

MAZ İNŞAAT TAAHHÜT PET. NAK. TUR. İŞL. SAN. VE TİC. LTD. ŞTİ.
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. GİRİŞ

1.1. AMAÇ

İşbu Kişisel Veri Saklama ve İmha Politikası ("**Politika**"), 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("**Kanun**"), kapsamında hazırlanan ve Resmi Gazetede 28.10.2017 tarihinde yayınlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in ("**Yönetmelik**") 5. ve 6. maddeleri uyarınca **MAZ İNŞAAT TAAHHÜT PET. NAK. TUR. İŞL. SAN. VE TİC. LTD. ŞTİ. ("Şirket")** tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek ve kanun kapsamında fiziki ve elektronik ortamda kayıtları işlenen Kişisel Verilerin saklama ve imha süreçlerini düzenlemek amacıyla hazırlanmıştır.

Kişisel verilerin saklanması ve imhasına işlemler, Şirket tarafından işbu Politika'ya uygun olarak gerçekleştirilir.

1.2. Veri Sorumlusunun Kimliği

UNVAN :
ADRES :
VERGİ DAİRESİ/NO :
TELEFON :
E-POSTA :

1.3. Hukuki Ve Teknik Tanımlar

Şirket	MAZ İNŞAAT TAAHHÜT PET. NAK. TUR. İŞL. SAN. VE TİC. LTD. ŞTİ.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.
Özel Nitelikli Kişisel Veri	İrk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.
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 işlemidir.

Kişisel Veri Sahibi/İlgili Kişi	Kişisel Verisi Şirket tarafından işlenen gerçek kişilerdir.
Veri Kayıt Sistemi	Kişisel Verilerin belirli kısıtlara göre yapılandırılarak işlendiği kayıt istemini ifade eder.
Veri Sorumluları Sicil Bilgi Sistemi	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi
Veri Sorumlusu	Kişisel Verilerin işleme amaçlarını ve yöntemlerini belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.
Veri İşleyen/İlgili Kullanıcı	Veri sorumlusunun verdiği yetkiye dayanarak onun adına Kişisel Veri işleyen veyahut Kişisel Verilere erişim yetkisi bulunan gerçek veya tüzel kişidir.
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.
Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
İmha	Kişisel Verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemlerinin bütünüdür.
Silme	Kişisel Verilerin veri işleyenler için herhangi bir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.
Yok Etme	Kişisel Verilerin herhangi bir kimse tarafından herhangi bir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
Anonim Hale Getirme	Daha önce bir kişiyle ilişkilendirilmiş olan Kişisel Verilerin, başka verilerle eşleştirilerek dahi herhangi bir suretle kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.
Periyodik İmha	Kanunda yer alan Kişisel Verilerin işleme şartlarının tamamının ortadan kalkması durumunda işbu Politikada belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemidir.
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 ortamdır.
Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunudur.
KVK Kurulu	Kişisel Verileri Koruma Kuruludur.

Yönetmelik

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

2. İLKELER SORUMLULUK VE GÖREV DAĞILIMLARI

Şirketin tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasıyla sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Şirket;

- Kanunun 4. maddesinde yer alan ilkeler ile Kanunun 12. maddesi kapsamında alınması gereken ve işbu Politikada belirtilen teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve Kişisel Verilerin İşlenmesi ve Korunması Hakkındaki Politika' ya göre hareket etmekte;

- Kişisel Verilerin imha edilmesiyle ilgili yapılan tüm işlemler kayıt etmekte ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süreyle saklamakta;

- Kurul tarafından aksine bir karar alınmadıkça veyahut Kişisel Veri Sahibinin talebine uygun yöntemin tercih edilmediği hallerde, re'sen Kişisel Verileri imha etme yöntemlerinden uygun olanı seçmekte;

- Kanunun 5. ve 6. maddelerinde yer alan Kişisel Veri işleme şartlarının ortadan kalkması halinde, Kişisel Verileri re'sen veya Kişisel Veri Sahibinin talebi üzerine imha etmekte; bu hususta Kişisel Veri Sahibi tarafından Şirkete başvurulması halinde;

a. İletilen talepleri en geç 30 (otuz) gün içerisinde sonuçlandırmakta ve Kişisel Veri Sahibine bilgi vermekte;

b. Talebe konu Kişisel Verilerin üçüncü kişilere aktarılmış olması durumunda, bu durumu Verilerin aktarıldığı üçüncü kişiye bildirmekte ve üçüncü kişiler nezdinde gerekli işlemlerin yapılmasını temin etmektedir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına aşağıda yer alan tabloda yer verilmiştir.

UNVAN	BİRİM	GÖREV
İnsan Kaynakları Sorumlusu	İnsan kaynakları Departmanı	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi ile çalışanların politikaya uygun hareket etmesinden sorumludur.

3. SAKLAMA VE İMHAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Şirket tarafından; Mevzuatta öngörülen tüm kişilere ilişkin kişisel veriler kanuna uygun olarak saklanır ve imha edilir.

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili

mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, Şirket faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır ve kanunun 7. Maddesinde öngörülen kurallara bağlı şekilde imha edilir.

3.1. Saklamayı Gerektiren İşleme Amaçları

Şirket tarafından Kişisel Veriler;

- Mevzuat ve akdi sorumlulukların yerine getirilmesi, Hukuk İşlerinin Takibi Ve Yürütülmesi
- iştegal alanı kapsamında sunulan ürün ve/veya hizmetleri ilgisine sunabilmesi, ürün ve/veya hizmetlerden Kişisel Veri Sahiplerini faydalandırmak için gerekli çalışmaların Şirketimizin iş birimleri tarafından yerine getirilmesi; pazarlama faaliyetlerini yürütebilmesi; mutabakat, ödeme ve tahsilat işlemlerinin gerçekleştirilebilmesi; bu işlemlerin gerçekleştirilmesi adına Kişisel Veri Sahipleri ile iletişimin sağlanabilmesi, ilgili belge ve bilgilerin gönderilmesi/temini,
- İş Faaliyetlerinin Yürütülmesi/ Denetimi, İş Sağlığı/ Güvenliği Faaliyetlerinin Yürütülmesi İş Süreçlerinin İyileştirilmesine Yönelik Önerilerinin Alınması ve Değerlendirilmesi İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi,
- Finans ve muhasebe ile birlikte tüm mali süreçlerin yürütülmesi,
- Gerekli evrakların düzenlenmesi evrakın (sözleşme, fatura, irsaliye, çek, imza sirküleri, vekâletname vb.) düzenlenmesi,
- Şirket faaliyeti kapsamındaki Müşteri, tedarikçi, taşeron İş ortakları ve ticari ilişki içindeki tüm kişilerle (kamu-özel) gerçekleştirilecek iş ve işlemlerin sağlanması, Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
- İhale, Ruhsat, izin vb. tüm kamusal süreçlere ilişkin iş ve işlemlerin gerçekleştirilmesi
- yürütülen iletişime yönelik idari ve hukuki işlemlerin sağlanması, denetimi,
- Kişisel Veri Sahiplerinin kayıtlarına gerekli olması halinde tekrar ulaşılmaması;
- Şirket faaliyetlerine ilişkin tüm süreçlerin posta, e- posta, SMS ve telefon yoluyla paylaşılması,
- Veri Güvenliğine ilişkin tüm süreçlerin yönetilmesi
- Mal ve Hizmet Satışına ilişkin Alım, Satım ve Destek Hizmetlerinin Yürütülmesi
- iletişim, pazar araştırması ve sosyal sorumluluk aktivitelerinin ve finans operasyonları ile ürün/proje/imalat/yatırım/kalite süreçlerinin yürütülmesi ve yönetilmesi,
- Müşteri ilişkileri ve memnuniyeti süreçlerine ilişkin tüm işlemlerin gerçekleştirilmesi
- talep ve şikâyetlerini ileten Kişisel Veri Sahipleri ile iletişime geçilmesi ve talep ve şikâyet takip ve yönetiminin sağlanması,
- Şirket faaliyetleri kapsamında gerçekleşen seyahat, toplantı, konaklama vb. süreçlere ilişkin işlemlerin gerçekleştirilmesi
- Erişim yetkilerinin belirlenmesi ve Fiziksel Mekan Güvenliğinin Sağlanması
- Şirkete ait işyerlerine giriş yapan ziyaretçilerin/personelin tespiti, ziyaretçi/personel kayıtlarının oluşturulması ve takibi,
- Şirkete insan kaynakları politikalarının yürütülmesi, iş sağlığı ve güvenliği çerçevesinde

yükümlülüklerinin yerine getirilmesi ve gerekli tedbirlerin alınması, Denetim / Etik Faaliyetlerinin Yürütülmesi

- Çalışan Adayı/ Stajyer/ Öğrenci Seçme ve Yerleştirme Süreçlerinin Yürütülmesi, Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi, Çalışan Memnuniyeti ve Bağlılığı Süreçlerinin Yürütülmesi, Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi, talep halinde idari ve yargı mercilerine sunulması;
- Acil Durum Süreçlerinin yürütülmesi, Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
- Şirket insan kaynakları süreçlerinin yürütülmesi;
- Şirket içi veya dışı eğitim faaliyetlerinin gerçekleştirilmesi;
- Lojistik faaliyetlerin Gerçekleştirilmesi

amaçlarıyla, fiziki veyahut elektronik ortamlarda güvenli bir biçimde Kanun ve ilgili mevzuatta belirtilen sınırlar çerçevesinde işlenmekte ve saklanmaktadır.

3.2. Saklamayı Gerektiren Hukuki Sebepler

- Sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması;
- Bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması;
- Kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketin meşru menfaatleri için saklanmasının zorunlu olması;
- Şirket tarafından yerine getirilmesi gereken hukuki yükümlülüklerin ifası;
- Mevzuatta Kişisel Verilerin saklanması gerekliliğinin açıkça öngörülmesi;
- Kişisel Veri Sahiplerinin açık rızasının bulunmasıdır.

Şirket, Kişisel Veri işleme şartlarının güncelliğinden sorumludur. Veri sorumlusunun verdiği yetkiye dayanarak veri işleyenler, veri işleme şartlarının ortadan kalktığı durumlarda veri işlemeye devam etmezler.

3.3. İmhayı Gerektiren Sebepler

Mevzuat uyarınca, aşağıda sayılan hallerde Kişisel Veri Sahiplerine ait Kişisel Veriler, Şirket tarafından re'sen veyahut talep üzerine imha edilir:

- Kişisel Verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya yürürlükten kaldırılması;
- Şirketin taraf olduğu ve bu doğrultuda Kişisel Verileri işlediği bir sözleşmenin hiç kurulmamış olması, geçersiz olması, kendiliğinden sona ermesi, feshi veya sözleşmeden dönülmesi;
- Kişisel Verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması;
- Kişisel Verilerin işlenmesini veya saklanmasını gerektiren amacın/amaçların ortadan kalkması;
- Kanunun 5. ve 6. maddelerindeki Kişisel Verilerin işlenmesini gerektiren şartların ortadan kalkması;
- Kişisel Verileri işlemenin sadece açık rıza şartına bağlandığı hallerde, Kişisel Veri Sahibinin açık rızasını geri alması;
- Kişisel Veri Sahibinin, Kanunun 11. maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde Kişisel Verilerinin imha edilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi;
- Veri sorumlusunun, Kişisel Veri Sahibi tarafından Kişisel Verilerinin imha edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde

cevap vermemesi hallerinde; Kurul'a şikâyetinde bulunulması ve Kişisel Veri Sahibinin şikâyetinin Kurul tarafından uygun bulunması;

- Kişisel Verilerin saklanması gerektiren azami sürenin geçmiş olmasına rağmen, Kişisel Verileri daha uzun süre saklamayı haklı kılabilecek bir şartın mevcut olmaması.

4. KİŞİSEL VERİLERİN SAKLAMA VE İMHA SÜRELERİ

Şirket, Kanun ve ilgili mevzuat hükümlerine uygun olarak elde edilen Kişisel Verileri saklama ve imha sürelerinin tespitinde aşağıda sırasıyla sayılan kıstaslar dâhilinde hareket etmektedir:

- Mevzuatta ilgili Kişisel Verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir.

- Kişisel Verinin saklanmasına ilişkin olarak mevzuatta öngörülen sürenin sona ermesi veya ilgili mevzuatta söz konusu Kişisel Verinin saklanmasına ilişkin olarak herhangi bir süre öngörülmemiş olması durumunda sırasıyla;

a. Kanunun 6. maddesinde yer alan tanımlar doğrultusunda; Kişisel Veriler, Kişisel Veriler ve Özel Nitelikli Kişisel Veriler olarak sınıflandırmaya tabi tutulur. Özel nitelikte olduğu tespit edilen tüm Kişisel Veriler imha edilir.

b. Kişisel Verinin saklanmasının Kanunun 4. maddesinde belirtilen ilkelere uygunluğu değerlendirilir; Kişisel Verinin saklanmasının Kanunun 4. maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilir ise, ilgili Kişisel Veriler imha edilir.

c. Kişisel Verinin saklanmasının Kanunun 5. ve 6. maddelerinde öngörülmüş olan istisnalardan hangisi/hangileri kapsamında değerlendirilebileceği tespit edilir. Tespit edilen istisnalar çerçevesinde Kişisel Verilerin saklanması gereken makul süreler tespit edilir. Söz konusu sürelerin sona ermesi akabinde Kişisel Veriler imha edilir.

Şirket tarafından saklama süresi sona eren Kişisel Veriler, imha süreleri kapsamında, 6 (altı)'şar aylık periyodlarla işbu Politikada yer verilen yöntemlere uygun olarak imha edilir. Kişisel Verilerin imha edilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç (3) yıl süreyle saklanır.

İlgili kişi, Kanunun 13 üncü maddesine istinaden şirkete başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

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

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

c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanunun 13 üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

4.1. Süreç Bazında Saklama ve İmha Süreleri Tablosu

VERİ	SAKLAMA SÜRESİ	İMHA SÜRESİ
------	----------------	-------------

Kimlik Verileri	Hukuki İlişki sonrası 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İletişim Verileri	Hukuki İlişki sonrası 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Lokasyon Verileri	Hukuki İlişki sonrası 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Fiziksel Mekan güvenliği Verileri	Hukuki İlişki sonrası 15 yıl Üçüncü Kişiler için 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Özlük Verileri	Hukuki İlişki sonrası 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuki İşlem Verileri	Hukuki İlişki sonrası 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşlem Güvenliği Verileri	Hukuki İlişki sonrası 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Finansal Veriler	Hukuki İlişki sonrası 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mesleki Deneyim Verileri	Hukuki İlişki sonrası 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Görsel ve İşitsel Kayıt verileri	Hukuki İlişki sonrası 15 yıl Üçüncü Kişiler için 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sendika Üyeliği Verileri	Hukuki ilişki Sonrası 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sağlık Bilgisi Verileri	Hukuki İlişki sonrası 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Biyometrik Veriler	Hukuki ilişki sonrası 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ceza Mahkumiyeti ve Güvenlik Tedbirleri Verileri	Hukuki ilişki sonrası 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

5. KİŞİSEL VERİLERİN SAKLAMA VE İMHA YÖNTEMLERİ

5.1.Kayıt Ortamları

Şirket kişisel verileri, aşağıdaki tabloda listelenen ortamlarda mevzuat ve uluslararası veri güvenliği prensipleri çerçevesinde hukuka uygun ve güvenli bir şekilde saklar. Şirketimiz, tabloda yer alan ortamlara eklenecek veya değiştirilecek hususları Politikaya dahil etmeyi ve duyurmayı taahhüt eder.

Elektronik ortamlar:
- Bilgisayarlar/sunucular,
- Ağ cihazları,
- Ağ üzerindeki Veri disk sürücülerini,
- Bulut sistemleri,
- Yazıcı, Tarayıcı, Parmak izi okuyucu vb. birimler,
-Yüz Tarama ve Tanıma Sistemleri
- Çıkarılabilir bellekler (USB, Hafıza Kart, optik diskler vb.)
- Mobil Cihazlar (Telefon, tablet vb.)
- BM – Bordro,
Fiziksel ortamlar:
- Kâğıt,
- Manuel Veri Kayıt Sistemleri (anket formları, ziyaretçi giriş defterleri vb.)
- Birim Dolapları,
- Arşiv.
- Yazılı Basılı, Görsel Ortamlar

5.2. Teknik Ve İdari Tedbirler

6698 Sayılı kişisel Verilerin Korunması Kanunu kapsamında şirket tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda belirtilmektedir :

a. İdari Tedbirler:

Kişisel Verilere Yönelik;

- Çalışanların Niteliği Ve Teknik Bilgi/ Becerisinin Geliştirilmesi faaliyetleri yürütülmekte, Eğitim ve Farkındalık faaliyetleri gerçekleştirilmekte,
- Kurum İçi Periyodik ve/veya Rastgele Denetimler gerçekleştirilmekte,
- Kişisel Veri İşleme Envanteri Hazırlanmakta,
- Kişisel Verilerin Hukuka Aykırı İşlenmesinin Kişisel Verilere Hukuka Aykırı Erişilmesinin Önlenmesi için gerekli tedbirler alınmakta,
- Kişisel Verilerin Muhafazasının Sağlanması, İletişim Teknikleri Ve İlgili Mevzuatlar Hakkında Eğitimler Verilmekte,
- Sözleşmeler (Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen Arasında) yapılmakta,
- Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.) sağlanmakta
- Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)

- Çalışanlara Gizlilik Sözleşmeleri/ taahhütnameleri imzalatılmakta,
- Güvenlik Politika Ve Prosedürlerine Uymayan Çalışanlara Yönelik Uygulanacak Disiplin Prosedürü Uygulanmakta,
- İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi)
- İlgili Kişileri Aydınlatma Yükümlülüğü Yerine Getirilmekte,
- Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim güncel şekilde yapılmakta,
- Şirket İçi Periyodik Ve Rastgele Denetimler Yapılmakta Ve Çalışanlara Yönelik Bilgi Güvenliği Eğitimleri Verilmektedir.
- Risk Analizleri yapılmakta,

Özel Nitelikli Kişisel Verilere Yönelik;

Kişisel Veriler İçin Alınan İdari Tedbirlerin Yanı Sıra Çalışanlara,

- Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,
- Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamalarının ve sürelerinin net olarak tanımlanması,
- Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması sağlanmaktadır.
- Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
- Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,

b. Teknik Tedbirler:

Kişisel Verilere Yönelik;

- Şirketin Bilişim Sistemleri Teçhizatı, Yazılım Ve Verilerin Fiziksel Güvenliği İçin Gerekli Önlemler Alınmakta,
- Hukuka Aykırı İşlemeyi Önlemeye Yönelik Riskler Belirlenmekte, Bu Risklere Uygun Teknik Tedbirler Alınmakta,
- Erişim Yetki Ve Rol Dağılımları İçin Prosedürler Oluşturulmakta Ve Uygulanmakta,
- Yetki Matrisi Uygulanmakta, Erişimler Kayıt Altına Alınarak Uygunsuz Erişimler Kontrol Altında Tutulmakta,
- Saklama Ve İmha Politikasına Uygun İmha Süreçleri Tanımlanmakta Ve Uygulanmakta,
- Hukuka Aykırı İşleme Tespiti Halinde İlgili Kişiye Ve Kurula Bildirmek İçin Bir Sistem Ve Altyapı Oluşturulmakta,
- Güvenlik Açıkları Takip Edilerek Uygun Güvenlik Yamaları Yüklenmekte, Şifreleme ve Sızma Testi uygulanmakta, Saldırı Tespit ve Önleme Sistemleri kullanılmakta Veri Kaybı Önleme Yazılımları Yedekleme periyodik olarak yapılmakta

- Güvenlik Duvarları ve Güncel Anti-Virüs Sistemleri kullanılmakta
- Silme, Yok Etme veya Anonim Hale Getirme işlemleri periyodik olarak yapılmakta Bilgi Sistemleri Güncel Halde Tutulmakta,
- Kişisel Verilerin İşlendiği Elektronik Ortamlarda Güçlü Parolalar Kullanılmakta Ve Güvenli Kayıt Tutma (Loglama) Sistemleri Kullanılmakta, Kişisel Verilerin Güvenli Olarak Saklanmasını Sağlayan Yedekleme Programları Kullanılmaktadır.

Özel Nitelikli Kişisel Verilere Yönelik;

Kişisel Veriler İçin Alınan Teknik Tedbirlerin Yanı Sıra;

- Özel Nitelikli Kişisel Verilerin Güvenliğine Yönelik Politika Ve Prosedürler Belirlenmekte,
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise;
- Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
- Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
- Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
- Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,
- Özel nitelikli kişisel veriler aktarılacaksa;
- Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,
- Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrenmesi ve kriptografik anahtarın farklı ortamda tutulması,
- Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,
- Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi sağlanmaktadır.

5.3. Kişisel Verilerin İmhası, Yöntem ve Usulleri

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

5.3.1. Kişisel Verilerin Silinmesi

Kâğıt ortamında bulunan Kişisel Veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki Kişisel Verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemez ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak veri işleyenlere görünmez hale getirilmesi şeklinde yapılır.

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz hale getirilir.

Verilerin Silinmesi işlemi gerçekleştirilirken aşağıdaki yöntemler kullanılır;

- Bulut sisteminde yer alan Kişisel Veriler silme komutu verilerek silinir; anılan işlem gerçekleştirilirken veri işleyen bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmaması sağlanır;
- Merkezi sunucuda bulunan dosyanın işletim sistemindeki silme komutu ile ilgili Kişisel Veri silinir veya dosya veya dosya ya da dosyanın bulunduğu dizin üzerinde veri işleyen ve/veya ilgili kullanıcının erişim hakları kaldırılır; anılan işlem gerçekleştirilirken veri işleyen ve/veya ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilir;
- Taşınabilir medyada yani flash ortamda bulunan Kişisel Veriler bu ortama uygun yazılımlar kullanılarak silinir;
- Veri tabanlarında ilgili satırlar veri tabanı komutları ile (DELETE vb.) silinir; anılan işlem gerçekleştirilirken veri işleyen ve/veya ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilir.

b. Teknik Gereklilik Halinde Uzman Desteği

Verilerin silinmesi işlemi sistemde yer alan diğer verilerin korunması veya başkaca bir teknik zorunluluk bulunması halinde şirketimizce anlaşılacak Kişisel Veriler için uzmanı tarafından veri işleyenler için herhangi bir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde güvenli olarak silinir.

5.3.2. Kişisel Verilerin Yok Edilmesi

Verilerin yok edilmesi işlemlerinde Kişisel Verilerin bulunduğu tüm kopyaları tespit eder ve Kişisel Verilerin bulunduğu sistemlerin türüne göre aşağıda yer alan yöntemlerden bir veya birkaçını uygulayarak yok etme işlemi gerçekleştirir.

a. Yerel Sistemlerde Yer Alan Kişisel Verilerin İmhası

i) Fiziksel Yok Etme:

Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel yöntemlerle Kişisel Verileri yok eder. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle Kişisel Verilerin erişilmez kılınması sağlanır.

ii) Üzerine Yazma:

Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski Kişisel Verinin kurtarılmasının önüne geçerek ve bu işleme özel yazılımlar kullanarak Kişisel Verileri yok edilir.

b. Çevresel Sistemlerde Yer Alan Kişisel Verilerin İmhası

i) Ağ cihazları (switch, router, firewall vb.):

Ağ cihazlarının içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Şirket Yerel Sistemlerde yer alan Kişisel Verilerin imha edilmesine yönelik usullerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanarak Kişisel Verileri yok edilir.

ii) Flash tabanlı ortamlar:

Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanlarını, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da Yerel Sistemlerde yer alan Kişisel Verilerin imha usullerinde belirtilen uygun yöntemlerin bir ya da birkaçı kullanmak suretiyle Kişisel Verileri yok edilir.

iii) Mobil telefonlar (Sim kart ve sabit hafıza alanları):

Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. Şirket Yerel Sistemlerde yer alan Kişisel Verilerin imha usullerinde belirtilen uygun yöntemlerin bir ya da birkaçı kullanmak suretiyle Kişisel Verileri yok edilir.

iv) Optik diskler:

CD, DVD gibi veri saklama ortamlarıdır. Şirketimiz yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle Kişisel Verileri yok edilir.

v) Veri kayıt ortamı çıkartılabilir veya sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:

Tüm veri kayıt ortamlarının söküldüğünü doğrulayarak, özelliğine göre Yerel Sistemlerde yer alan Kişisel Verilerin imha usullerinde belirtilen uygun yöntemlerin bir ya da birkaçı kullanmak suretiyle Kişisel Verileri yok edilir.

c. Kâğıt ve Mikrofiş Ortamlarında Bulunan Kişisel Verilerin İmhası:

Kâğıt ve Mikrofiş Ortamlarında bulunan Kişisel Veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan Şirket tarafından ana ortam yok edilir. Bu işlem gerçekleştirilirken ortam kâğıt imha veya kırma makineleri ile anlaşılabilir boyutta, geri birleştirilemeyecek şekilde küçük parçalara bölünür. Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan Kişisel Veriler ise buldukları elektronik ortama göre Yerel Sistemlerde yer alan Kişisel Verilerin imha usullerinde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

d. Bulut Ortamda Bulunan Kişisel Verilerin İmhası:

Bulut Ortamda yer alan Kişisel Verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenir ve Kişisel Veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılır. Bulut bilişim hizmet ilişkisi sona erdiğinde; Kişisel Verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir.

Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan Kişisel Verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

i) İlgili cihazlar, üzerlerinde yapılacak bakım, onarım vb. işlemler için, üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içlerinde yer alan Kişisel Veriler Yerel Sistemlerde yer alan Kişisel Verilerin imha usullerinde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir;

ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamı sökülerek saklanır, arızalı diğer parçalar üretici, satıcı, servis gibi üçüncü kurumlara gönderilir,

iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, Kişisel Verileri kopyalayarak kurum dışına çıkartmasını engellemek için gerekli önlemler alınır.

5.3.3. Kişisel Verilerin Anonim Hale Getirilmesi:

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, Kişisel Veri Sahibinin 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 Veri Sahibi gerçek kişiyi tespit eden bilgiyken, bu işlemden sonra Veri Sahibi ile ilişkilendirilemeyecek hale gelmiş ve Veri Sahibi ile bağlantısı kopartılmıştır.

Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağı kopartılmasıdır. Kişisel Verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleyme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir.

Anonim Hale Getirme Yöntemleri aşağıda sıralanmıştır:

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

• Değişkenleri Çıkartma • Kayıtları Çıkartma • Bölgesel Gizleme • Genelleştirme • Alt ve Üst Sınır Kodlama • Global Kodlama • Örneklem

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

• Mikro Birleştirme • Veri Değiş Tokuşu • Gürültü Ekleme

Anonim Hale Getirmeyi Kuvvetlendirici İstatistiksel Yöntemler

• K-Anonimlik • L-Çeşitlilik • T-Yakınlık

6. DİĞER HUSUSLAR

Mevzuat hükümleri ile işbu Politika arasında uyumsuzluk olması halinde, öncelikle Kanun ve ilgili diğer mevzuat hükümleri uygulanacaktır.

İşbu Politika' da değişiklik olması durumunda, politikada mevzuata uygun değişiklikler işlenecek ve sistem kayıtları ile duyuruları sağlanacaktır.

MAZ İNŞAAT TAAHHÜT PET. NAK. TUR. İŞL. SAN. VE TİC. LTD. ŞTİ.