ELMOR TESİSAT MALZEMESİ TİCARET A.Ş.

Tic.Sicil No: 88120

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

VERSİYON

Versiyon No	Versiyon Tarihi	Değişiklik Açıklaması
01	01.09.2021	-
02	04.01.2023	Mevzuat ve Kurul Kararı değişiklikleri sebebiyle

İÇİNDEKİLER

1. GİRİŞ 3
1.1. Amaç 3
1.2. Kapsam 3
2. TANIMLAR 3
3. İLKELER 4
4. KAYIT ORTAMLARI 4
5. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR 5
5.1. Saklamaya İlişkin Açıklamalar 5
5.2. Saklamayı Gerektiren Hukuki Sebepler 5
5.3. Saklamayı Gerektiren İşleme Amaçları 6
5.4. İmhayı Gerektiren Sebepler 7
6. TEKNİK VE İDARİ TEDBİRLER 7
7. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ 9
7.1. Kişisel Verilerin Silinmesi 9
7.2. Kişisel Verilerin Yok Edilmesi 10
7.3. Kişisel Verilerin Anonim Hale Getirilmesi 12
8. BİRİMLER VE GÖREVLERİ 16
9. SAKLAMA VE İMHA SÜRELERİ 16
10. DİĞER HUSUSLAR 16
EK-1 SAKLAMA VE İMHA SÜRECİNDE YER ALAN BİRİMLER VE GÖREVLERİ TABLOSU 17
EK-2 SAKLAMA VE İMHA SÜRELERİ TABLOSU 18

1. GİRİŞ

1.1. Amaç

İşbu Kişisel Veri Saklama ve İmha Politikası ("**Politika**"), 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 28 Ekim 2017 tarihli Resmi Gazete'de yayımlanarak 1 Ocak 2018 tarihi itibariyle yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca veri sorumlusu sıfatını haiz olan Elmor Tesisat Malzemesi Ticaret A.Ş. ("**Şirket**") tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır. Politika ile kişisel verilerinizin işlendikleri amaç için gerekli olan azami süreyi belirleme esasları ile silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirme sağlanması amaçlanmaktadır.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Şirketimiz tarafından bu doğrultuda hazırlanmış olan Politika'ya uygun olarak gerçekleştirilir.

1.2. Kapsam

İşbu Politika'nın kapsamına Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler dahil olup, Şirket'in sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

2. TANIMLAR

- **Açık Rıza:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
- **Alıcı Grubu:** Veri Sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
- **Elektronik Ortam:** Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
- **Elektronik Olmayan Ortam:** Elektronik ortamların dışında kalan tüm yazılı, basılı ve diğer otamlar.
- **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.
- **Hizmet Sağlayıcı:** Şirketimiz'e belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
- **Kayıt Ortamı**: Tamamen veya kısmen otomatik olan ya da herhangi bir verikayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı.
- **KVKK:** 6698 Sayılı Kişisel Verilerin Korunması Kanunu.
- **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, 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 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, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem**.**
- **Kişisel Verilerin Anonim Hale Getirilmesi:** Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi işlemi.

- **Kişisel Verilerin Silinmesi:** Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
- **Kişisel Verilerin Yok Edilmesi:** Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
- **Kurul:** Kişisel Verileri Koruma Kurulu.
- **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 mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.
- **Periyodik İmha:** KVKK'da yer alan kişisel 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:** İşbu Kişisel Veri Saklama ve İmha Politikası.
- **Veri İşleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.
- **Veri Kayıt Sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistem.
- **Veri Sahibi/İlgili Kişi:** Kişisel verisi işlenen gerçek kişi.
- **Veri Sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
- **Veri Sorumluları Sicili Bilgi Sistemi/VERBİS:** Veri Sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kişisel Verileri Koruma Kurumu Başkanlığı tarafından oluşturulan ve yönetilen bilişim sistemi.
- **Yönetmelik:** 28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanan ve 1 Ocak 2018 tarihi itibariyle yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

3. İLKELER

Politika'nın hazırlanmasında, uygulanmasında ve kişisel verilerin işlenmesinde Yönetmelik'in 7. maddesinde yer alan aşağıdaki ilkelere uyulmaktadır.

- KVKK'nın 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir.
- Kişisel verilerin silinmesinde KVKK'nın 4. maddesinde sayılan aşağıdaki ilkelere tamamen uyulmaktadır:
    a) Hukuk ve dürüstlük kurallarına uygun olma,
    b) Doğru ve gerektiğinde güncel olma,
    c) Belirli, açık ve meşru amaçlar için işlenme,
    d) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
    e) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.
- KVKK'nın 12. maddesi kapsamında düzenlenen teknik ve idari tedbirlere uyulmaktadır.
- Kurul kararlarına uygun hareket edilmektedir.
- Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi ile ilgili yapılan tüm işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süreyle saklanmaktadır.
- Veri sorumlusu, kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı seçmektedir. İlgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçecektir.

4. KAYIT ORTAMLARI

Siz veri sahiplerine ait kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere diğer ilgili mevzuata uygun olarak güvenli bir şekilde saklanmaktadır:

Elektronik ortamlar:
Sunucular (etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.)
Yazılımlar (ofis yazılımları, portal)
Bilgi güvenliği cihazları duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virus vb.
Kişisel bilgisayarlar (masaüstü, dizüstü)
Mobil cihazlar (telefon, tablet, vb.)
Optik diskler (CD, DVD, vb.)
Çıkartılabilir bellekler (USB, Hafıza Kart vb.)

Fiziksel ortamlar:
Arşiv
Kilitli Birim Dolapları
Kilitli Olmayan Birim Dolapları
Şifreli Birim Dolapları
Kilitli Kişisel Dolaplar
Kilitli Olmayan Kişisel Dolaplar
Kilitli Kişisel Çekmeceler
Kilitli Olmayan Kişisel Çekmeceler

5. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirketimiz tarafından; çalışanlar, çalışan adayları, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler KVKK'ya uygun olarak saklanır ve imha edilir.
Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

5.1. Saklamaya İlişkin Açıklamalar

KVKK m. 3'te kişisel verilerin işlenmesi kavramı tanımlanmış, m. 4'te işlenen kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen süre kadar muhafaza edilmesi gerektiği belirtilmiş, m. 5'te ise kişisel verilerin işleme şartları sayılmıştır.

Buna göre, Şirket'imiz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

5.2. Saklamayı Gerektiren Hukuki Sebepler

Şirket'imizde, faaliyetlerimiz kapsamında işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 213 sayılı Vergi Usul Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 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.

5.3. Saklamayı Gerektiren İşleme Amaçları

Şirketimiz, iş faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

Kişisel Veri İşleme Amaçlarımız	**Örnekler**
Potansiyel tedarikçi/iş ortaklarını değerlendirme	Risk kurallarımız gereği inceleme ve çıkar çatışması sürecimizin yürütülmesi
Müşteri ilişkilerinin kurulması ve yönetimi, Tedarikçi/iş ortaklarımızla sözleşme sürecinin yürütülmesi ve sonuçlandırılması	Şirketimizin mal ve hizmetlerin satışı ve servis edilmesi işlemlerinin gerçekleştirilmesi, yönetimsel süreçlerin yürütülmesi (operasyon, hukuk, mali, teknik ve pazarlama süreçleri), teklif sunulması, mal tedariki, faturalandırma, sözleşme kurulması ve ifa edilmesi, sözleşme sonrası hukuki işlem güvenliğinin sağlanması, hizmet geliştirmek, yeni teknoloji ve uygulamaların değerlendirilmesi ile Şirketimizin ticari ve iş stratejilerinin belirlenmesi ve uygulanması, operasyonların yönetilmesi (talep, teklif, değerlendirme, sipariş, bütçelendirme, sözleşme), finans operasyonları, mali işlerin yönetilmesi, ticari ilişki içerisinde olduğu tüzel/gerçek kişilere alternatifler sunabilmek
Doğrudan pazarlama süreçlerinin yürütülmesi	E-posta ve telefon ile hizmetlerimize ilişkin pazarlama bildirimleri yapmak, memnuniyet anketleri yapılması ya da sosyal medya, online platformlar veya başka mecralar üzerinden yaptığınız görüş, şikayet ve yorumların değerlendirilmesi, dönüş yapılması, şirket yenilikleri, kampanyalarla ilgili müşterilerimizi bilgilendirmek, kampanya ve yarışma çalışmalarının yürütülmesi, yapılacak etkinliklerde katılımcılar ile pazarlama aktiviteleri yapılması
İletişim ve destek (talebiniz üzerine)	Hizmetlerimizle ilgili bilgi alma taleplerinin yanıtlanması, iletişim kanallarımız aracılığıyla gelen taleplere ilişkin destek sağlanması, kayıtlarımızın ve veri tabanımızın güncellenmesi
Yasal yükümlülüklere uyum	Vergi ve sigorta süreçlerinin yürütülmesi, 5651 sayılı Kanun ve sair mevzuat, 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ve sair mevzuat, 5237 sayılı Türk Ceza Kanunu ve 6698 sayılı Kişisel Verilerin Korunması Kanunu başta olmak üzere, ilgili mevzuattan kaynaklanan yasal yükümlülüklerimizin yerine getirilmesi, resmi kurumlar nezdindeki süreçlerin yürütülmesi, kayıt tutma ve bilgilendirme yükümlülükleri, uyum ve denetim, resmi mercilerin denetim ve teftişleri, yasal haklarımızın ve davalarımızı takibi ve sonuçlandırılması, resmi mercilerin talebi üzerine veri ifşası gibi tabi olduğumuz kanun ve düzenlemelere uyum kapsamında gerekli süreçlerin yürütülmesi, düzenleyici ve denetleyici kurumlarla, yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde KVKK'da belirtilmiş yasal yükümlülüklerin yerine getirilmesini sağlamak üzere belirlenmiş gereklilik ve zorunluluklar kapsamında,
Şirket menfaatlerinin korunması ve güvenliğinin sağlanması	Şirket çıkarlarının ve menfaatlerinin korunması için gerekli denetim faaliyetlerinin yürütülmesi, çıkar çatışması kontrollerinin yapılması, Şirketimizle iş ilişkisinde olan kişilerin hukuki ve ticari güvenliğinin temini, şirket cihaz ve varlıklarının korunması için CCTV kayıtlarının tutulması, teknik ve idari güvenlik önlemlerinin alınması, sunduğumuz hizmetlerin geliştirilmesi için gerekli çalışmaların yürütülmesi, işyeri kurallarının uygulanması ve denetlenmesi, sosyal sorumluluk aktivitelerinin planlanması ve icrası, Elginkan Topluluğu grup şirketlerinin ticari itibarının ve oluşturduğu güvenin korunması, bina içinde meydana gelen tüm olay, kaza, şikayet, kayıp çalıntı vb.

Kişisel Veri İşleme Amaçlarımız	Örnekler
	durumların raporlanarak gerekli müdahalenin yapılması ve önlem alınması, bakım ve onarım yapılması sırasında oluşabilecek tehlikeli durumlar için uyulması gereken kuralların aktarılması ve taşeronların mesleki yeterliliklerinin ölçülmesi, firma çalışanlarının giriş ve çıkışlarının düzenini sağlamak ve güvenlik açısından gerekli bilgileri edinmek, gerekli kalite ve standart denetimlerimizi yapabilmek ya da kanun ve yönetmelikler ile belirlenmiş raporlama ve sair yükümlülüklerimizin yerine getirilmesi, tedarikçilerin sahaya kabulünün uygunluğunun değerlendirilmesi
Şirket ticari faaliyetlerinin planlanması ve icrası	Şirket'in kısa, orta ve uzun vadede ticari politikalarının tespit edilmesi, planlanması ve uygulanması, ticari ve iş stratejilerinin belirlenmesi ve uygulanması amacı doğrultusunda; Şirketimiz tarafından yürütülen iletişim, pazar araştırması ve sosyal sorumluluk aktiviteleri, satın alma işlemlerinin yürütülmesi,
Raporlama ve denetim	Türkiye'de kurulu Elginkan Topluluğu grup şirketleri ile iletişimin sağlanması, gerekli faaliyetlerin, iç denetim ve raporlama süreçlerinin yürütülmesi
Hak ve menfaatlerin korunması	Şirketimiz aleyhine açılan dava, soruşturma vb. hukuki hak taleplerine karşı savunma

5.4. İmhayı Gerektiren Sebepler

Kişisel Veriler,

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ortadan kalkması,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- KVKK m. 11 gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun KVK Kurumu tarafından kabul edilmesi,
- KVK Kurumu'nun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya KVKK'da öngörülen süre içinde cevap vermemesi hallerinde; KVK Kurulu'na şikâyette bulunması ve bu talebin KVK Kurulu 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, Şirketimiz tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

6. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla KVKK'nın 12. maddesindeki ve KVK Kurumu'nun yayınladığı Kişisel Veri Güvenliği Rehberi'nde yer alan ilkeler çerçevesinde Şirket tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır:

TEKNİK TEDBİRLER

Şirketimiz tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Sızma (Penetrasyon) testleri ile Kurumumuz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- 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.
- Kurum içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Kurum, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Kurum tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- 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.
- Kurum internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- 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. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.

İDARİ TEDBİRLER

Kurum tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri, 657 sayılı Kanun ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Kurum tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce Kurum 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.

7. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ

7.1. Kişisel Verilerin Silinmesi

Şirketimiz ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri silebilir. Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirketimizce, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirler alınır.

Kişisel Verilerin Silinmesi Süreci

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi.
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi.
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi.
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

Kişisel Verilerin Silinmesi Yöntemleri

Veri Kayıt Ortamı	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 tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi 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 tutulankişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir. Buna ilişkin örnekler aşağıda yer almaktadır:

- Hizmet Olarak Uygulama Türü Bulut Çözümleri (Office 365 Salesforce, Dropbox gibi: Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.
- Kâğıt Ortamında Bulunan Kişisel Veriler: Kâğıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.
- Merkezi Sunucuda Yer Alan Ofis Dosyaları: Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının ayni zamanda sistem yöneticisi olmadığına dikkat edilmelidir.
- Taşınabilir Medyada Bulunan Kişisel Veriler: Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.
- Veri Tabanları: Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının ayni zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

7.2. Kişisel Verilerin Yok Edilmesi

Şirketimiz ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri yok edebilir. Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

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.

- 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.

- Yazılımdan Güvenli Olarak Silme: Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.
- Uzman Tarafından Güvenli Olarak Silme: 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.
- Karartma: Kişisel verilerin fiziksel olarak okunamayacak hale getirilmesidir.

Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir:

- Yerel Sistemler: Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir. i) De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir. ii) Fiziksel Yok Etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Kati hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir. iii) Üzerine Yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

- Çevresel Sistemler: Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır: İ) Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. ii) Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. iii) Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir. iv) Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir. v) Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. vi) Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir. vii) Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. viii) Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

- Kağıt ve Mikrofiş Ortamları: Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem

gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir. Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

- Bulut Ortamı: Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir. Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir: i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi, ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı servis gibi üçüncü kurumlara gönderilmesi, iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

7.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder. Şirketimiz, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya alıcı grupları 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. Şirketimiz, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri almaktadır.

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 dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır.

<u>Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri</u>

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.

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır. Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Bu yöntemlerin uygulanması sonucunda elde edilen verilerin belirli bir kişiyi tanımlayamaz olması gerekmektedir.

Örnek alınabilecek anonim hale getirme yöntemleri aşağıdaki açıklanmaktadır:

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri: Değer düzensizliği sağlamayan yöntemlerde kümedeki verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satir veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar.

a. Değişkenleri Çıkartma
Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Böyle bir durumda tablodaki bütün sütun tamamıyla kaldırılacaktır. Bu yöntem, değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin kamuya ifşa edilemeyecek kadar hassas bir veri olması veya analitik amaçlara hizmet etmiyor olması gibi sebeplerle kullanılabilir.

b. Kayıtları Çıkartma
Bu yöntemde ise veri kümesinde yer alan tekillik ihtiva eden bir satirin çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır. Örneğin anket sonuçlarının yer aldığı bir veri kümesinde, herhangi bir sektörden yalnızca tek bir kişi ankete dahil edilmiş olsun. Böyle bir durumda tüm anket sonuçlarından "sektör" değişkenini çıkartmaktansa sadece bu kişiye ait kaydı çıkartmak tercih edilebilir.

c. Bölgesel Gizleme
Bölgesel gizleme yönteminde de amaç veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmaktır. Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görülebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabilecekse istisnai durumu yaratan değer "bilinmiyor" olarak değiştirilir.

ç. Genelleştirme
İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkânsız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir. Örneğin TC Kimlik No 12345678901 olan bir kişi e-ticaret platformundan çocuk bezi aldıktan sonra ayni zamanda ıslak mendil de almış olsun. Yapılacak anonim hale getirme işleminde genelleştirme yöntemi kullanılarak e-ticaret platformundan çocuk bezi alan kişilerin %xx'i ayni zamanda ıslak mendil de satın alıyor şeklinde bir sonuca ulaşılabilir.

d. Alt ve Üst Sınır Kodlama
Alt ve üst sinir kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir.

e. Global Kodlama
Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir. Genelde belli değerlerin öbeklenerek tahmin ve varsayımlar yürütmeyi kolaylaştırdığı hallerde kullanılır. Seçilen değerler için ortak ve yeni bir grup oluşturularak veri kümesindeki tüm kayıtlar bu yeni tanım ile değiştirilir.

f. Örnekleme
Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da

paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur. Örnekleme yapılacak alt kümenin belirlenmesinde basit istatistik metotları kullanılır. Örneğin; İstanbul ilinde yaşayan kadınların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir veri kümesini anonim hale getirerek açıklanması ya da paylaşılması halinde İstanbul'da yaşadığı bilinen bir kadına dair ilgili veri kümesinde taramalar yapmak ve tahmin yürütmek anlamlı olabilir. Ancak ilgili veri kümesinde yalnızca nüfusa kayıtlı olduğu il İstanbul olan kadınların kayıtları bırakılır ve nüfus kaydı diğer illerde olanlar veri kümesinden çıkartılarak anonimleştirme uygulanır ve veri açıklanır ya da paylaşılırsa, veriye erişen kötü niyetli kişi İstanbul'da yaşadığını bildiği bir kadının nüfus kaydının İstanbul'da olup olmadığını tahmin edemeyeceğinden tanıdığı bu kişiye ait bilgilerin elindeki verinin içerisinde yer alıp almadığına dair güvenilir bir tahmin yürütemeyecektir.

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri: Değer düzensizliği sağlayan yöntemlerle yukarıda bahsedilen yöntemlerden farklı olarak; mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır. Bu durumda kayıtların taşıdığı değerler değişmekte olduğundan veri kümesinden elde edilmesi planlanan faydanın doğru hesaplanması gerekmektedir. Veri kümesindeki değerler değişiyor olsa bile toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.

Mikro Birleştirme
Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.

Veri Değiş Tokuşu
Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiflerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir.

Gürültü Ekleme
Bu yöntem ile seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkarmalar yapılır. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır.

Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler
Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya kişisel verilerine dair varsayımların türetilebilmesi ihtimali ortaya çıkabilmektedir.

Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirirken, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

a. K-Anonimlik
Anonim hale getirilmiş veri kümelerinde, dolaylı tanımlayıcıların doğru kombinasyonlarla bir araya gelmesi halinde kayıtlardaki kişilerin kimliklerinin saptanabilir olması veya belirli bir kişiye dair bilgilerin rahatlıkla tahmin edilebilir duruma gelmesi anonim hale getirme süreçlerine dair olan güveni sarsmıştır. Buna istinaden çeşitli istatistiksel yöntemlerle anonim hale getirilmiş veri kümelerinin daha güvenilir duruma getirilmesi gerekmiştir. K-anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilerek oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır

b. L-Çeşitlilik

K-anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan L-çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır.

c. T-Yakınlık

L-çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır. Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denmektedir.

Anonim Hale Getirme Yönteminin Seçilmesi

Şirketimiz, yukarıdaki yöntemlerden hangilerinin uygulanacağına ellerindeki verilere bakarak ve sahip olunan veri kümesine dair aşağıdaki özellikler dikkate alınarak karar vermektedir;

- Verinin niteliği,
- Verinin büyüklüğü,
- Verinin fiziki ortamlarda bulunma yapısı,
- Verinin çeşitliliği,
- Veriden sağlanmak istenen fayda / işleme amacı,
- Verinin işleme sıklığı,
- Verinin aktarılacağı tarafın güvenilirliği,
- Verinin anonim hale getirilmesi için harcanacak çabanın anlamlı olması,
- Verinin anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı,
- Verinin dağıtıklık/merkezilik oranı,
- Kullanıcıların ilgili veriye erişim yetki kontrolü ve
- Anonimliği bozacak bir saldırı kurgulanması ve hayata geçirilmesi için harcayacağı çabanın anlamlı olması ihtimali.

Bir veri anonim hale getirilirken, Şirketimiz kişisel veriyi aktardığı diğer kurum ve kuruluşların bünyesinde olduğu bilinen ya da kamuya açık bilgilerin kullanılması ile söz konusu verinin yeniden bir kişiyi tanımlar nitelikte olup olmadığını, yapacağı sözleşmelerle ve risk analizleriyle kontrol etmektedir.

Anonimlik Güvencesi

Şirketimiz, bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilirken, anonim hale getirilmiş veri kümesinin bin başka veri kümesiyle birleştirilerek anonimliğin bozulamaması, bin ya da birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bin bütün oluşturulmaması, anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi noktalarına dikkate dilemekte olup, Şirketimizce anonim hale getirdikleri veri kümeleri üzerinde bu maddede sıralanan özellikler değiştikçe kontroller yapılmakta ve anonimliğin korunduğundan emin olunmaktadır.

Anonim Hale Getirilmiş Verilerin Tersine İşlem İle Anonimleştirmenin Bozulmasına Dair Riskler

Anonim hale getirme işlemi, kişisel verilere uygulanan ve veri kümesinin ayırt edici ve kimliği belirleyici özelliklerini yok etme işlemi olduğundan bu işlemlerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski bulunmaktadır. Bu durum anonimliğin bozulması olarak ifade edilir. Anonim hale getirme işlemleri yalnızca manuel işlemlerle veya otomatik geliştirilmiş işlemlerle ya da her iki işlem tipinin birleşiminden oluşan melez işlemlerle sağlanabilir. Ancak önemli olan anonim hale getirilmiş verilerin paylaşıldıktan veya ifşa edildikten sonra veriye erişebilen veya sahip olan yeni kullanıcılar tarafından anonimliğin bozulmasını engelleyecek önlemlerin alınmış olmasıdır. Anonimliğin bozulmasına dair bilinçli olarak yürütülen işlemlere "anonimliğin bozulmasına yönelik saldırılar" denilmektedir. Bu kapsamda, Şirketimizce anonim hale getirilmiş kişisel verilerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin

yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski olup olmadığı araştırılarak ona göre işlem tesis edilmektedir.

8. BİRİMLER VE GÖREVLERİ

Şirket'in 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 güvenliği sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel veri saklama ve imha sürecinde yer alan birimlere ve görev tanımlarına işbu Politika'nın EK-1'nde yer alan tablodan ulaşabilirsiniz.

9. SAKLAMA VE İMHA SÜRELERİ

Şirketimiz 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 Politikası'nda yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Bilgi İşlem departmanı/birimi tarafından güncellemeler yapılır. Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme ya da anonim hale getirme işlemi Bilgi İşlem departmanı/birimi tarafından yerine getirilir.

Şirketimiz tarafından KVKK ve diğer ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerinizin Şirketimiz tarafından saklama, imha ve periyodik imha sürelerini gösterir tabloya, işbu Politika'nın Ek-2'sinde yer alan "Saklama ve İmha Süreleri Tablosu"ndan ulaşabilirsiniz.

İşbu Politika'nın Ek-2'sinde yer verilen imha sürelerinin yanında, Şirket 6 aylık periyodlarla saklama süresi dolan kişisel verileri İşbu Politika'da yer verilen usullere uygun olarak imha eder. Buna göre Şirket, her yıl Mart ve Eylül aylarında periyodik imha işlemini gerçekleştirir.

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

10. DİĞER HUSUSLAR

KVKK ve ilgili diğer mevzuat hükümleri ile işbu Politika arasında uyumsuzluk olması halinde, öncelikle KVKK ve ilgili diğer mevzuat hükümleri uygulanacaktır. İşbu Politika'nın basılı nüshası Mali ve İdari İşler departmanı tarafından saklanır.

Şirket tarafından hazırlanan işbu Politika 01.09.2021 tarihinde yürürlüğe girmiştir. Politika'da değişiklik olması durumunda, Politika'nın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir.

Elmor Tesisat Malzemesi Ticaret A.Ş.

EK-1 SAKLAMA VE İMHA SÜRECİNDE YER ALAN BİRİMLER VE GÖREVLERİ TABLOSU

Kişisel verilere ilişkin farkındalığın sürekliliğinin sağlanması için lüzumlu eğitimlerin planlanması ve icrası	İnsan Kaynaklar Departmanı
Kişisel verilerin korunmasına ilişkin personel görev tanımlarının ilgili çalışanlara ve hizmet alınan şirket personeline tebliği ve takibi	İnsan Kaynaklar Departmanı
Kişisel verilerin işlendiği güvenlik kamerası veya ziyaretçi kayıt defteri gibi harici ortamların fiziksel denetimi	Bilgi İşlem Departmanı
Kişisel veri imha dosyasının oluşturulup düzenli bir şekilde imhanın sağlanması ve bu işlemlerin kayıt altına alınması	İnsan Kaynaklar Departmanı
Kişisel veri saklama ortamlarının fiziki ve bilişim sistemi güvenlik araçlarının geliştirilmesi ve güncellenmesi	Bilgi İşlem ve İnsan Kaynakları Departmanları
Kişisel verilerin korunması ve imhası sürecine ilişkin kurulmuş olan sistemin geliştirilmesi için lüzumlu takip, araştırma ve önerilerin ortaya konması	İnsan Kaynaklar Departmanı

EK-2 SAKLAMA VE İMHA SÜRELERİ TABLOSU

SÜREÇ	**SAKLAMA SÜRESİ**	**İMHA SÜRESİ**
İş Başvuruları	- 6 ay - 2 yıl	- İş başvurusu olumsuz değerlendirilen ve işe alımına karar verilmeyen çalışan adaylarının özgeçmiş ve iş başvuru formları ilk periyodik imha döneminde imha edilir. - İş başvuruları olumlu değerlendirilen ancak işe alınmasına karar verilmeyen adayların özgeçmişleri ve iş başvuru formları ileride değerlendirilebileceği düşüncesiyle 2 yıl saklanır ve iki yıllık sürenin ardından ilk periyodik imha döneminde imha edilir.
İşe Alım ve İstihdam	15 yıl	Çalışanın işten ayrıldığı veya iş akdine son verildiği tarihten itibaren veya çalışan ile ilgili görülmekte olan yargı sürecinin sona ermesinden itibaren **15 yılın** ardından ilk periyodik imha döneminde imha edilir.
Çalışan Performans Değerlendirme	3 yıl	Çalışanın performans değerlendirmesinden itibaren veya çalışan ile ilgili görülmekte olan yargı sürecinin sona ermesinden itibaren üç yılın ardından ilk periyodik imha döneminde imha edilir.
Çalışan Sabıka Kayıtları	Derhal	Çalışanın iş ilişkisinin bitiminden itibaren ilk periyodik imha döneminde imha edilir.
Ticari defterler, faturalar ve ilgili kayıtların tutulması	10 yıl	Saklama süresi, ticari defterlere son kaydın yapıldığı, envanterin çıkarıldığı, ara bilançonun düzenlendiği, yılsonu finansal tablolarının hazırlandığı ve konsolide finansal tabloların hazırlandığı, ticari yazışmaların yapıldığı veya muhasebe belgelerinin oluştuğu takvim yılının bitişiyle başlar ve 10 yılın ardından ilk periyodik imha döneminde imha edilir.
Standart Müşteri ve Tedarikçi sözleşmeleri ve evrakları (Sözleşmenin kurulması ve sözleşmede kararlaştırılan hizmetlerin ifası için gereken belgeler)	10 yıl	Sözleşmenin ifasının ve/veya ticari ilişkinin sona ermesinin ardından veya sözleşme konusu hizmet yargı karşısındaki bir uyuşmazlığa konu ise kesinleşmiş yargı kararının ardından **10 yıl** sonra ilk periyodik imha döneminde imha edilir.
Log Kayıt Takip Sistemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde imha edilir.
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde imha edilir.
Ziyaretçi ve Toplantı Katılımcılarının Kaydı	Etkinliğin sonra ermesini takiben 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kamera Kayıtları	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde