RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

2024

İÇİNDEKİLER

1. AMAÇ 3
2. KAPSAM 3
3. TANIMLAR VE KISALTMALAR 3
4. KAYIT ORTAMLARI 5
5. ROL VE SORUMLULUK 6
6. HUKUKİ YÜKÜMLÜLÜKLER… 6
6.1 Aydınlatma Yükümlülüğü 6
6.2 Veri Güvenliğini Sağlama Yükümlülüğü 6
7. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR 7
7.1. Saklamaya İlişkin Açıklamalar… 7
7.2. Saklamayı Gerektiren Hukuki Sebepler 7
7.3. İmhayı Gerektiren Sebepler… 8
8. TEKNİK VE İDARİ TEDBİRLER 8
8.1. Teknik Tedbirler… 8
8.2. İdari Tedbirler 9
9. KİŞİSEL VERİ İMHA YÖNTEMLERİ… 8
9.1. Kişisel Verilerin Silinmesi 10
9.2. Kişisel Verilerin Yok Edilmesi… 11
9.3. Anonim Hale Getirme… 11
10. SAKLAMA VE İMHA SÜRELERİ… 12
11. POLİTİKANIN YAYINLANMASI VE SAKLANMASI… 12
12. POLİTİKANIN GÜNCELLENMESİ… 12

1. AMAÇ

RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ tarafından gerçekleştirilmekte olan saklama ve imha (silinme, yok etme, anonim hale getirme) faaliyetlerine ilişkin işlemler hakkında usul ve esasları belirlemek maksadıyla **"Kişisel Veri Saklama ve İmha Politikası"** hazırlanmıştır.

RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ tarafından temel ilkeler doğrultusunda; çalışan, hissedar/ortak, çalışan adayları, gerçek kişi müşteri/çalışanı/yetkilisi, tüzel kişi müşterinin çalışanı/yetkilisi, potansiyel iş ortaklarının çalışanı/yetkilisi, iş ortaklarının çalışanı/yetkilisi, üçüncü kişi ziyaretçiler şeklinde kategorize edilen gerçek kişilere ait kişisel verilerin Anayasa, Uluslararası Sözleşmeler, GDPR, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir. Kişisel verilerin saklanması ve imhasına ilişkin işlemler, bu doğrultuda hazırlanan politikaya uygun olarak gerçekleştirilir.

2. KAPSAM

RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ'nin çalışan, hissedar/ortak, çalışan adayları, potansiyel gerçek kişi müşteri/ müşteri çalışanı/yetkilisi, gerçek kişi müşteri/ müşteri çalışanı/yetkilisi, iş ortaklarının çalışanı/yetkilisi, üçüncü kişi ziyaretçiler şeklindeki gerçek kişilere ait kişisel veriler bu politika kapsamındadır.

Şirket tarafından toplanan, Şirket'e aktarılan ve Şirket tarafından işlenen tüm kişisel verilere ilişkin silme, yok etme veya anonimleştirmesine ilişkin kuralları düzenler ve Şirket'in sahip olduğu kişisel verilerin kendi bünyesinde veya 3. Kişi bünyesinde işlendiği ve/veya paylaşıldığı tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu politika uygulanır.

3. TANIMLAR VE KISALTMALAR

Alıcı Grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.

Anonim Hale Getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.

Çalışan: Şirket çalışanı.

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: Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.

İlgili Kişi: Kişisel Verisi İşlenen 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.

Kanun: 6698 Sayılı Kişisel Verilerin Korunması Kanunu.

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.

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü 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, varsa 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.

Kurum: Kişisel Verileri Koruma Kurumu.

Özel Nitelikli Kişisel Veri: Kanunun 6. maddesi uyarınca, öğrenilmesi halinde ilgili kişiler hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki verilerdir. Kanuna göre bu veriler; 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 verilerdir.

Periyodik İmha: 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 işlemi.

Politika: Kişisel Verileri Saklama ve İmha Politikası.

Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicili.

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen 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 kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.

Yönetmelik: 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

4. KAYIT ORTAMLARI

Kişisel veriler, Şirket tarafından Tablo 1'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 1: Kişisel Veri Saklama Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
➢ Sunucular (Etki alanı, bulut, yedekleme, e-posta, veritabanı, web, dosya paylaşım vb.) ➢ Yazılımlar (ofis yazılımları, portal) ➢ Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) ➢ Kişisel bilgisayarlar (Masaüstü, dizüstü bilgisayar) ➢ Mobil cihazlar (telefon, tablet vb.) ➢ Optik diskler (CD, DVD vb.) ➢ Çıkartılabilir bellekler (USB, Hafıza Kart vb.)	➢ Kağıt ➢ Manuel veri kayıt sistemleri (ziyaretçi giriş defteri) ➢ Yazılı, basılı, görsel ortamlar

5. ROL VE SORUMLULUK

RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ'nin bütün çalışan ve birimleri, 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.

Şirket işbu Politika'nın onaylanmasından sorumludur. İşbu Politika'nın oluşturulmasının, yayınlanmasının, gerektiğinde güncellenmesinin ve yürürlükten kaldırılmasının sağlanması konusunda yetkili onay mekanizmasıdır. Politika ile ilgili uygulamaların yürürlüğe alınması, şirket bünyesinde faaliyetlerin etkinliğinin artırılması ve denetlenmesi Şirket'in sorumluluğundadır. Şirket ilgili birimleri belirleyerek yetki ve denetleme işleminin yürütülmesine dair tedbirleri alır.

6. HUKUKİ YÜKÜMLÜLÜK

6.1. Aydınlatma Yükümlülüğü

Veri sorumlusu, 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un 10. maddesi çerçevesinde kişisel verilerin elde edilmesi sırasında bizzat veya yetkilendirdiği kişi aracılığıyla aşağıdaki bilgileri ilgili kişiye sağlamakla yükümlüdür:

• Veri sorumlusunun ve varsa temsilcisinin kimliği,

• Kişisel verilerin hangi amaçla işleneceği,

• Kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,

• Kişisel veri toplamanın yöntemi ve hukuki sebebi,

• Kanunun 11. maddesinde sayılan diğer hakları,

6.2. Veri Güvenliğini Sağlama Yükümlülüğü

Kanunun veri güvenliğine ilişkin 12. maddesine göre veri sorumlusu;

• Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

• Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

• Kişisel verilerin muhafazasını sağlamak,

ile yükümlüdür.

7. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

ŞİRKET tarafından; çalışan, hissedar/ortak, çalışan adayları, gerçek kişi müşteri/çalışanı/yetkilisi, tüzel kişi müşterinin çalışanı/yetkilisi, potansiyel iş ortaklarının çalışanı/yetkilisi, iş ortaklarının çalışanı/yetkilisi, üçüncü kişi ziyaretçiler şeklindeki gerçek kişilere ait kişisel veriler 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'a uygun olarak saklanır ve imha edilir.

Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

7.1. Saklamaya İlişkin Açıklamalar

6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un 3. maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4. 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. maddelerde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, **veri sorumlusu** olarak faaliyetlerimiz çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

7.2. Saklamayı Gerektiren Hukuki Sebepler

RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

• 6698 sayılı Kişisel Verilerin Korunması Kanunu,

• 6098 sayılı Türk Borçlar Kanunu,

• 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,

• 6102 sayılı Türk Ticaret Kanunu,

• 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,

• 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,

• 4857 sayılı İş Kanunu,

• 2828 sayılı Sosyal Hizmetler Kanunu,

• 213 sayılı Vergi Usul Kanunu,

• 6502 sayılı Tüketicinin Korunması Hakkında Kanun,

• İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

Kanunlarda süre öngörülmediği hallerde veriye olan ihtiyacın ortadan kalkmasına müteakip ilk periyodik imha işlemine kadar veri saklanmaktadır.

7.3. 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,

• 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun **RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ** tarafından kabul edilmesi,

• **RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ'nin** 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, **Şirket** tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

8. 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 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12. maddesi ve 6. maddesinin dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde **veri sorumlusu şirket** tarafından teknik ve idari tedbirler alınır.

8.1. Teknik Tedbirler

RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Şifreleme yapılmaktadır.

.

8.2. İdari Tedbirler

- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.

- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

9. KİŞİSEL VERİ İMHA YÖNTEMLERİ

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

9.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. İlgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması ve Yönetmelik'te düzenlenmiş hallerin ortaya çıkması halinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri siler veya yok eder.

Veriler silinirken mevzuatta öngörülen işlem/standartlara ve aşağıda yer alan kurallara uyulmalıdır:

- Veriler kayıtlı oldukları fiziki evraklardan silinmelidir.
- Veriler kayıtlı oldukları fiziki dosyalardan silinmelidir.
- Veriler kayıtlı oldukları sayısal ortamlardan silinmelidir.
- Veriler kayıtlı oldukları kamera kayıtları veya teyp yedekleri gibi manyetik ortamlardan silinmelidir.
- Sayısal veya manyetik ortamların içinde bulunmakla birlikte tüm ortamın imhasının gerekmediği durumlarda verilerin silinmesi işlemleri yapılmalıdır.
- Veriler kayıtlı oldukları aktif kullanımda olmayan yedekleme cihazları ve yedekleme amaçlı kullanılan depolama birimleri (örneğin bulut depolama vb.) üzerinden silinmelidir.
- Tamamen veya kısmen otomatik olan yollarla işlenen ve sayısal ortamlarda muhafaza edilen veriler ilgili yazılımın veri silinmesine ilişkin yöntemleri ile silinir.

9.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde

erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Yok etme işlemi, verilerin fiziksel kayıt ortamlarında işlendiği durumlarda yapılacaktır. Yok etme işlemi ile bu veriler, tekrar geri getirilmesi mümkün olmayacak hale getirilmektedir.

Veriler yok edilirken mevzuatta öngörülen işlem/standartlara ve aşağıda yer alan kurallara uyulmalıdır:

- Veriler tekrar kullanılamayacak şekilde, kaydedildiği fiziki evraktan imha edilir.
- Veriler tekrar kullanılamayacak şekilde, kaydedildiği fiziki dosyalardan imha edilir.
- Veriler tekrar kullanılamayacak şekilde, kaydedildiği sayısal ortamlar imha edilir.
- Veriler tekrar kullanılamayacak şekilde, kaydedildiği manyetik ortamlar imha edilir.
- Sayısal veya manyetik ortamlarda bulunmakla birlikte tüm ortamın imhasını gerektirmeyecek olan silme işlemleri yapılır ve veriler imha edilir.

9.3. 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.

Aşağıda belirtilen örnek yöntemler ve mevzuatta öngörülen işlem/standartlar ile kişisel verilerin anonimleştirilmesi işlemi sağlanabilir:

a) Veri Maskeleme

Doğrudan tanımlayıcı olabilecek kişisel verinin şifrelenerek veri tabanı üzerinde korunması veya tekilliği ortadan kaldıracak şekilde saklanması ve ilgili kişinin verisinin geriye dönük olarak belirlenmesinin engellenmesidir. Örneğin ilgili kişinin talebi üzerine kişisel verileri içindeki T.C. Kimlik numarası alanı veri tabanı içinde sha512 veya benzeri bir şifreleme yöntemiyle maskelenebilir. Ancak ilgili kişinin adı için aynı yöntem uygulanmaz, çünkü aynı ada sahip olabilecek kişilerden yola çıkarak yapılabilecek bir süzme işleminde tekil kişiye ulaşma durumu söz konusu olabilir. Maskelemeye ilişkin başka bir örnek ise; parmak izi görüntüsünün yok edilmesi sırasında hep aynı grafik bilgisinin verinin üzerine basılmasıdır.

b) Veri Türetme

Kişisel verilerin ilgili kişiyle ilişkilendirilmesini engellemek amacıyla başta parazit yayma veya rastgele karakter serpiştirme gibi yöntemlerle geri dönüşümü olanaksız olarak yeniden yapılandırılmasıdır. Örneğin ilgili kişiyi tekilleştirebilecek biçimdeki açık adreslerdeki il verisini gruplama amaçlı sabit tutup kalan alanlardaki (sokak, ev numarası vb.) bilgilerin rastgele karakterlerle doldurulması gibi.

Anonimleştirme işlemleri sırasında, veri alanlarının özelliklerine göre farklı yöntemler, aynı veri grubunun değişik veri alanlarındaki veri tabanlarının ve ilgili yazılımların izin verdiği ölçüde kullanılabilir. Örneğin T.C. Kimlik numarası için farklı, adres için farklı yöntemler kullanılarak anonimleştirme yapılabilir. Başarılı şekilde anonimleştirilen bilgiler, artık kişisel veri olarak kabul edilemez. Bu durumda, anonimleştirme işlemi için ilgili kişinin açık rızası aranmayacaktır ve ilgili kişi anonim hale getirilen bilgiler hakkında KVKK ve ilgili mevzuatta belirtilen haklarını kullanamayacaktır.

10. SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından, faaliyetleri kapsamında işlenmekte olan kişisel veriler yasal mevzuat sürelerine uygun olarak saklanır ve saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Veri Sorumlusu tarafından yerine getirilir.

Yönetmeliğin 11. maddesi gereğince **RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ** periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, şirkette her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

11. POLİTİKANIN YAYIMLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında ayrıca yayımlanır.

12. POLİTİKANIN GÜNCELLENMESİ

Politika, ihtiyaç duyuldukça güncellenir ve yeniden yayımlanır.

RHİNO TECH DANIŞMANLIK LİMİTED ŞİRKETİ