SENSÖRLER VE İLERİ CİHAZLAR KONTROL A.Ş.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

SENSÖRLER VE İLERİ CİHAZLAR KONTROL A.Ş.

Adres : Bayraktar Bulvarı No:23 Şerifali 34775 /Ümraniye/İSTANBUL

Telefon/Faks : 0(216) 528 5000 / 0(216) 528 5050

Web : http://www.sick.com/tr

İçindekiler Tablosu

1. GİRİŞ

1.1. **SENSÖRLER VE İLERİ CİHAZLAR KONTROL A.Ş.** *("SICK")* için kişisel verilerin korunması büyük bir öneme sahiptir. Şirket ortaklarımızın, yetkililerimizin, çalışanlarımızın, stajyerlerimizin, referans gösterilen kişilerin, çalışanlarımızın aile bireyleri ve yakınlarının, çalışan adaylarımızın, ziyaretçilerimizin; tedarikçilerimizin, tedarikçi çalışanlarının-yetkililerinin ve ortaklarının; müşterilerimizin, potansiyel müşterilerimizin, müşteri çalışanlarının-yetkililerinin-iş ortaklarının; iş ortaklarımızın-yetkililerinin-çalışanlarının ve ilgili üçüncü kişilerin kişisel verilerinin korunmasında büyük hassasiyet gösterilmektedir.

1.2. Kişisel verilerin işlenmesi ve korunması konusunda SICK tarafından benimsenen ilkeleri ortaya koyan "*Kişisel Verilerin Korunması ve İşlenmesi Politikası*", http://www.sick.com/tr internet sitesinde ilgili kişilerin bilgisine sunulmuştur.

2. POLİTİKA'NIN AMACI

2.1. Kişisel Veri Saklama ve İmha Politikası ("***Politika***"), SICK tarafından gerçekleştirilen kişisel verilerin saklanması, imhası, yok edilmesi, anonim hale getirilmesi süreçlerine ilişkin iş ve/veya işlemler hakkındaki usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

2.2. Kişisel verilerin saklanması, imhası, yok edilmesi ve anonim hale getirilmesi süreçlerine ilişkin iş ve/veya işlemler, SICK tarafından bu doğrultuda hazırlanmış olan Politika'ya uygun biçimde gerçekleştirilir.

3. POLİTİKA'NIN KAPSAMI

3.1. İşbu Politika; Şirket ortaklarımıza, yetkililerimize, çalışanlarımıza, stajyerlerimize, referans gösterilen kişilere, çalışanlarımızın aile bireyleri ve yakınlarına, çalışan adaylarımıza, ziyaretçilerimize; tedarikçilerimize, tedarikçi çalışanlarına-yetkililerine ve ortaklarına; müşterilerimize, potansiyel müşterilerimize, müşteri çalışanlarına-yetkililerine-iş ortaklarına; iş ortaklarımızın-yetkililerine-çalışanlarına ve ilgili üçüncü kişilere ait tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen her türlü kişisel veriyi kapsamaktadır.

3.2. SICK'in sahip olduğu veya SICK tarafından yönetilen, kişisel verilerin işlendiği ilgili kayıt ortamları ve kişisel verilere ilişkin iş, işlem ve faaliyetlerde işbu Politika uygulanır.

4. TANIMLAR

Bu Politika'da geçen,

- **Açık Rıza:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
- **Alıcı Grubu:** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,
- **Anonim Hâle Getirme:** Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,

- **SICK Kişisel Verilerin Korunması Komisyonu ("Komisyon"):** Şirket içi İmha Politikası ve Kişisel Verilerin Korunması ve İşlenmesi Politikasının uygulanmasından sorumlu komisyonu,
- **İlgili Kişi:** Kişisel verisi işlenen gerçek kişiyi,
- **Çalışan:** SICK personelini,
- **Çalışan Adayı:** SICK bünyesinde çalışan olmak amacıyla, elektronik veya fiziki ortamda, SICK'e herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini SICK'in incelemesine bizzat veya bir sistem veya kişi aracılığıyla açmış/iletmiş olan gerçek kişileri,
- **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 kişileri,
- **Ziyaretçi:** SICK'in sahip olduğu fiziksel yerleşkelere çeşitli amaçlarla girmiş olan veya internet sitelerimizi ziyaret eden gerçek kişileri,
- **İş Ortağı:** SICK'in ticari faaliyetlerini yürütürken birlikte muhtelif projeler yapmak, hizmet almak, şirket içi operasyonel verimliliği arttırmak gibi amaçlarla iş ortaklığı kurduğu tarafları,
- **Şirket Yetkilisi:** SICK yönetim kurulu üyelerini ve diğer yetkili kişileri,
- **Şirket Ortakları:** SICK ortağı gerçek kişileri,
- **Müşteri:** SICK'in iş birimlerinin yürüttüğü operasyonlar kapsamında SICK'in iş ilişkileri üzerinden kişisel verileri elde edilen gerçek kişiler,
- **İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
  Silme: Kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi,
  Yok Etme: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi,
  Anonim Hale Getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi,
- **İmha Politikası:** İşbu Kişisel Veri Saklama ve İmha Politikası'nı
- **Kanun:** 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,
- **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 ortamı,
- **Elektronik Ortamlar:** Kişisel verilerin ilgili teknolojik altyapıya sahip cihazlar ile oluşturulabildiği, işlenebildiği, saklanabildiği ve iletilebildiği ortamı,
- **Elektronik Olmayan Diğer Ortamlar:** Elektronik ortamların dışında kalan her türlü yazılı, görsel ve sair ortamları,
- **Hizmet Sağlayıcı:** SICK ile yapmış olduğu ilgili sözleşme çerçevesinde, herhangi bir hizmet sağlayan gerçek veya tüzel kişiyi,
- **Kişisel Veri**: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

- **Özel Nitelikli (Hassas) 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,
- **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 işlemi,
- **Kişisel Veri İşleme Envanteri:** Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,
- **Kişisel Verilerin Korunması ve İşlenmesi Politikası:** Kişisel veri işleme süreçlerinde SICK tarafından uygulanacak usul ve esasları, alınan teknik ve idari tedbirleri ihtiva eden politikayı,
- **Kişisel Veri Saklama ve İmha Politikası:** Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı,
- **Kurul:** Kişisel Verileri Koruma Kurulunu
- **Kurum:** Kişisel Verileri Koruma Kurumunu,
- **Periyodik İmha:** Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini,
- **Sicil (VERBİS):** Kişisel Verileri Koruma Kurumu tarafından tutulan veri sorumluları sicil bilgi sistemini,
- **Stajyer:** Uygulamalı meslek eğitimi alma amacıyla çalışan kişiyi,
- **Veri İşleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi
- **Veri Kayıt Sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,
- **Veri Sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,
- **Yönetmelik:** 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği ifade eder.

Bu Politika'da yer almayan tanımlar için **6698 sayılı Kanun** ve ilgili mevzuatta yer alan tanımlar geçerlidir.

5. KAYIT ORTAMLARI

SICK tarafından kişisel verilerin bulundurulduğu kayıt ortamları; SICK adına/tarafından kullanılan sunucular, yazılımlar, bilgi güvenliği aygıtları (güvenlik duvarı, antivirüs, periyodik kayıt dosyaları vs.) kişisel bilgisayarlar, mobil cihazlar (akıllı tabletler, akıllı telefonlar) kullanılan elektronik programlar, iletişim altyapıları, MSSQL Sistemleri, Back Up yazılımları, aktarım programları ve sunucuları, VPN sunucusu dataları, ağ üzerinde veri saklaması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri, USB, harici disk, hafıza kartı gibi veri depolama özelliğine sahip diğer taşıyıcılar, yazıcı ve tarayıcılar, kağıt, birim dolapları, arşivdir.

SICK, sayılan kayıt ortamlarına ek olarak kullanabileceği diğer kayıt ortamlarını da gecikmeksizin işbu İmha Politikası'na dahil edecektir.

6. SORUMLULUK VE GÖREV DAĞILIMLARI

SICK tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir. Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir. İşbu tabloda yer alan kişiler SICK Kişisel Verilerin Korunması Komisyonu üyelerini ihtiva etmektedir.

SICK KİŞİSEL VERİLERİN KORUNMASI KOMİSYONU		
UNVAN	**BİRİM**	**GÖREV**
İnsan Kaynakları Uzmanı	İnsan Kaynakları Departmanı	Çalışanların İmha Politikası ve Kişisel Verilerin Korunması ve İşlenmesi Politikası'na uygun hareket etmesinden sorumludur.
Bilgi Güvenliği Müdürü	Bilgi İşlem Departmanı	İmha Politikası ve Kişisel Verilerin Korunması ve İşlenmesi Politikası'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

7. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLER

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, Şirketimiz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanmaktadır.

a. Saklamayı Gerektiren Hukuki Sebepler

İlgili kişisel veriler, SICK tarafından, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu çerçevede kişisel veriler:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 4982 Sayılı Bilgi Edinme Hakkı Kanunu,
- 4857 sayılı İş Kanunu,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun ve bu kanunlara ilişkin ikincil mevzuat, kapsamında öngörülmüş olan saklama sürelerine uygun biçimde veriler saklanmaktadır.

b. Saklamayı Gerektiren İşleme Amaçları

- SICK insan kaynakları operasyonlarının planlanması ve yürütülebilmesi,
- Bilgi güvenliği faaliyetlerinin planlanması, yürütülebilmesi, denetimi,
- Kurumsal iletişimin sağlanabilmesi,
- Eğitim çalışmalarının gerçekleştirilmesi,
- Denetim faaliyetlerinin gerçekleştirilebilmesi,
- Acil durum süreçlerinin yürütülebilmesi,
- Çalışanlar için iş akdi ve mevzuat kaynaklı yükümlülüklerin yerine getirilebilmesi,
- Stratejik planlama ve yönetim faaliyetlerinin yürütülebilmesi,
- Yasal ve sözleşmesel yükümlülüklerin yerine getirilebilmesi,
- SICK'in, her türlü operasyonel faaliyetinin güvenliğinin sağlanabilmesi,
- İlerde doğabilecek hukuki ihtilaflarda ispat yükümlülüğünün yerine getirilebilmesi,
- Başvuru ve şikayet süreçlerinin yönetilebilmesi,
- Kişisel verilerin doğruluğunun ve güncelliğinin sağlanabilmesi,
- SICK'in iş süreçlerine ilişkin stratejilerin belirlenmesi ve tatbik edilmesi,
- Ücret yönetimi, yan hak ve menfaatlere ilişkin süreçlerin yönetilebilmesi,
- SICK ticari faaliyetleri kapsamında iş sürekliliğinin sağlanması, sözleşme süreçlerinin yönetilmesi,
- Hukuk işlerinin denetimi ve takibi,
- Yetkili kurum ve kuruluşlara ilgili yasal düzenleme dolayısıyla bilgi verilmesi,

- Tedarikçiler, iş ortakları, hizmet sağlayıcılar ile olan iş süreçlerinin yürütülebilmesi ve bu kişilerle iletişimin sağlanabilmesi.

hallerinden biri veya birkaçının bulunması halinde kişisel verilerinizi işleyebilecektir. Kişisel verilerin işlenmesine ilişkin detaylı bilgiye ulaşmak için http://www.sick.com/tr adresinde yer alan Kişisel Verilerin Korunması ve İşlenmesi Politikasını inceleyebilirsiniz.

c. İmha Nedenleri

SICK bünyesinde bulunan kişisel veriler ilgili kişinin talebi halinde ya da Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenlerin ortadan kalkması halinde resen işbu imha politikası uyarınca silinir, yok edilir veya anonim hale getirilir.

Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenler aşağıdakilerden ibarettir:

1. Kanunlarda açıkça öngörülmesi.
2. Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
3. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
4. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
5. İlgili kişinin kendisi tarafından alenileştirilmiş olması.
6. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
7. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

İlgili kişilerin kişisel verileri, yukarıda sayılmış olan kişisel veri işleme nedenlerinin ortadan kalkması, işlemeye esas teşkil eden mevzuatın değişmesi veya mülga hale gelmesi, 6698 sayılı KVKK m.11 uyarınca ilgili kişinin kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun SICK tarafından kabul edilmesi, SICK'in, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya 6698 sayılı KVKK'da öngörülen süre içinde cevaplamaması ihtimallerinde; ilgili kişinin Kurul'a şikayette bulunması ve bu talebin Kurul tarafından uygun görülmesi durumlarında gerçekleştirilecek ilk periyodik imha sırasında imha edilmektedir. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler tutanak ile kayıt altına alınır ve söz konusu kayıtlar imha tarihinden itibaren en az üç yıl süreyle saklanır.

8. KİŞİSEL VERİLERİN GÜVENLİĞİ

SICK, kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini sağlamaya yönelik gerekli her türlü teknik ve idari tedbirleri almaktadır.

Bu kapsamda öncelikle SICK tarafından işlenen kişisel verilerin neler olduğunun tespitine dair çalışmalar gerçekleştirilmiş ve işlenen kişisel verilerin özel nitelikli kişisel veri olup olmadığı da gözetilerek, bu verilerin korunmasına ilişkin ortaya çıkabilecek riskler belirlenerek, risklerin azaltılması veya ortadan kaldırılmasına yönelik gerekli teknik ve idari tedbirler uygulamaya konmuştur.

Kişisel verilerin hukuka, mevzuata ve ilgili güvenlik önlemlerine uygun şekilde işlenmesi, muhafaza edilmesi, saklanması, imha edilmesi ve sair süreçleri düzenleyen şirket içi politikalar ve prosedürler benimsenmiştir.

Kişisel veri güvenliğinin sağlanması için, kişisel verilerin hukuka aykırı şekilde açıklanması ve paylaşılmasının önüne geçebilmek ve KVKK'ya yönelik farkındalık yaratabilmek amacıyla, çalışanlara ve yöneticilere düzenli olarak eğitimler verilmektedir.

Ayrıca kişisel veri işleme süreçlerine dahil olan çalışanlardan, iş süreçlerinin bir parçası olarak gizlilik anlaşmaları, taahhütleri imzalamaları istenmekte, çalışanların güvenlik politika ve prosedürlerine aykırı hareket ettiklerinin tespiti halinde gerekli disiplin sürecine başvurulacağı önemle hatırlatılmaktadır.

SICK ile çalışan, tedarikçi, iş ortağı, müşteri vs. arasında yapılan sözleşmeler ile veri işleyenler ile SICK arasında yapılan sözleşmeler incelenmiş ve bu kapsamda başta KVKK ve sair mevzuat kapsamında revize çalışmaları yapılmış ve ek protokoller hazırlanmıştır.

Şirket tarafından veri işleme süreçlerine dahil olan kişisel verilere personel bazında erişim, yetki sınırlandırması yapılmış, sınırlı sayıda personele yetki süreleri tam olarak tanımlanarak yürüttükleri iş süreçleri ile ilgili olan kişisel verilere erişim yetkisi tanınmıştır. Personel tarafından gerçekleştirilen veri işleme faaliyetleri kayıt altına alınmaktadır. Görev değişikliği veya işten ayrılan personellerin ivedilikle bu alandaki yetkileri kaldırılmaktadır.

Kişisel verilerin hukuka aykırı şekilde işlenmesinin ve kişisel verilere hukuka aykırı şekilde erişilmesinin önüne geçmek için, kişisel verilerin işlenmesine ilişkin süreçlerin takibi ve denetimi için teknik sistemler kurulmuştur. Ağ güvenliği, veri akışı güvenliği çalışmaları yapılmış, veri kaybının önlenmesi için hali hazırdaki yazılımlar güncellenmiştir. Kişisel verilerin hukuka aykırı şekilde işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek için iç denetimler gerçekleştirilmiştir.

Şirketimiz, kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, verilere hukuka aykırı olarak erişilmesinin önlenmesi ve verilerin muhafazasını sağlamaya yönelik farkındalığın artırılması için iş ortaklarına gerekli bilgilendirmeler yapmaktadır. İş ortaklarıyla, tedarikçilerle, müşterilerle Şirketimiz arasında imzalanan sözleşme, protokol ve gizlilik anlaşmalarında KVK mevzuatı kapsamında gerekli olan uyarılara ve ikazlara atıf yapılmakta kişisel veri aktarımları karşılıklı taahhütler ile güvence altına alınmaktadır. Kişisel verilere erişime ve işlemeye yetkili olan kullanıcılar, bilgi sistemlerinin ve ağlarının güvenliğinin gerekliliği ve güvenliği artırmak için neler yapabilecekleri konularında sürekli eğitilmekte ve bilinçli olmaları sağlanmaktadır.

Tüm kullanıcılar kullandıkları bilgi sistemleri bileşenlerinin ve kişisel verilerin güvenliğinden ortak sorumlu olduğunun bilincindedir.

Sistem güvenlik boşlukları takip edilerek uygun güvenlik düzeyinin sağlanabilmesi için yamalar yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.

SICK nezdinde bulunan kişisel verilere ilişkin çalışmaların akabinde tespit edilen kişisel veriler analiz edilmiş, mevzuat kapsamında incelenmiştir. Bu çerçevede gereksiz olan veriler silinmiş, verilerin mümkün olduğunca azaltılması ilkesi benimsenmiştir.

Kişisel verilere hukuka aykırı şekilde erişilmesini engellemek ve kişisel verilerin güvenli ortamlarda saklanmasını sağlamak için uygun güvenlik düzeyine sahip teknik yöntemler kullanılmakta ve söz konusu yöntemler gelişen teknolojiye uygun şekilde güncellenmektedir.

Şirketin veri kayıt sistemine herhangi bir saldırı olması halinde, bu durumun erken fark edilmesi ve erken müdahale edilebilmesi için bir sistem kurulmuş, bilişim ağlarında hangi yazılım ve servislerin çalıştığı ve bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığı düzenli şekilde kontrol edilmekte olup tüm kullanıcıların işlem hareketleri düzenli olarak tutulmaktadır.

Kişisel verilerin hukuka aykırı olarak başkaları tarafından ele geçirilmesi durumunda bu hususun ilgili kişiye ve Kurula bildirilebilmesi için SICK tarafından buna uygun bir sistem ve altyapı kurulmuş, SICK nezdinde bir bildirim prosedürü benimsenmiştir.

Özel nitelikli kişisel veriler e-mail ortamında aktarılacaksa şifreli kurumsal e-mail hesabından veya KEP hesabı üzerinden aktarılmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN yöntemiyle veri aktarımı gerçekleştirilmektedir. Veri aktarımı fiziki olarak gerçekleşecekse evrakın çalınması, hasar görmesi, kaybolması ya da yetkisiz kişiler tarafından ele geçirilmesi gibi risklere karşı gerekli tedbirler alınmakta ve evrak dışarıdan okunamayacak şekilde, kapalı dosyalarda ve “gizli” formatta gönderilmektedir.

Çevresel risklere karşı bilgi ve bilişim sistemleri güvenliğinin sağlanması amacıyla sistem odasına sadece yetkili personelin girişinin sağlanması, kilit altındaki veri saklama birimlerinin anahtarlarının belirli kişilerde olması, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, antivirüs sistemleri vb. gibi birçok önlem alınmaktadır.

9. SAKLAMA VE İMHA SÜRELERİ

SICK 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 yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde SICK tarafından güncellemeler yapılır. Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi SICK Kişisel Verilerin Korunması Komisyonu tarafından yerine getirilir.

10. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

10.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbiri almaktadır.

Kişisel verilerin silinmesi sürecinde, silme işlemine konu teşkil edecek kişisel veri belirlenmekte, söz konusu kişisel veriye erişim yetkisi olan ilgili kullanıcılar ve kullanıcıların kişisel veri üzerindeki yetkileri tespit edilmekte ve ilgili kullanıcıların söz konusu kişisel veri kapsamındaki erişim, geri getirme, tekrar kullanma yetkileri kaldırılmaktadır.

Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmektedir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, geri dönülemeyecek ve teknolojik çözümlemelerle okunamayacak şekilde sabit mürekkep kullanılarak ya da kesilerek, ilgili kullanıcılar için görünemez hale getirilmesi işlemidir.

Kişisel verilerin bulunduğu veri tabanlarında, kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (*Delete vb*.) silinmekte, dosya işletim sisteminde bulunan kişisel veriler için, dosyanın işletim sistemindeki silme komutu ile kişisel verinin silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması ile silme işlemi yapılmaktadır.

10.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirket kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almaktadır.

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyalar tespit edilerek, verilerin bulunduğu sistemlerin türüne göre, manyetik medya bulunan veriler için, de-manyetize etme, optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi ya da bir metal öğütücüden geçirilmesi, kâğıt ortamında bulunan kişisel veriler için kâğıt ötücüden geçirilmesi yöntemlerinden uygun olanı kullanılmaktadır.

10.3 Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Anonim hale getirilmedeki amaç, veri ile bu verinin tanımlandığı kişi arasındaki bağın kopartılmasıdır. Kişisel verilerin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleşme, rastgele hale getirme gibi yöntemler anonim hale getirme yöntemlerinden bazılarıdır.

11. PERİYODİK İMHA SÜRELERİ

6698 sayılı KVKK m.7 gereğince, yasal mevzuata uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması veya mevzuatta öngörülen sürenin sona ermesi halinde kişisel veriler periyodik olarak imha edilir. Şirketimiz, 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 yılda iki kez olmak üzere 6 aylık zaman aralıkları ile gerçekleştirilir.

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