşyeri Hekimi / Sağlık Süreçlerini Yürüten Birimler

- Sağlık verileri başta olmak üzere kendi faaliyet alanlarında işlenen özel nitelikli kişisel verilerin hukuka uygun şekilde işlenmesi, gizliliğinin korunması ve yalnızca yetkili kişilerce erişilmesinin sağlanmasından sorumludur.

15.7. Birim Yöneticileri

- Kendi sorumluluk alanlarındaki özel nitelikli kişisel veri işleme faaliyetlerinin bu Politika'ya uygun şekilde yürütülmesini sağlamaktan,
- çalışanların erişim yetkilerini ve veri işleme ihtiyaçlarını gözden geçirmekten,
- uygunsuzlukları ilgili birimlere bildirmekten sorumludur.

15.8. Tüm Çalışanlar

- Bu Politika, ilgili prosedürler, talimatlar ve veri güvenliği kurallarına uygun davranmaktan,
- görevleri kapsamında öğrendikleri özel nitelikli kişisel verilerin gizliliğini korumaktan,
- olası veri ihlali, güvenlik zafiyeti veya uygunsuzlukları gecikmeksizin bildirmekten sorumludur.

15.9. Veri İşleyenler ve Hizmet Sağlayıcılar

- Veri sorumlusunun talimatlarına, sözleşmesel yükümlülüklere ve veri güvenliği kurallarına uygun hareket etmekten,
- işledikleri özel nitelikli kişisel verilerin güvenliğini sağlamaktan,
- ihlal, kayıp veya yetkisiz erişim durumlarında veri sorumlusunu gecikmeksizin bilgilendirmekten sorumludur.

16. YÜRÜRLÜK VE GÖZDEN GEÇİRME

Bu Politika, veri sorumlusu tarafından onaylandığı tarihte yürürlüğe girer. Politika; mevzuat değişiklikleri, Kurul kararları, iç denetim bulguları, teknik gelişmeler, organizasyonel değişiklikler ve ihtiyaçlar doğrultusunda periyodik olarak gözden geçirilir ve gerektiğinde güncellenir.