Makstone İşitme Ürünleri Perakende Satış Pazarlama A.Ş
Kişisel Veri Saklama ve İmha Politikası

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI
I. VERİ SAKLAMA VE İMHA TAAHHÜDÜ

1. İşbu Kişisel Veri Saklama ve İmha Politikası ("Politika"), Makstone İşitme Ürünleri Perakende Satış Pazarlama A.Ş ("Şirket" veya "MAKSTONE") nezdinde, 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun 7. Maddesi uyarınca oluşturulan ilgili Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik doğrultusunda Şirket içerisinde ve/veya Şirket tarafından uyulması gereken esasları belirleyecektir.

2. Şirket, bünyesinde bulundurduğu, tamamen veya kısmen otomatik olan ya da herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesi sırasında işbu Politika'ya ve Politika'ya bağlı olarak uygulanacak araç, program ve süreçlere uygunluk sağlayacağını taahhüt eder.

3. Şirket işbu politika ile kişisel veri bulunan aşağıda belirtilen kayıt ortamlarındaki ve belirtilen ortamlara ek ortaya çıkabilecek tüm ortamlardaki kişisel verileri kapsamayı kabul eder.

a) Şirket adına kullanılan bilgisayarlar/sunucular,
b) Ağ cihazları,
c) Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri,
d) Bulut sistemleri,
e) Mobil telefonlar ve içerisindeki tüm saklama alanları,
f) Kâğıt,
g) Mikrofiş,
h) Yazıcı, Parmak izi okuyucu gibi çevre birimler,
i) Manyetik bantlar,

j) Optik diskler,
k) Flash hafızalar.

II. POLİTİKA'NIN KAPSAMI

1.İşbu Politika; Şirket'in kişisel verileri işlediği herhangi bir sürece dâhil olan tüm departmanlarını, çalışanlarını ve 3.partileri kapsamaktadır.

2.İşbu Politika; Şirket'in kişisel veriler üzerinde uygulayacağı tüm imha faaliyetlerini kapsayacak olup, her türlü imha gereksinimi sonucunda uygulanacaktır.

3.İşbu Politika kişisel veri olmayan veriler hakkında uygulanmayacaktır.

4.Konuyla alakalı yeni mevzuatlar ile belirlenmesi veya ilgili mevzuatın güncellenmesi durumunda, Şirket politikasını ilgili mevzuatlara uyumlu olacak şekilde güncelleyerek mevzuat gerekliliklerine uyacaktır.

5.İşbu Politika'nın Şirket tarafından uygulanmasında hukuki bir engel olduğuna kanaat getirildiği durumlarda, Şirket uygulayacağı adımları, gerek görülmesi durumunda Kurul'a da danışarak, yeniden belirleyecektir.

Tanımlar:

İşbu Politika'da ve ilgili yönetmelikte geçen tanımlar şu şekilde açıklanmaktadır;

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 personeli.

EBYS: Elektronik Belge Yönetim Sistemi

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.

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, 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

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.

Politika: Kişisel Verileri Saklama ve İmha Politikası

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

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.

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

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

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 ortama verilen addır.

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi

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

Periyodik imha: Kanunda 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 işlemidir.

Sicil: Başkanlık tarafından tutulan veri sorumluları sicilidir.
Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

Doğrudan tanımlayıcılar: Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılardır.

Dolaylı tanımlayıcılar: Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılardır.

İlgili kişi: Kişisel verisi işlenen gerçek kişidir.

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 gerçek veya tüzel kişilerdir.

Kişisel Verilerin Korunması Politikası içerisinde bulunan tanımlar işbu Politika için de geçerlidir.

III. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; çalışanlar, çalışan adayları, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

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

1.Saklamaya İlişkin Açıklamalar

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.

a) Saklamayı Gerektiren Hukuki Sebepler

Şirket'de, 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,
- 4734 sayılı Kamu İhale Kanunu,
- 657 sayılı Devlet Memurları Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 5018 sayılı Kamu Mali Yönetimi Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 2547 sayılı Yükseköğretim Kanunu,
- 5434 sayılı Emekli Sağlığı Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu,
- 6446 sayılı Güncel Elektrik Piyasası Kanunu,
- EPDK Yönetmelikleri,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,

- Arşiv Hizmetleri Hakkında Yönetmelik
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

b) Saklamayı Gerektiren İşleme Amaçları

Şirket, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar:

- İnsan kaynakları süreçlerini yürütmek.
- Kurumsal iletişimi sağlamak.
- Kurum güvenliğini sağlamak.
- İstatistiksel çalışmalar yapabilmek.
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- Kurum ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- Yasal raporlamalar yapmak.
- Çağrı merkezi süreçlerini yönetmek.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

2.Kişisel Veri İşleme Şartlarını Ortadan Kaldıran Haller

Kişisel verilerin işlenmesi ile ilgili hüküm ve esaslar Şirket'in Kişisel Veri Politikası içerisinde belirtilmiş olup, tüm Şirket çalışanları bu politikadaki hallerden sorumludur. İşbu Veri Saklama ve İmha Politikası içerisinde Veri Saklama ve İmha dışında kalan "İşleme" konusu ilgili Kişisel Veri Politikası'nın bir özeti şeklindedir.

Aşağıda belirtilen kapsamda bir ihlal olması durumunda Potansiyel Güvenlik İhlali Protokolü içerisindeki ihlal durumu kabul edilerek Şirket tarafından aksiyon alınacaktır:

a. Kanun'a Aykırılık

Şirket, kişisel verileri Kanun'da belirtildiği şekle aykırı olarak işlemediğini taahhüt eder.

Yani Şirket Kanun'un 5 ve 6. maddelerindeki kişisel verilerin işlenmesi şartlarındaki istisnalar mevcut olmadığı sürece;

i. Kanun'da belirtilen istisnalar dışında açık rızasını almadığı kişilerin kişisel verilerini saklamaz.
ii. Şirket, özel nitelikli kişisel verileri sakladığı durumlarda, verileri ilgili Kanun'a bağlı kalarak Şirket KVKK Sorumlusu ve İnsan Kaynakları Departmanı'nın bilgisi dâhilinde işler.

b. Veri İşlenme Şartlarının Ortadan Kalkması

Şirket, veri işlenme şartlarının güncelliğinden sorumludur ve bu sorumluluğunu tüm çalışanları ile paylaşır.

Çalışanlar, veri işlenme şartlarının ortadan kalktığı durumlarda veri işlemeye devam edemez. Şirket Bilgi Teknolojileri Birimi, şartların ortadan kalktığı ortamları işbu Politika'ya uygun bir şekilde ortadan kaldırmakla yükümlüdür.

Şirket aşağıda listelenen ve Yönetmelik içinde de belirtilen durumlarda veri işlenme şartlarının ortadan kalktığını kabul eder (İlgili maddeler Yönetmelik'ten alınmıştır):

i. Kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
ii. Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,
iii. Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,
iv. Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması
v. Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
vi. İlgili kişinin, Kanunun 11 inci maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,

vii. Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,

viii. Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

IV. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ

Kişisel verilerin imhası, verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi şeklinde üç farklı şekilde sağlanabilir. İmha işlemindeki amaç, kalan veriler ile gerçek kişiye ulaşabilmenin mümkün olmamasıdır.
İşbu Politika'nın, IV bölümünde kişisel verilerin silinmesi, yok edilmesi ve anonimleştirilmesi yöntemleri sıralanacak olup, V bölümünde imha ile ilgili bilgilendirme yer alacaktır.

1.Kişisel Verilerin Silinmesi

1.1. Kişisel Verilerin Silinme Süreci

Silme işlemi, Şirket'in verileri tamamen veya otomatik yollarla işlediği durumlarda yapılacaktır ve Şirket, kişisel verileri sildiği durumlarda, verileri hiçbir şekilde erişilemez veya tekrar kullanılamaz hale getirmelidir. Şirket, bu işlemi yaparken verilerin hiçbir kullanıcı tarafından erişilemez veya tekrar kullanılamaz olduğunu garanti etmelidir. Bu garanti, veri sorumlusunun sorumluluğu altındadır.

Silme sırasında, silinmemesi gereken kişisel veriler de yapılan silmeden etkileniyorsa ve erişilemeyecek ve/veya kullanılamayacak hale geliyorsa Şirket'in, KVKK Sorumlusu ve Şirket Avukatı ve İnsan Kaynakları Departmanı ile birlikte karar alarak uygulayabileceği aşağıdaki yöntemlerin bir arada sağlanması da silme olarak değerlendirilecektir

a) 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 verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
b) Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
c) 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.
d) Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

Belirtilen silme yöntemleri, Yönetmelik'e bağlı olup, ilgili durumlarda güncellenmesi Veri Sorumlusu'nun sorumluluğundadır.

1.2. Kişisel Verilerin Silinme Yöntemleri

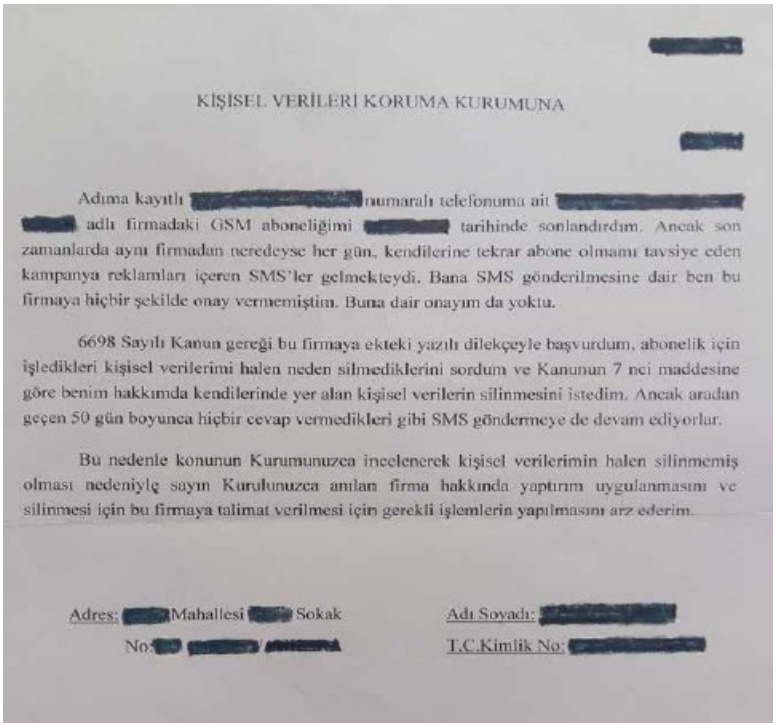
Kişisel veriler kayıtlı oldukları ortamlara uygun yöntemlerle silinmelidir.

1.2.1. Bulut Sisteminde Yer Alan Kişisel Veriler

Office 365, Oracle Forms, Logo ve Logo Bordro Plus gibi sistemlerde yer alan veriler silinirken kullanıcıların verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

1.2.2. Basılı Dokümanlarda Yer Alan Kişisel Veriler

Basılı dokümanlarda bulunan kişisel veriler karartma yöntemi ile 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 görünmez hale getirilmesi şeklinde yapılır.



KİŞİSEL VERİLERİ KORUMA KURUMUNA

Adıma kayıtlı [redacted] numaralı telefonuma ait [redacted] adlı firmadaki GSM aboneliğimi [redacted] tarihinde sonlandırdım. Ancak son zamanlarda aynı firmadan neredeyse her gün, kendilerine tekrar abone olmamı tavsiye eden kampanya reklamları içeren SMS'ler gelmekteydi. Bana SMS gönderilmesine dair ben bu firmaya hiçbir şekilde onay vermemiştim. Buna dair onayım da yoktu.

6698 Sayılı Kanun gereği bu firmaya ekteki yazılı dilekçeyle başvurdum, abonelik için işledikleri kişisel verilerimi halen neden silmediklerini sordum ve Kanunun 7 nci maddesine göre benim hakkımda kendilerinde yer alan kişisel verilerin silinmesini istedim. Ancak aradan geçen 50 gün boyunca hiçbir cevap vermedikleri gibi SMS göndermeye de devam ediyorlar.

Bu nedenle konunun Kurumunuzca incelenerek kişisel verilerimin halen silinmemiş olması nedeniyle sayın Kurulunuzca anılan firma hakkında yaptırım uygulanmasını ve silinmesi için bu firmaya talimat verilmesi için gerekli işlemlerin yapılmasını arz ederim.

Adres: [redacted] Mahallesi [redacted] Sokak
No: [redacted]

Adı Soyadı: [redacted]
T.C.Kimlik No: [redacted]

Kişisel Verilen Karartılması Örneği

1.2.3. Merkezi Sunucuda Yer Alan Ofis Dosyaları

Oracle Forms, Logo ve Logo Bordro Plus gibi sistemlerdeki dosyaların işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir.

1.2.4. Taşınabilir Disk Üzerinde Bulunan Kişisel Veriler

Taşınabilir (harici) disk üzerinde bulunan kişisel veriler, şifreli olarak saklanmalı ve disk özelliğine uygun yazılımlar kullanılarak silinmelidir.

1.2.5. Veri Tabanları Üzerinde Bulunan Kişisel Veriler

Oracle Forms, Logo ve Logo Bordro Plus gibi sistemlerdeki kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir.

2.Kişisel Verilerin Yok Edilmesi

Yok etme işlemi, Şirket'in verileri fiziksel kayıt ortamlarında işlediği durumlarda yapılacaktır ve Şirket bu verileri tekrar geri getirilmesi ve tekrar kullanılması mümkün olmayacak hale getirmekle yükümlüdür. Bu işlemler sırasında Şirket çalışanları ve ilgili departmanlar Veri Sorumlusu'na yok edilecek ilgili departmanları bildirmekle yükümlüdür, sonrasında ise Veri Sorumlusu gerekli her türlü teknik ve idari tedbiri alacaktır.

2.1. Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespiti ve verilerin tutulduğu sistemlere göre aşağıdaki yöntemlerden bir veya birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir.

2.1.1. Yerel Sistemler Üzerindeki Kişisel Veriler

2.1.1.1. De-manyetize Etme

Manyetik medyanın özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

2.1.1.2. Fiziksel Yok Etme

Optik medya ve manyetik medyanın eritilmesi, yakılması, toz haline getirilmesi veya metal öğütücüden geçirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Katı hal diskler (SSD) gibi de-manyetize edilemeyen cihazlar için fiziksel yok etme işlemleri uygulanmalıdır.

2.1.1.3. Üzerine Yazma

Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kere 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir.

2.1.2. Çevresel Sistemler Üzerindeki Kişisel Veriler

2.1.2.1. Ağ cihazları (switch, router vb.)

Söz konusu cihazların silme komutları vardır ama yok etme özelliği bulunmamaktadır. (2.1.1)'de belirtilen uygun yöntemlerin bir ya da birkaçı kullanılarak yok edilmesi gerekir.

2.1.2.2. Flash tabanlı diskler

Flash tabanlı sabit disklerin ATA (SATA, PATA, vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanarak, desteklenmiyorsa üreticinin önerdiği yöntem ya da (2.1.1)'de belirtilen uygun yöntemleri kullanarak yok edilmesi gerekir.

2.1.2.3. Manyetik bant ve manyetik disk üniteleri

Manyetik bantları ve manyetik disk ünitelerini güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok etmek gerekir.

2.1.2.4. Mobil telefonlar (Sim kart ve sabit hafıza alanları)

Mobil telefonlardaki sabit hafıza alanlarının (2.1.1)'de belirtilen uygun yöntemleri kullanarak yok edilmesi gerekir.

2.1.2.5. Optik diskler (CD, DVD vb.)

Optik disklerin yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleri ile yok edilmesi gerekir.

2.1.2.6. Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri

Tüm veri kayıt ortamlarının söküldüğü doğrulanarak (2.1.1)'de belirtilen uygun yöntemlerin kullanılıp yok edilmesi gerekir.

2.1.2.7. Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri

Söz konusu sistemler için (2.1.1)'de belirtilen uygun yöntemler kullanılarak yok edilme işlemi gerçekleştirilmelidir.

2.1.3. Kâğıt ve Mikrofiş Ortamları

Kalıcı ve fiziksel ortam üzerine yazılı olan kişisel verilerin yok edilmesi için ortamın kâğıt imha veya kırpma makineleri ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünmesi gerekir.

2.1.4. Bulut Ortamı

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve mümkünse kişisel verilerin depolandığı her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Kişisel verilerin yok edilmesi için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

Yukarıda yer alan 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 (2.1.1)'de belirtilen uygun yöntemleri kullanarak yok edilmesi,
ii. Yok etmenin mümkün 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.

3.Kişisel Verilerin Anonimleştirilmesi

Anonim hale getirme işlemi, Şirket'in kişisel verileri tamamen veya otomatik yollarla işlediği durumlarda, bu verilerin doğrudan ve/veya dolaylı tanımlayıcılarının çıkartılarak ya da değiştirilerek, başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonimleştirilmesi Şirket içerisinde Veri Sorumlusu'nun görevidir. Veri Sorumlusu, verilerin yok edilmesi için denetimi kendisi tarafından yapılmak kaydıyla Şirket'in farklı departmanlarından destek alabilir.

Verilerin anonimleştirilmesi sırasında Şirket geri dönülemez şekilde maskeleme, tek yönlü fonksiyonlar ile şifreleme gibi yöntemler kullanılabilir. Uygulanacak yöntemin doğruluğu, Veri Sorumlusu tarafından onaylanamıyorsa kurula danışılmalıdır.

3.1. Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	• Değişkenleri Çıkartma • Kayıtları Çıkartma • Alt ve Üst Sınır Kodlama • Bölgesel Gizleme
Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	• Mikro-Birleştirme • Veri Değiş-Tokuşu • Gürültü Ekleme • Tekrar Örnekleme

3.1.1. 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 satır veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar.

3.1.1.1. Değişkenleri Çıkartma

Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Bu yöntem değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin hassas bir veri olması gibi sebeplerle kullanılabilir.

Yaş	Cinsiyet	Posta Kodu	Gelir	Din
20	K	S017	20,000	~~Budist~~
28	E	S018	22,000	~~Müslüman~~
29	E	S016	32,000	~~Hristiyan~~

3.1.1.2. Kayıtları Çıkartma

Bu yöntemde ise veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır.

Yaş	Cinsiyet	Doğum Y.	Sektör	Derece
31	K	İstanbul	Mimarlık	3.22
31	E	İstanbul	Mimarlık	3.04
31	E	Ankara	Sanayi	3.22
43	K	Ankara	Sanayi	3.40
~~51~~	~~E~~	~~Eskişehir~~	~~Sanat~~	~~2.45~~

3.1.1.3. Bölgesel Gizleme

Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görünebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine sebep olacaksa istisnai durumu yaratan değer “bilinmiyor” olarak değiştirilir.

Yaş	Cinsiyet	Meslek	HIV Durumu
52	K	Öğretmen	Pozitif
28	E	Mimar	Negatif
64	E	Mühendis	Pozitif
30	K	-	Pozitif

Orijinal Veri Kümesi

Yaş	Cinsiyet	Meslek	HIV Durumu
52	K	Öğretmen	Pozitif
28	E	Mimar	Negatif
64	E	Mühendis	Pozitif
Bilinmiyor	K	-	Pozitif

Bölgesel Gizleme Sonrası Veri Kümesi

3.1.1.4. 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.

3.1.1.5. Alt ve Üst Sınır Kodlama

Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir.

Yaş	Cinsiyet	Meslek	Gelir Yıllık	Test Sonucu	Harcamalar
3*	K	Mühendis	92,000	Negatif	8,000
4*	E	Mimar	110.000	Negatif	9.600
4*	E	Doktor	149.000	Negatif	10.000
5*	E	Doktor	125.000	Pozitif	11.100

Orijinal Veri Kümesi

Tablodaki Gelir ve Harcamalar değişkenleri kendi içlerinde sınıflanarak aşağıdaki tabloda anonim halini almıştır.

Yaş	Cinsiyet	Meslek	Gelir Yıllık	Test Sonucu	Harcamalar
3*	K	Mühendis	Düşük	Negatif	Düşük
4*	E	Mimar	Orta	Negatif	Düşük
4*	E	Doktor	Yüksek	Negatif	Orta
5*	E	Doktor	Yüksek	Pozitif	Yüksek

Alt ve üst sınır kodlama sonrası veri kümesi

3.1.1.6. 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.

Cinsiyet	Meslek	İlçe	Medeni Durum
K	Mimar	Çankaya	Evli
K	Mühendis	Çankaya	Bekâr
K	Mimar	Çankaya	Boşanmış
K	Mühendis	Çankaya	Evli

Orijinal Veri Kümesi

Cinsiyet	Meslek	İlçe	Medeni Durum
K	Mimar veya Mühendis	Çankaya	Evli
K	Mimar veya Mühendis	Çankaya	Bekâr
K	Mimar veya Mühendis	Çankaya	Boşanmış
K	Mimar veya Mühendis	Çankaya	Evli

Global kodlama sonrası veri kümesi

3.1.1.7. Örnekleme

Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme 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.

3.1.2. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlayan yöntemlerle mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır. Veri kümesindeki değerler değişiyor olsa bile toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.

3.1.2.1. 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.

Aşağıdaki tabloda "Gelir" sütunundaki değerlerine göre birbirine yakın olan üçerli gruplara ayrılmıştır. Her grup, içindeki değerlerin aritmetik ortalaması alınmış ve bulunan yeni değerler orijinal değerlerin yerine yazılmıştır.

Yaş	Cinsiyet	Posta Kodu	Gelir
23	K	1556	25.000
37	K	1559	28.000
41	E	1559	37.000
25	K	1557	49.000
34	E	1558	56.000
48	E	1556	60.000

Orijinal Veri Kümesi

Yaş	Cinsiyet	Posta Kodu	Gelir
23	K	1556	30.000
37	K	1559	30.000
41	E	1559	30.000
25	K	1557	55.000
34	E	1558	55.000
48	E	1556	55.000

Mikro Birleştirme sonrası veri kümesi

3.1.2.2. Veri Değiş Tokuşu

Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır.

Yaş	Cinsiyet	İl	Gelir
23	K	İstanbul	20.000
37	K	Ankara	30.000
41	E	İzmir	30.000
25	K	İstanbul	25.000
34	E	Ankara	55.000
48	E	İzmir	15.000

Orijinal Veri Kümesi

Yaş	Cinsiyet	İl	Gelir
23	K	İstanbul	25.000
37	K	Ankara	55.000
41	E	İzmir	15.000
25	K	İstanbul	20.000
34	E	İzmir	30.000
48	E	İzmir	30.000

Veri değiş tokuş sonrası veri kümesi

3.1.2.3. Gürültü Ekleme

Bu yöntem ile seçilen değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkarmalar yapılır. Bozulma her değerde eşit ölçüde uygulanır.

Yaş	Cinsiyet	İl	Gelir
21	K	İzmir	45.000
35	E	Ankara	123.000
45	E	Ankara	18.000

Orijinal veri kümesi

Yaş	Cinsiyet	İl	Gelir
21	K	İzmir	50.000
35	E	Ankara	128.000
45	E	Ankara	23.000

Gürültü sonrası veri kümesi

3.2. 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 indirerek veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

i. K-Anonimlik

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.

ii. L-Çeşitlilik

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

iii. T-Yakınlık

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

V. SAKLAMA VE İMHA SÜRELERİ

1. Periyodik İmha ve Yasal Saklama Süreleri

Yasal saklama ve imha sürelerini dolduran fiziksel ve dijital veriler, periyodik olarak imha edilir. Şirket, Kişisel Verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, Kişisel Verileri siler, yok eder veya anonim hale getirir. Periyodik imha, tüm Kişisel Veriler için 6 aylık zaman aralıklarında gerçekleştirilir. Periyodik imha sırasında baz alınacak yasal saklama ve imha süreleri, Şirket Kişisel Veri İşleme Envanteri'nde belirlenmiştir. Şirket,

Yönetmelik madde 11(4) kapsamında Kurul'un süreleri kısaltması durumunda, yeni sürelere uyum sağlayacağını taahhüt eder.

Silinen, yok edilen ve anonim hale getirilen verilere ilişkin işlemlerin diğer hukuki yükümlülüklerden ari en az 3 yıl süre ile saklanır. Şirket'in diğer hukuki yükümlülüklerden kaynaklanan Kişisel Veri saklama hakları saklıdır.

2. Veri Sahiplerinin Talep Etmesi Durumunda Silme ve Yok Etme Süreci

Veri sahiplerinin Şirket'e başvurarak kendisine ait Kişisel Verilerin silinmesini veya yok edilmesini talep ettiği durumlarda Kişisel Verileri işleme şartlarının mevcut durumunu kontrol eder ve buna bağlı ilgili aksiyonları alır.

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

Kişisel Verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan Kişisel Veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

Kişisel Verileri işleme şartlarının tamamı ortadan kalkmamışsa, Şirket ilgili veri sahibine gerekçesini açıklayarak talebi reddedebilir ve ret cevabını ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirir.

VI. KİŞİSEL VERİLERİN SAKLANMASI, İŞLENMESİ VE İMHASI İÇİN ALINAN TEDBİRLER

Şirket, Kişisel Verilerin hukuka uygun şekilde saklanması, işlenmesi ve erişimini sağlamak için korunacak verinin niteliği, teknolojik imkânlar ve uygulama maliyetlerine göre teknik ve idari tedbirler almaktadır.

a. Teknik Tedbirler

Şirket tarafından Kişisel Verilerin hukuka aykırı saklanması, işlenmesi ve erişimini engellemek için alınan başlıca teknik tedbirler aşağıda sıralanmaktadır:

- Belirli periyotlarla ile (yılda en az 1 kez) bilgi sistemlerinin tüm bileşenlerini kapsayacak bir kapsamda sızma testleri yapılmaktadır. Şirket IT sistemlerinde tam kapsamlı (iç ağ, dış ağ, dns, e-posta, etki alanı ve son kullanıcı

bilgisayarları, kablosuz ağ sistemleri, sanallaştırma sistemleri, güvenlik bileşenleri, aktif cihazlar, sınır güvenliği bileşenleri, sosyal mühendislik, web uygulamaları, mobil uygulamalar) sızma testi, yerel bilişim sistemleri ve uygulamalarında ise zafiyet tarama işlemi yapılmaktadır.

- Teknolojideki gelişmelere uygun teknik önlemler alınmakta, alınan önlemler periyodik olarak güncellenmekte ve yenilenmektedir.
- İş birimi bazlı belirlenen hukuksal uyum gerekliliklerine uygun olarak erişim yetkileri etki alanı kontrolcüsü (Active Directory Domain Controller) üzerinden yönetilir ve geriye dönük olarak kontrol edilir.
- Bu kapsamda virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılım ve donanımlar kurulmakta, düzenli yedeklemeler yapılmaktadır.
- Merkezi loglama sisteminin bilişim sistemlerinde kullanılmakta ve loglama mekanizmasının dışarıdan müdahaleye karşı korumak için zaman damgası ile imzalanarak erişim kontrolleri yapılmış bir alanda arşivlenmektedir. Sistemlerin loglarının en az 2 yıl saklanacak şekilde yapılanmıştır.
- SOC / SOME, Şirket'in tüm bilgi sistemlerini çeşitli çözümler vasıtasıyla sürekli olarak izlemek, incelemek ve olası saldırılar karşısında savunma aksiyonları almak için tahsis edilmiş ekibin oluşturduğu yapılanmadır. Şirket bilişim sistemlerinde sistemleri sürekli izlenmekte ve oluşan alarmlara göre önlemler alınmaktadır.

- Kişisel veri içeren fiziksel alanların güvenliğinin sağlanması, erişim kontrollerinin sürekli olarak sağlanması, kişisel veri içeren fiziki dokümanların dış etmenlerden korunan bir alanda saklanmaktadır.
- Fiziksel olarak saklanan kişisel veri içeren dokümanların imhası için politikanın uygulanması önerilmektedir.
- Kişisel veri içeren tüm sistemlerde yetkisiz erişimlerin önüne geçmek amacıyla tüm disk ve medya aygıtlarının şifrelenir. (full disk encryption)
- Kişisel verilerin iletildiği uygulamalar veya ağ bileşenlerinde, ağ trafiğinin güvenli bir protokol/kanal üzerinden yapılması (SSL, VPN, https vb.) ağ trafiğinin dinlenerek bilgi ifşasına maruz kalma riskini azaltmaktadır. Kişisel veri içeren web uygulamalarının sadece "https" üzerinden hizmet vermesi ve kişisel

veri içeren bilgilerin transferinin ise kriptografik olarak güvenli kabul edilen bir kanal (sFTP, VPN vb.) ile yapılmaktadır.

- Bu kapsamda güvenlik duvarları, saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Alınan teknik önlemler periyodik olarak Şirket KVKK Sorumlusuna raporlanmakta, risk teşkil eden hususlar yeniden değerlendirilerek gerekli teknolojik çözüm üretilmektedir.
- Teknik konularda bilgili personel ihtiyacı KVKK sorumlusu tarafından takip edilir, ihtiyaç halinde bu kişiler istihdam edilmekte ve KVKK Komitesi'nin daimi üyesi yapılmaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Şirket'e bildirmek için Şirket tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- 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.

b. İdari Tedbirler

Şirket tarafından Kişisel Verilerin hukuka aykırı saklanması, işlenmesi ve erişimini engellemek için alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

- Şirket çalışanlarına Kişisel Verileri Koruma mevzuatı kapsamında bilgilendirmiş ve bu konuda gerekli eğitimlerden geçirmiştir. Eğitimler kapsamında, çalışanlara rolleri ve sorumlulukları anlatılmış, “yasaklanmadıkça her şey serbest” değil “izin verilmedikçe her şey yasak” prensibi hakkında bilgilendirme yapılmıştır.
- Çalışanlar ile öğrendikleri Kişisel Verileri ilgili mevzuat hükümlerine aykırı olarak başkasına açıklayamayacağı, işleme amacı dışında kullanamayacağı ve bu yükümlülüğün görevden ayrılmalarından sonra da devam edeceği konusunda gizlilik sözleşmesi imzalanarak Kişisel Verilerin Korunması adına gerekli taahhütler alınmıştır. Bu kapsamda İş Sözleşmeleri ve disiplin yönetmeliklere Kanun’a uygun hükümler eklenmiştir. Şirket içi organizasyonlarında, bu taahhütlere ve sair gizlilik yükümlülüklerine uyulmaması durumunda işletilecek disiplin süreçlerini hazırlamıştır.
- Veri Sorumluları Sicil Bilgi Sistemine bildirim yapılabilmesi için gerekli hazırlıklarını tamamlamıştır.
- İş birimi bazlı hukuksal uyum gerekliliklerine uygun olarak Şirket içinde Kişisel Verilere erişim ve yetkilendirme süreçleri tasarlanmış ve uygulanmaktadır.
- Şirket tarafından Kişisel Verilerin hukuka uygun olarak aktarıldığı kişiler ile akdedilen sözleşmelere; Kişisel Verilerin aktarıldığı kişilerin, Kişisel Verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlayacağına ilişkin hükümler eklenmektedir.
- Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha konularında işbu Politika kapsamında gerekli düzenlemeleri yapmıştır
- Kişisel Veri İşleme Envanteri hazırlanmış ve Kişisel Verilerin işlenmesi, muhafazası ve aktarılmasına ilişkin sözleşmelerde gerekli hükümlere yer vermiş,
- Kurum İçi Periyodik ve/veya Rastgele Denetimler için gerekli hazırlıklar yapılmıştır. Risk Analizleri gerçekleştirilerek gerekli önlemler alınmıştır.
- İhlal durumunda kurumsal iletişim prosedürleri ve bilgilendirme süreçleri işbu Politika’da belirleniştir.

- Kişisel Verilerin Korunması Konusunda Alınan Tedbirlerin Denetimi
- Şirket, KVK Kanunu'nun 12. maddesine uygun olarak, kendi bünyesinde oluşturduğu KVKK Komitesi aracılığı ile gerekli denetimleri yapmakta veya yaptırmaktadır. Bu denetim sonuçları Şirket'in iç işleyişi kapsamında konu ile ilgili bölüme raporlanmakta ve alınan tedbirlerin iyileştirilmesi için gerekli faaliyetler yürütülmektedir.

VII. SAKLAMA VE İMHA SÜREÇLERİNDE YER ALACAK KİŞİLERİN BİLGİLERİ

Şirket kendi bünyesinde, işbu Politika ve bu Politika ile ilişkili diğer politikaları yönetmek üzere Şirket Yönetim Kurulu kararı gereğince "KVKK Komitesi" kurmuştur. Bu komitenin görevleri aşağıda belirtilmektedir.

- Kişisel Verilerin Korunması ve İşlenmesi ile ilgili temel politikaları hazırlamak ve yürürlüğe koymak üzere Yönetim Kurulu'nun onayına sunmak.
- Kişisel Verilerin Korunması ve İşlenmesine ilişkin politikaların uygulanması ve denetiminin ne şekilde yerine getirileceğine karar vermek ve bu çerçevede Şirket içi görevlendirmede bulunmak ve koordinasyonu sağlamak hususlarını Yönetim Kurulu'nun onayına sunmak.
- Kanun ve ilgili mevzuata uyumun sağlanması için yapılması gereken hususları tespit etmek ve yapılması gerekenleri Yönetim Kurulu'nun onayına sunmak; uygulanmasını gözetmek ve koordinasyonunu sağlamak.
- Kişisel Verilerin Korunması ve İşlenmesi konusunda Şirket içerisinde ve Şirket'in işbirliği içerisinde olduğu kurumlar nezdinde farkındalığı arttırmak.
- Şirket'in Kişisel Veri işleme faaliyetlerinde oluşabilecek riskleri tespit ederek gerekli önlemlerin alınmasını temin etmek; iyileştirme önerilerini Yönetim Kurulu'nun onayını sunmak.
- Kişisel Verilerin korunması ve politikaların uygulanması konusunda eğitimler tasarlamak ve icra edilmesini sağlamak.
- Kişisel Veri sahiplerinin başvurularını en üst düzeyde karara bağlamak.
- Kişisel Veri sahiplerinin; Kişisel Veri işleme faaliyetleri ve kanuni hakları konusunda bilgilenmelerini temin etmek üzere bilgilendirme ve eğitim faaliyetlerinin icrasını koordine etmek.

- Kişisel Verilerin Korunması ve İşlenmesi ile ilgili temel politikalardaki değişiklikleri hazırlamak ve yürürlüğe koymak üzere Yönetim Kurulu'nun onayına sunmak.
- Kişisel Verilerin Korunması konusundaki gelişmeleri ve düzenlemeleri takip etmek; bu gelişmelere ve düzenlemelere uygun olarak Şirket içinde yapılması gerekenler konusunda Yönetim Kurulu'na tavsiyelerde bulunmak.
- Kişisel Verilerin Korunması Kurulu ve Kurumu ile olan ilişkileri koordine etmek.
- Yönetim Kurulu'nun Kişisel Verilerin korunması konusunda vereceği diğer görevleri icra etmek.

KVKK Komitesi, ... üyeden oluşur ve salt çoğunluk ile karar alır. Üyeler 2 yıl süre ile Yönetim Kurulu tarafından belirlenir. Yönetim Kurulu Kişisel Verilerin Korunması mevzuatı uyarınca bütün görev ve yetkilerini TTK 367 uyarınca Şirket KVKK Komitesi'ne devretmiştir.

KVKK Komitesi, bu Politikada sayılan görevleri aşağıda birimleri, unvanları ve görev tanımları verilen üyeleri aracılığı ile yerine getirir. Üyelerin görevlerini yerine getirmesi sırasında KVKK Komitesi denetim görevini icra eder. Herhangi bir KVKK Komitesi üyesinin görevi bırakması durumunda ayrılan üyenin görev süresini tamamlamak üzere KVKK Komitesi yeni bir üye seçer, bu üye seçimini takip eden ilk Yönetim Kurulu'nda onaya sunulur. Şirket, yeni üyeleri de işbu Politika ve Kişisel Verileri korunması mevzuatı konusunda bilgilendirecek ve yeni çalışanlar bu görevlerin kesintisiz olarak yerine getirilmesini sağlayacaktır.

Şirket KVKK Komitesi Üyeleri			
	Unvan	**Birim**	**Görev Tanımı**
1.	KVKK Sorumlusu		KVKK'na uyumun sağlanması ve korunması
2.			
3.			
4.			
5.			

VIII. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11'inci maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Kurumda her yıl Ocak ve Temmuz aylarında periyodik imha işlemi gerçekleştirilir.

IX. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da …… dosyasında saklanır.

X. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Şirket'in internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları Kurul Kararı ile …. tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile …. tarafından saklanır.

XI. POLİTİKA'DA YAPILACAK DEĞİŞİKLİKLER

1. İlgili mevzuatta yapılacak her türlü resmi değişikliğin ardından bu değişiklerle uyumlu olacak şekilde Şirket tarafından işbu Politika'da değişiklik yapılabilir.
2. Şirket, Politika üzerinde yaptığı değişiklikler izlenebilecek şekilde, güncellenen Politika'yı e-posta yolu ile çalışanlarıyla paylaşacak ve aşağıdaki web adresi üzerinden çalışanlarının erişimine sunacaktır.
   İlgili web adresi: makstone@hs02.kep.tr

XII. POLİTİKA'NIN YÜRÜRLÜK TARİHİ

İşbu Politika 25.11.2020 tarihinde yürürlüğe girmiştir.