SANİTER	KVKK VERİ KORUMA POLİTİKASI

İÇİNDEKİLER

SANİTER	KVKK VERİ KORUMA POLİTİKASI

1- GİRİŞ

a. Amaç

Bu dokümanın amacı, Kişisel Veri Saklama ve İmha Politikası ("Politika"), 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("KVKK" ya da "Kanun") ve Kanun'un ikincil düzenlenmesini teşkil eden 28 Ekim 2017 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") uyarınca yükümlülüklerimizi yerine getirmek ve veri sahiplerini kişisel verilerinizin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirmek amacıyla veri sorumlusu sıfatıyla Saniter tarafından hazırlanmıştır.

b. Kapsam

Kurum çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Kurumun sahip olduğu ya da Kurumca yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

c. Kısaltma ve Tanımlar

KISALTMA	TANIM
AÇIK RIZA	Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza.
GDPR	95/46/EC sayılı direktifi 25.05.2018 tarihinde yürürlükten kaldıran 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nü
İLGİLİ KULLANICI	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 kişilerdir.
İMHA	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
KANUN / KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
KAYIT ORTAMI	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
KİŞİSEL VERİ	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
KİŞİSEL VERİLERİN AKTARILMASI	Kişisel verilerin KVKK'ya uygun bir biçimde işbu Politika'nın 5. maddesine uygun olarak yurt içi veya dışındaki kurum, kuruluş, tedarikçi vb. paylaşılması,
KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ	Kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilmeyecek hale getirilmesi.

KİŞİSEL VERİLERİN İŞLENMESİ	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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
KİŞİSEL VERİLERİN SİLİNMESİ	Kişisel verilerin silinmesi; kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
KİŞİSEL VERİLERİN YOK EDİLMESİ	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
KOMİTE	Saniter Kişisel Verileri Koruma Komitesi
KURUM	Kişisel Verileri Koruma Kurumu
OTOMATİK VERİ İŞLEME	İnsan müdahalesi ya da yardımı konusundaki ihtiyacı asgari seviyeye indiren, kendi aralarında bağlantılı ve etkileşimli elektrikli veya elektronik bir sistem tarafından gerçekleştirilen kişisel veri işleme faaliyetini
OTOMATİK OLMAYAN VERİ İŞLEME	İnsan müdahalesi ya da yardımı yoluyla yani elle yapılan kişisel veri işleme faaliyetini,
ÖZEL NİTELİKLİ KİŞİSEL VERİ	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 mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.
PERİYODİK İMHA	Kanun'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 ve anonim hale getirme işlemi
VERİ SAHİBİ / İLGİLİ KİŞİ	Kişisel verisi işlenen gerçek kişi
VERİ SORUMLUSU	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
YÖNETMELİK	28 Ekim 2017 tarihinde Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2- KİŞİSEL VERİLERİN İŞLENMESİ VE KORUNMASINA İLİŞKİN OLARAK SANİTER TARAFINDAN BENİMSENEN İLKELER

a. Temel Kişisel Veri İşleme İlkelerine Uygunluk

Firma tarafından, kişisel verilerin korunması mevzuatına uyum sağlanması ve uyumun sürdürülmesi kapsamında aşağıda sıralanan temel ilkeler benimsenmektedir:

(1) Kişisel verileri hukuka ve dürüstlük kurallarına uygun olarak işleme

Firma, Türkiye Cumhuriyeti Anayasası başta olmak üzere, kişisel verilerin korunması mevzuatına uygun olarak, kişisel veri işleme faaliyetlerini hukuka ve dürüstlük kuralına uygun olarak yürütür.

(2) İşlenen kişisel verilerin doğruluğunu ve güncelliğini temin etme

Firma tarafından kişisel verilerin işlenmesi faaliyeti yürütülürken, teknik imkânlar dâhilinde kişisel verilerin doğruluğunu ve güncelliğini sağlamaya yönelik gerekli her türlü idari ve teknik tedbirler alınmaktadır.

(3) Kişisel verilerin belirli, açık ve meşru amaçlar için işlenmesi

Firma tarafından kişisel verilerin işlenmesi faaliyetleri, kişisel veri işleme faaliyeti başlamadan önce belirlenmiş olan, açık ve hukuka uygun amaçlar dâhilinde yürütülmektedir.

(4) Kişisel verileri amaçla bağlantılı, sınırlı ve ölçülü bir biçimde işleme

Firma tarafından, kişisel veriler, veri işleme şartları ile bağlantılı ve bu hizmetlerin gerçekleştirilmesi için gerektiği kadar işlenmektedir. Bu kapsamda, kişisel veri işleme amacı, kişisel veri işleme faaliyetine başlanmadan önce belirlenerek, ileride kullanılabileceği varsayımı ile veri işleme faaliyeti yürütülmemektedir.

(5) Kişisel verileri ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etme

Firma, kişisel verileri, ilgili mevzuatta öngörülen veya veri işleme amacının gerektirdiği süre ile sınırlı olarak muhafaza etmektedir. Bu doğrultuda mevzuatta öngörülen sürenin bitimi veya kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler Firma tarafından silinmektedir.

b. Kişisel Veri İşleme Şartlarına Uygunluk

Firma, kişisel veri işleme faaliyetlerini, KVKK'nın 5. maddesinde ortaya konulan veri işleme şartlarına uygun olarak yürütmektedir. Bu kapsamda, yürütülen kişisel

veri işleme faaliyetleri aşağıda sıralanan kişisel veri işleme şartlarının varlığı halinde gerçekleştirilmektedir:

(1) Kişisel Veri Sahibinin Açık Rızasının Varlığı
(2) Kişisel Veri İşleme Faaliyetinin Kanunlarda Açıkça Öngörülmüş Olması
(3) Fiili İmkânsızlık Nedeniyle Veri Sahibinin Açık Rızasının Elde Edilememesi ve Kişisel Veri İşlemenin Zorunlu
(4) Kişisel Veri İşleme Faaliyetinin Bir Sözleşmenin Kurulması veya İfasıyla Doğrudan Doğruya İlgili Olması
(5) Firma'nın Hukuki Yükümlülüğünü Yerine Getirmesi için Kişisel Veri İşleme Faaliyeti Yürütülmesinin Zorunlu Olması
(6) Bir Hakkın Tesisi, Kullanılması veya Korunması için Veri İşlemenin Zorunlu Olması
(7) Veri Sahibinin Kişisel Verisini Alenileştirmesi
(8) Veri Sahibinin Temel Hak ve Özgürlüklerine Zarar Vermemek Şartıyla Kişisel Veri İşleme Faaliyetinin Yürütülmesinin Saniter'in Meşru Menfaatleri için Gerekli Olması

c. Özel Nitelikli Kişisel Veri İşleme Şartlarına Uygunluk

Özel nitelikli kişisel veriler, Firma tarafından belirlenen yeterli önlemlerin alınması şartıyla aşağıdaki durumlarda işlenebilmektedir:

(1) Firma tarafından kişisel sağlık verileri, aşağıda sıralanan şartlardan birinin varlığı halinde işlenebilmektedir:

- Kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından veya
- Kişisel veri sahibinin açık rızasının varlığı.

(2) Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler (ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri); veri sahibinin açık rıza vermesi veya kanunlarda öngörülen hallerde işlenebilmektedir.

3- SORUMLULUK VE GÖREV DAĞILIMLARI

a. Komite'nin Görev ve Sorumlulukları

- Düzenli olarak toplanmalı, Şirketin veri politikasına uygunluğu ve Kurum kararlarını incelemeli, değerlendirilmeli
- Komite her toplantısının toplantı tutanaklarını yönetimle ve gerek duyduğunda şirket avukatları ile paylaşmalı
- Kişisel Verileri Koruma Kurumu karar ve uygulamalarını Kurum'un web sitesinden güncel olarak takip etmek
- İhtiyaç duyduğu ya da tereddüde düştüğü her konuda şirket avukatları ile iletişim halinde olmak
- İlgililer tarafından kişisel verileri hakkında Şirket'e yapılan başvuru işlemlerinin sonuçlandırılmasını gerçekleştirmek

b. Firma Departmanları'nın Görev ve Sorumlulukları

Unvan	Görev
Genel Müdür	İşyerindeki görev tanımı dâhilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, işlenen kişisel verilerin amaç ile orantılı şekilde saklanmasının sağlanması, ilgililerden gelebilecek her türlü başvuruya gerekli özenin gösterilerek başvuruların takip edilmesi ve sonuçlandırılması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi, şirket ağından erişilebilen dijital verilerle ilgili teknik tedbirlerin alınması,
İdari İşler ve Muhasebe Sorumlusu	İşyerindeki görev tanımı dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, işlenen kişisel verilerin amaç ile orantılı şekilde saklanmasının sağlanması, ilgililerden gelebilecek her türlü başvuruya gerekli özenin gösterilerek başvuruların takip edilmesi ve sonuçlandırılması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi,insan kaynakları süreçleriyle ilgili gerekli teknik ve idari tedbirlerin alınması
Sistem Yöneticisi	İşyerindeki görev tanımı dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, işlenen kişisel verilerin amaç ile orantılı şekilde saklanmasının sağlanması,

Teknik Müdür	İşyerindeki görev tanımı dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, işlenen kişisel verilerin amaç ile orantılı şekilde saklanmasının sağlanması,

4- KAYIT ORTAMLARI

Kişisel veriler, aşağıda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Elektronik ortamlar	Elektronik olmayan ortamlar
- Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) - Yazılımlar (ofis yazılımları, IK portal,….) - Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) - Kişisel bilgisayarlar (Masaüstü, dizüstü) - Mobil cihazlar (telefon, tablet vb.) - Optik diskler (CD, DVD vb.) - Çıkartılabilir bellekler (USB, Hafıza Kart vb.) - Yazıcı, tarayıcı, fotokopi makinesi	- Kağıt - Manuel veri kayıt sistemleri (tur ve transfer bilet koçanları) - Yazılı, basılı, görsel ortamlar

5- KİŞİSEL VERİLERİN AKTARIMI

Kişisel veriler, Saniter tarafından hizmetin görülebilmesi amacıyla iş ve çözüm ortakları ile ve Saniter iştirakleri ile paylaşılabilir.

KVKK başta olmak üzere ulusal ve uluslararası mevzuat hükümleri çerçevesinde Firma, işlediği kişisel verileri yurt içinde ya da yurt dışına aktarabilir. Transfer işlemlerine tabi tutabilir. Bu işlemler sırasında KVK Kanunu 8 ve 9 uncu maddeleri ile 95/46/EC Sayılı Direktif ve bu direktifi yürürlükten kaldıran GDPR hükümleri dikkate alınmaktadır. Firma,

kişisel verilerin yurt içinde ve dışına aktarımı konusunda yukarıda belirtilen kanun maddeleri ile direktiflerin öngördüğü şartları yerine getirmiştir.

a. Kişisel Verilerin Yurtiçinde Aktarılması

Firma, KVKK'nın 8. ve 9.maddelerinin verdiği yetki ve işbu politika çerçevesinde ilgili kişinin açık rızasını almak suretiyle, işlediği verileri üçüncü kişilere aktarabilir. Firma tarafından, kişisel verilerin korunması mevzuatına uyum sağlanması ve uyumun sürdürülmesi kapsamında aşağıda sıralanan temel ilkeler işbu Politikanın 2. Bölümünde açıklanmıştır.

Kişisel verilerin yurtiçinde aktarılmasında diğer kanunlarda yer alan hükümler saklıdır.

İşbu KVK Politikası kapsamında herhangi bir Veri İşleyen 'in söz konusu olması halinde, Veri İşleyen ile Firma arasındaki kişisel veri transferlerinde KVK Kanunu'nun 8 inci madde hükümleri uygulanır. Hemen belirtmek gerekir ki; Veri sorumlusu sıfatına sahip Saniter tüzel kişiliği bünyesinde gerçekleşen, tüzel kişilikte faaliyet gösteren çalışanlar ve farklı departmanlar arasındaki veri aktarımı, KVK Kanunu'nun 8. maddesi çerçevesinde aktarım olarak kabul edilmemektedir. Ancak Saniter ile işbirliği veya çözüm ortağı olarak faaliyet gösteren ayrı tüzel kişiliğe sahip olanlarla gerçekleşen veri aktarımları, KVK Kanunu 8 inci ve 9 uncu madde ile işbu KVK Politikası kapsamında veri transferi olarak değerlendirilmektedir

b. Kişisel Verilerin Yurtdışında Aktarılması

Firma tarafından, KVKK'nın 9. maddesi gereğince kişisel veriler;

(1) Kişisel veri işleme şartlarına uygun olarak,
(2) Aktarım yapılacak ülkenin Kişisel Verileri Koruma Kurulu tarafından ilan edilen yeterli korumaya sahip ülkelerden olması veya ilgili yabancı ülkede yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve KVK Kurulunun izninin bulunması ile yurtdışına aktarılabilmektedir.

6- SAKLAMA VE İMHAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Veri sahiplerine ait kişisel veriler, Firma tarafından özellikle ticari faaliyetlerin sürdürülebilmesi, hukuki yükümlülüklerin yerine getirilebilmesi, çalışan haklarının ve yan haklarının planlanması ve ifası ile müşteri ilişkilerinin yönetilebilmesi amacıyla yukarıda

sayılan fiziki veyahut elektronik ortamlarda güvenli bir biçimde KVKK ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

a. Saklamaya İlişkin Açıklamalar

Hukuka ve işbu Politika'ya uygun olarak işlenen kişisel veriler aşağıdaki şartların varlığında saklanabilecektir.

- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Firma'nın meşru menfaatleri için saklanmasının zorunlu olması,
- Kişisel verilerin Firma'nın herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

b. İmhayı Gerektiren Sebepler

Yönetmelik uyarınca, aşağıda sayılan hallerde veri sahiplerine ait kişisel veriler, Firma tarafından re'sen yahut talep üzerine silinir, yok edilir veya anonim hale getirilir.

- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ifası,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kanun'un 5. Ve 6. Maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- Kişisel verileri işlemeni sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alma,
- İlgili kişinin, Kanun'un 11. Maddesinin 2 (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesini, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
- 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 Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunulması,

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

7- KİŞİSEL VERİ SAHİPLERİNİN HAKLARI VE FİRMA TARAFINDAN TALEPLERİNİN SONUÇLANDIRILMASI

Veri sahiplerinin kişisel verilerine ilişkin taleplerini Firma'ya yazılı olarak veya KVK Kurulu tarafından belirlenen diğer yöntemler ile iletmeleri durumunda, Firma veri sorumlusu sıfatıyla KVK Kanunu'nun 13. maddesine uygun olarak, talebin niteliğine göre en kısa sürede ve en geç otuz (30) gün içinde sonuçlandırılmasını sağlamak üzere gerekli süreçleri yürütmektedir. Veri sahipleri kişisel verilerine ilişkin taleplerini Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ doğrultusunda gerçekleştirmelidir.

Firma, veri güvenliğinin sağlanması kapsamında, başvuruda bulunan kişinin başvuruya konu kişisel verinin sahibi olup olmadığını tespit etmek amacıyla bilgi talep edebilir. Şirketimiz ayrıca kişisel veri sahibinin başvurusunun talebe uygun bir biçimde sonuçlandırılmasını sağlamak adına, kişisel veri sahibine başvurusu ile ilgili soru yöneltebilir.

Veri sahibinin başvurusunun; diğer kişilerin hak ve özgürlüklerini engelleme ihtimali olması, orantısız çaba gerektirmesi, bilginin kamuya açık bir bilgi olması gibi durumlarda, Firma tarafından gerekçesi açıklanarak talep reddedilebilecektir.

Kişisel Veri Sahiplerinin Hakları KVK Kanunu'nun 11. maddesi uyarınca, Şirketimize başvurarak aşağıda yer alan konularda talepte bulunabilirsiniz:

(1) Kişisel verilerinizin işlenip işlenmediğini öğrenmek,

(2) Kişisel verileriniz işlenmişse buna ilişkin bilgi talep etmek,

(3) Kişisel verilerinizin işlenme amacı ve bunların amacına uygun kullanılıp kullanılmadığını öğrenmek,

(4) Kişisel verilerinizin yurt içinde veya yurt dışında aktarıldığı üçüncü kişileri öğrenmek,

(5) Kişisel verilerinizin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini istemek ve bu kapsamda yapılan işlemin kişisel verilerinizin aktarıldığı üçüncü kişilere bildirilmesini istemek,

(6) KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerinizin silinmesini, yok edilmesini veya anonim hale getirilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerinizin aktarıldığı üçüncü kişilere bildirilmesini istemek,

(7) İşlenen verilerinizin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle aleyhinize bir sonucun ortaya çıkmasına itiraz etmek,

(8) Kişisel verilerinizin kanuna aykırı olarak işlenmesi sebebiyle zarara uğramanız halinde zararın giderilmesini talep etmek.

8- TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12 nci maddesiyle Kanunun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Komite tarafından teknik ve idari tedbirler alınır. Saniter' de IT departmanı olmamakla birlikte Teknik tedbirler dış satın alım ile gerçekleşmektedir.

a. Teknik Tedbirler

- Sızma (Penetrasyon) testleri ile Şirketimiz 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.

- Şirketimizin 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.
- Şirket 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.
- Şirket, 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 Şirket tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.(E-Posta sistemi) Bu gibi durumlarda şirketimiz kep adresi olan saniter@hs02.kep.tr adreslerinden iletilen taleplere kanunen uygun görülen süre içinde yanıt verilmektedir.
- 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.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir. Bu verilerin dijital ortamda olan kısmı Web üzerinden hizmet veren ve gerekli güvenlik sertifikasyonlarına sahip olan İnsan Kaynakları uygulamasında, dijital olmayan dosyalar ise özlük dosyalarında kilit altında tutulmakta ve yalnızca İnsan Kaynakları departmanı çalışanları tarafından erişilebilmektedir.
- 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.

- Bilgisayar ortamında muhafaza edilen kayıtlara internet üzerinden karşılaşılabilecek tehditlere karşı sisteme fortinet firewall güvenlik duvarı kurulmuş olup, güvenlik duvarı üzerinden gerekli web giriş kısıtlamaları ve log kayıtları tutulmaktadır. Virüs kontrolü için bilgisayarlar da bulunan ESET NOD 32 antivirüs programı kullanılmaktadır. Virüs programı her yıl güncellenir. Bilgisayarda muhafaza edilen Kalite Kayıtları, Comoda Back Up Programı ile her gün 12.30-13.30 saatleri arasında otomatik olarak harici hard diske yedeklenir. Kayıtların güvenliği dosya erişimlerinin kısıtlanması şifrelenmesi suretiyle sağlanır. Güvenli yedekleme için TeraCopy programı kullanılır ayrıca Manuel yedeklemelerde yapılmaktadır. Hard diskler için kritik stok seviyesi 50 GB olup kritik stok seviyesinde yeni hard satın alınacağı beyan edilir.

b. İdari Tedbirler

Şirket 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 ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Şirket tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Şirket içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

9- KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

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.

a. Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için İdari İşler ve Muhasebe Sorumlusu 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, veritabanı 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 kontrolünde imha edilir.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, İdari İşler ve Muhasebe Sorumlusu tarafından yedeklenerek ve erişim yetkisi sadece İdari İşler ve Muhasebe Sorumlusuna verilerek güvenli ortamlarda saklanır.

b. Kişisel Verilerin Yok Edilmesi

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.

10- SAKLAMA VE İMHA SÜRELERİ

Şirket 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 P.03 Kalite Kayıtları Prosedürüne bağlı L.03.01 Kalite Kayıt Listesinde

yer alır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Komite tarafından yerine getirilir.

Süreç	Saklama Süresi	İmha Süresi
Sözleşmelerin hazırlanması	Sözleşmenin sona ermesini takiben 6 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	İş Başvurusu Amaçlı Toplanan Kayıtlar 1 ay İşe kabul edilen, Çalışan Personel Kayıtları Çalıştığı Süre boyunca ve İşten Ayrıldıktan Sonra 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Takip Sistemleri (5651 sayılı kanuna istinaden)	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi ve Toplantı	Etkinliğin sona ermesini	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kamera Kayıtları	13 gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kullanılan Yazılımlara Erişim (acente otomasyon, e-posta vb.)	Faaliyetin sona ermesiyle	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Nasserver Üzerinden Saklama	6 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

5651 sayılı kanununa istinaden şirketimizde bulunan tüm bilgisayarların ip adresleri ve bu ip adreslerin hangi sitelere çıkış yaptıkları, çıkış yapılan sitelerin ip adresleri erişim tarihleri kayıt altında tutulmaktadır. Şirketimizde yasal olmayan tüm siteler güvenlik duvarı üzerinden kısıtlanmıştır. Şirketimiz içerisinden engelli sitelere giriş yapan kullanıcılar engellenir ve giriş yapılma denemeleri kayıt altına alınır.

Nasserver Depolama Ünitesinde her personel kullanıcı hesap üzerinde ayrı bölümlerde ayrı dosyalama ile verilere ulaşım sağlar. Personel kendi bölümleri dışındaki dosyalara erişim sağlayamayacaktır. İçerisinde Bulunan Disk Anlık Olarak Tüm Verileri İçindeki 2. Diske

Aktarım Yapar. Yedekleme yazılımı ile her gün akşam Saat: 20:00 da korumalı olarak harici diske otomatik yedeklenir. Depolama ünitesine dışardan girişler engellidir. Girişler sadece güvenlik duvarı kontrolü üzerinden şifreli olarak yapılır.

11- PERİYODİK İMHA SÜRESİ

Periyodik imha süreleri 12 ay olarak belirlenmiştir. Şirket bünyesinde her yıl Ocak ayında arasında Komite tarafından uygun görülen tarihte, saklama süresini geçen tüm süreçler için periyodik imha işlemi gerçekleştirilir.

12- POLİTİKANIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kağıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kağıt nüshası İnsan Kaynakları Departmanında bulunan kilitli kartoteks dolapta saklanır.

13- POLİTİKA'NIN GÜNCELLENME PERİYODU

Politika ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir. Güncellemeler kurum web sayfasında yayınlanır.