KONECTA TEKNOLOJİ VE MÜŞTERİ HİZMETLERİ A.Ş

SAKLAMA VE İMHA POLİTİKASI

Yayın Tarihi: 08.02.2018 Doküman No:POL.KSY.03
Revizyon Tarihi:12.01.2024 Revizyon No:05

1 KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASININ HAZIRLANMASININ AMACI VE İLKELER

Veri sorumlusu sıfatı ile KONECTA TEKNOLOJİ VE MÜŞTERİ HİZMETLERİ ANONİM ŞİRKETİ ("ŞİRKET") tarafından elde edilmiş olan kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla, başta 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") ve diğer ilgili mevzuatlar uyarınca işbu Kişisel Veri Saklama ve İmha Politikası ("Politika") hazırlanmıştır.

ŞİRKET ile ilgili kanun ve mevzuatlar kapsamında, Şirket çalışanları, çalışan adayları, çalışan yakınları, şirket ortakları, topluluk şirketleri çalışanları, mevcut ve muhtemel müşterileri, müşterinin müşterisi, hizmet sağlayıcıları, tedarikçi, müşteri ve hizmet alınan şirketlerin çalışanları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin işlenmesine, saklanmasına, imhasına ve ilgili kişilerin haklarını etkin bir şekilde kullanmasına önem vermektedir. Bu doğrultuda Şirket olarak, sözü edilen iş ve işlemlerin yerine getirilmesi ve ilgili kişinin haklarının korunması ve kullanılmasına yönelik olarak mümkün olan tüm idari ve teknik tedbirleri almaktadır. Bununla birlikte ŞİRKET tüm süreçlerinde Kanun'da açıkca belirtilmiş olan kişisel verilerin işlenmesini sağlamaktadır;

- hukuka ve dürüstlük kurallarına uygun olması,
- doğru ve gerektiğinde güncel olması,
- belirli, açık ve meşru amaçlar için işlenmesi,
- işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması,
- ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi,
- ilkelerine uygun olarak faaliyetlerini yürütmektedir.

2 POLİTİKANIN KAPSAMI

ŞİRKET'in sahip olduğu veya ŞİRKET tarafından yönetilen kişisel verilerin otomatik yöntemlerle veya otomatik olmayan yollarla işlendiği tüm kayıt ortamları ve kişisel verilerin işlenmesine yönelik tüm faaliyet ve süreçlerde bu Politika uygulanır.

Bu kapsamda ŞİRKET çalışanları, çalışan adayları, çalışan yakınları, şirket ortakları, topluluk şirketleri, mevcut ve muhtemel müşterileri, müşterinin müşterisi, hizmet sağlayıcıları, tedarikçi, müşteri ve hizmet alınan şirketlerin çalışanları, ziyaretçileri ve diğer üçüncü kişilere ait kişisel verilerin işlenmesi ve ilgili süreçlerle alakalı olarak alınan idari ve teknik tedbirler bu Politika'nın konusudur.

ŞİRKET, bir başkası namına Veri İşleyen olarak kişisel veri işlediği durumlarda bu Politika'da yer alan düzenlemelere ve varsa, söz konusu üçüncü kişi ile imzalanan her türden sözleşmedeki, Politika'ya aykırı olmayan, talimatlara uyar.

3 TANIMLAR

Alıcı Grubu: Veri Sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirmeye 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: KONECTA TEKNOLOJİ VE MÜŞTERİ HİZMETLERİ A.Ş personeli.

İlgili Kişi: Kişisel verisi işlenen gerçek kişi.

İlgili Kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler.

Kanun: 07.04.2016 tarih ve 29677 sayılı Resmi Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu.

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 ortam.

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

Kişisel Veri İşleme Envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.

Kişisel Verileri Koruma Komitesi: Kişisel Verileri Koruma Kanunu'na, Kurul kararlarına ve ilgili mevzuat hükümlerine uyum sağlanmasını, düzenlenen politika ve prosedürlerin uygulanmasını ve gerekli denetimlerin gerçekleştirilmesini sağlamakla yükümlü olan ŞİRKET bünyesinde oluşturulan komite.

- hukuka ve dürüstlük kurallarına uygun olması,
- doğru ve gerektiğinde güncel olması,
- belirli, açık ve meşru amaçlar için işlenmesi,
- işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması,
- ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi,

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, güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler.

Periyodik İmha: Kanun'da yer alan kişisel verileri işlenme şartlarının tamamının ortadan kalkması durumunda Kişisel Verileri Saklama ve İmha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek, silme, yok etme veya anonim hale getirme işlemi.

Politika: https://www.konecta.com/ adresinden ulaşılabilecek, KONECTA TEKNOLOJİ VE MÜŞTERİ HİZMETLERİ A.Ş sorumluluğunda bulunan kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen işbu Kişisel Verileri Saklama ve İmha Politikası.

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

Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlusu gerçek veya tüzel kişidir.

Veri Sorumluları Sicil Bilgi Sistemi (VERBİS): Veri sorumlularının sicile başvuruda ve sicile ilişkin ilgili diğer işlemlerde kullanacakları internet üzerinden erişilebilen, Kişisel Veri Yönetimi Dairesi Başkanlığı tarafından oluşturulan ve yönetilen bilişim sistemidir.

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

4 SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

ŞİRKET; çalışanları, çalışan adayları, çalışan yakınları, şirket ortakları, topluluk şirketleri çalışanları, mevcut ve muhtemel müşterileri, müşterinin müşterisi, hizmet sağlayıcıları, tedarikçi, müşteri ve hizmet alınan şirketlerin çalışanları, ziyaretçileri ve diğer üçüncü kişilere ait kişisel verileri Kanun'a ve ilgili mevzuat ve yönetmeliklerine uygun olarak saklar ve imha eder.

Başta tabi olduğumuz Kanun ve ilgili mevzuatları ve Politika kapsamında ŞİRKET tarafından yürütülen kişisel verilerin saklanması ve imhasına yönelik yürütülen faaliyetlere ilişkin açıklamalara aşağıda sırasıyla yer verilmiştir.

4.1 SAKLAMAYA İLİŞKİN AÇIKLAMALAR

Kanun'un 3. maddesinde ***"kişisel verilerin işlenmesi"*** kavramı tanımlanmış, 4. 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. maddelerde ise ***"kişisel verilerin işleme şartları"*** söylenmiştir.

Buna göre, kişisel veriler, Şirket'in iş faaliyetleri çerçevesinde ilgili mevzuatta öngörülen veya işleme amaçlarına ve işbu Politika'nın 9. Maddesine uygun süre kadar saklanır.

4.1.1 Saklamayı Gerektiren Hukuki Sebepler

ŞİRKET faaliyetleri çerçevesinde işlenen kişisel veriler, aşağıda belirtilen, bunlarla sınırlı kalmamak üzere, ilgili mevzuatlarda öngörülen süre kadar muhafaza edilir.

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 5237 Sayılı Türk Ceza 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,
- 213 Sayılı Vergi Usul Kanunu ve ilgili mevzuat
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4857 sayılı İş Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu
- 5411 sayılı Bankacılık Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

4.1.2 Saklamayı Gerektiren İşleme Amaçları

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

- ✔ Acil Durum Yönetimi Süreçlerinin Yürütülmesi,
- ✔ Bilgi Güvenliği Süreçlerinin Yürütülmesi,
- ✔ Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi,
- ✔ Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi,
- ✔ Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi,
- ✔ Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi,
- ✔ Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi,
- ✔ Denetim / Etik Faaliyetlerinin Yürütülmesi,
- ✔ Eğitim Faaliyetlerinin Yürütülmesi,
- ✔ Erişim Yetkilerinin Yürütülmesi,
- ✔ Faaliyetlerin Mevzuata Uygun Yürütülmesi,
- ✔ Finans Ve Muhasebe İşlerinin Yürütülmesi,
- ✔ Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi,
- ✔ Fiziksel Mekan Güvenliğinin Temini,
- ✔ Görevlendirme Süreçlerinin Yürütülmesi,
- ✔ Hukuk İşlerinin Takibi Ve Yürütülmesi,
- ✔ İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi,
- ✔ İletişim Faaliyetlerinin Yürütülmesi,
- ✔ İnsan Kaynakları Süreçlerinin Planlanması,
- ✔ İş Faaliyetlerinin Yürütülmesi / Denetimi,
- ✔ İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi,
- ✔ İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi,
- ✔ İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi,
- ✔ Lojistik Faaliyetlerinin Yürütülmesi,
- ✔ Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi,
- ✔ Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi,
- ✔ Mal / Hizmet Satış Süreçlerinin Yürütülmesi,
- ✔ Mal / Hizmet Üretim Ve Operasyon Süreçlerinin Yürütülmesi,
- ✔ Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi,
- ✔ Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi,
- ✔ Organizasyon Ve Etkinlik Yönetimi,
- ✔ Performans Değerlendirme Süreçlerinin Yürütülmesi,
- ✔ Risk Yönetimi Süreçlerinin Yürütülmesi,
- ✔ Saklama Ve Arşiv Faaliyetlerinin Yürütülmesi,
- ✔ Sözleşme Süreçlerinin Yürütülmesi,
- ✔ Talep / Şikayetlerin Takibi,
- ✔ Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi,
- ✔ Ücret Politikasının Yürütülmesi,
- ✔ Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi,

- ✔ Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi,
- ✔ Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi,
- ✔ Veri Sorumlusu Operasyonlarının Güvenliğinin Temini,
- ✔ Yönetim Faaliyetlerinin Yürütülmesi,
- ✔ Ziyaretçi Kayıtlarının Oluşturulması ve Takibi.

4.2 İMHAYI GEREKTİREN SEBEPLER VE AÇIKLAMALAR

ŞİRKET bünyesinde bulunan kişisel veriler ilgili kişinin talebi halinde ya da Kanun'un 5. Ve 6. Maddelerinde sayılan nedenlerin ortadan kalkması halinde re'sen işbu Politika uyarınca silinir, yok edilir veya anonim hale getirilir. Aynı zamanda kişisel veriler;

- ✔ İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- ✔ İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- ✔ Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- ✔ Kanunun 11. Maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurul tarafından kabul edilmesi,
- ✔ Kurulun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- ✔ Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması

durumlarında, Şirket tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

5 KAYIT ORTAMLARI

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, kayıt ortamı kapsamına girmektedir.

ŞİRKET bünyesinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklere uygun bir kayıt ortamında tutulur. ŞİRKET, veri sorumlusu olarak, kişisel

verileri Kanun'a, ilgili mevzuatlarına ve bu yönde hazırlanmış olan Politika ve prosedürlerine uygun olarak işlemekte ve korumaktadır.

Bu kapsamda kişisel veriler aşağıda belirtilen ortamlarda saklanmaktadır.

- Elektronik Ortamlar
  - Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.)
  - Yazılımlar (CRM, Salesforce gibi kurumsal yazılımlar)
  - Bilgi güvenliği yazılımları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)
  - Bulut Sistemleri (Office 365, Google)
  - Kamera Kayıt Sistemleri
  - Çıkartılabilir Bellekler (USB, Hafıza kartı vb.)
  - Optik Diskler (CD, DVD)
  - Mobil Cihazlar (Akıllı telefon, tablet vb.)
  - Yazıcı, tarayıcı vb. ağ cihazları

- Elektronik Olmayan Ortamlar
  - Basılı Evrak (Standart form, sözleşme, yazışmalar ile ihtiyaca binaen oluşturulan her tür yazılı belge, doküman, arşiv)
  - Manuel veri kayıt sistemleri (anket formları, müşteri şikâyet formları, iş başvuru form ve evrakları, raporlar ve sair yazılar)
  - Yazılı, basılı, görsel ortamlar

6 KİŞİSEL VERİLERİN SİLİNMESİ VE İMHASINA İLİŞKİN AÇIKLAMALAR

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin yok edilmesi ise, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

ŞİRKET, kişisel verileri, başta kanunlar ve ilgili mevzuatlarında öngörülen ve Politika'nın 9. Maddesinde belirtilen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda veya saklanma amaçlarının ortadan kalkması durumunda re'sen veya ilgili kişinin başvurusu üzerine yine ilgili kanunlar ve mevzuat hükümlerine uygun olarak aşağıda belirtilen yöntemlerle siler ve imha eder.

6.1 KİŞİSEL VERİLERİN SİLİNMESİ

Sunucularda Yer Alan Kişisel Veriler: Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.

Elektronik Ortamda Yer Alan Kişisel Veriler: Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

Fiziksel Ortamda Yer Alan Kişisel Veriler: Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.

Bulut Ortamlarında Yer Alan Kişisel Veriler: Bulut ortamlarında yer alan kişisel verilere erişim şifreli olarak sağlanmaktadır. Bulut sistemindeki veriler silme komutu ile silinir ve bu ortamlarda yer alan kişisel verilere ilgili kullanıcıların erişim ve geri getirme yetkileri ortadan kaldırılır.

Taşınabilir Medyada Yer Alan Kişisel Veriler: 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.

6.2 KİŞİSEL VERİLERİN İMHASI

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.

Elektronik Ortamda Yer Alan Kişisel Veriler: Ağ cihazları (router, switch vb.), flash tabanlı sabit diskler (ATA, SCSI vb.) ve akıllı telefonlar vb. ortamlarda yer alan kişisel veriler, fiziksel yok etme (Optik veya manyetik medyanın eritilmesi, yakılması, parçalanması veya toz haline getirilmesi işlemidir) veya üzerine yazma (Optik veya manyetik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir) tekniklerinden uygun olanı ile imha edilir.

Bulut Ortamında Yer Alan Kişisel Veriler: Bulut ortamlarındaki kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan herbir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

6.3 KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

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

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

ŞİRKET olarak, gerekli hallerde, aşağıda belirtilen yöntemler ile kişisel verilerin anonimleştirilmesini sağlamaktayız.

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

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

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

Veri değiş tokuşu: Bu yöntemde 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 ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir.

7 KİŞİSEL VERİLERE YÖNELİK ALINAN İDARİ VE TEKNİK TEDBİRLER

Kişisel verileri güvenli olarak Kanun'a ve ilgili mevzuatlarına uygun bir şekilde saklamak ve hukuka aykırı işlenmesini ve erişilmesini önlemek için ŞİRKET olarak aldığımız idari ve teknik tedbirler, sayılanlarla sınırlı olmamak üzere, aşağıda belirtilmiştir.

7.1 TEKNİK TEDBİRLER

- ✔ Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- ✔ Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- ✔ Bilgi teknolojileri sistemleri tedarik, gelistirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- ✔ Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

- ✔ Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- ✔ Çalışanlar için yetki matrisi oluşturulmuştur.
- ✔ Erişim logları düzenli olarak tutulmaktadır.
- ✔ Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- ✔ Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- ✔ Gizlilik taahhütnameleri yapılmaktadır.
- ✔ Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- ✔ Güncel anti-virüs sistemleri kullanılmaktadır.
- ✔ Güvenlik duvarları kullanılmaktadır.
- ✔ İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- ✔ Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- ✔ Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- ✔ Kişisel veri güvenliğinin takibi yapılmaktadır.
- ✔ Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- ✔ Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- ✔ Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- ✔ Kişisel veriler mümkün olduğunca azaltılmaktadır.
- ✔ Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- ✔ Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- ✔ Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- ✔ Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- ✔ Mevcut risk ve tehditler belirlenmiştir.
- ✔ Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- ✔ Sızma testi düzenli olarak uygulanmaktadır.
- ✔ Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- ✔ Şifreleme yapılmaktadır.
- ✔ Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
- ✔ Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- ✔ Veri kaybı önleme yazılımları kullanılmaktadır.
- ✔ 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 testleri düzenli olarak yapılmakta/yaptırılmakta ve test sonuçları kayıt altına alınmaktadır.

- ✔ Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- ✔ Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak Şirket e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.

7.2 İDARİ TEDBİRLER

- ✔ Kişisel verilerin güvenliğine ilişkin mevcut risk ve tehditler ŞİRKET tarafından belirlenmekte ve söz konusu risk ve tehditlerin azaltılması veya ortadan kaldırılmasına yönelik olarak çözüm planlamaları yapılmaktadır. Buna ek olarak olası bir güvenlik ihlali durumunda olay yönetimi prosedürü mevcuttur.
- ✔ Kişisel verilere fiziksel ve elektronik ortamlarda ŞİRKET içerisinde erişim iş tanımı gereği erişmesi gereken personel ile sınırlandırılmaktadır.
- ✔ Kişisel verilerin saklandığı arşiv ve depolar mevzuata uygun ve gerekli güvenlik önlemleri alınmış durumdadır. Depolarda veriler kilitli dolaplarda saklanmakta olup depolar ayrıca kilitlenmektedir ve bu depolara erişim yetkileri sınırlandırılmıştır. Depolar güvenlik amacıyla kamera ile 24 saat izlenmektedir ve yangın, sel gibi doğal afetlere karşı gerekli önlemler ŞİRKET tarafından alınmaktadır.
- ✔ ŞİRKET bünyesinde tutulan kişisel veriler doğru ve güncel durumda, işlendikleri amaç için gerekli olan süre kadar muhafaza edilmektedir.
- ✔ Kişisel verilerin paylaşılması hususunda ise ŞİRKET tarafından kişisel verilerin paylaşıldığı üçüncü kişilerce kişisel verilerin korunması ve veri güvenliğine ilişkin olarak Gizlilik ve Veri Koruma Taahhüdü imzalanmakta ve/veya bu kişilerle yapılan sözleşmelere kişisel verilerin korunmasına ilişkin bir hüküm eklenerek veri güvenliği sağlanmaktadır.
- ✔ Çalışanlar, kişisel verilerin hukuka uygun olarak saklanması, işlenmesi konusunda bilgilendirilmekte ve çalışanlara bu hususlarda eğitim ve farkındalık çalışmaları sunulmaktadır.
- ✔ Çalışanlar öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak üçüncü kişilere açıklayamayacakları, işleme amacı dışında kullanamayacakları ve bu yükümlülüklerinin görevden ayrılmalarından sonra da devam edeceği konusunda bilgilendirilmekte ve bu doğrultuda iş sözleşmeleriyle ve/veya çalışanlara ilişkin hazırlanan aydınlatma ve rıza metni ile kendilerinden gerekli taahhütler alınmaktadır.

- ✔ ISO 9001 ve 27001 gibi yönetim sistemleri ŞİRKET kapsamında aktif olarak uygulanmakta olup iç ve dış denetimler periyodik olarak yapılmakta ve yaptırılmaktadır.

8 SORUMLULUK VE GÖREV DAĞILIMLARI

İş yeri işleyişinin başta Kanun ve ilgili mevzuatlara uyumunun sağlanması ve iş birimlerinin bünyesinde bulunan kişisel verilerin Politika'ya uygun olarak işlenmesinin sağlanması ve ilgili süreçlerin denetimi amacıyla Şirketimiz bünyesinde Kişisel Verileri Koruma Komitesi ("***Komite***") oluşturulmuştur. ŞİRKET'in tüm departmanları ve çalışanları, Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, çalışanların 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 ŞİRKET adına başka bir gerçek veya tüzel kişi tarafından işlenmesi durumunda, Şirket ve veri işleyen taraflar, veri güvenliğine yönelik önlemlerin alınması ve uygulanması hususunda yetkili merciilere ve kişisel verisi işlenen ilgili kişilere karşı, Kanun ve ilgili mevzuatlar çerçevesinde, müştereken sorumludurlar.

ŞİRKET bünyesinde oluşturulmuş olan Komite'nin detayları aşağıdaki tabloda belirtilmiştir.

UNVAN	DEPARTMAN	GÖREV TANIMI
Hukuk Müşaviri	Hukuk	Komitenin periyodik olarak toplanması, kişisel veri politikaların uygulanması ve yürütülmesi, Komite üyeleri ile koordinasyonun sağlanması ve süreçlere ilişkin Yönetim Kurulunun bilgilendirilmesi, Kişisel Verilerin Korunması Kurulu ile ilişkilerin takibi, Kurul kararlarının takibi, uygulanması ve süreçlerin yönetimi, Şirketin Kişisel Verilerin Korunması Kurulu nezdindeki temsilinden sorumludur.
İnsan Kaynakları Müdürü	İnsan Kaynakları	Şirket insan kaynakları işlemlerinin yürütülmesi esnasında kişisel verilerin Kanun ile uyumlu bir biçimde işlenmesinin, imha edilmesinin ve anonimleştirilmesinin sağlanması ve bu işlemlere ilişkin gerekli adımların

		atılması ve Komite'nin bu konularda bilgilendirilmesinden sorumludur.
IT Bölüm Müdürü/Bilgi Güvenliği Uzmanı	Bilgi Teknolojileri	Kanun ve ilgili mevzuatları uyarınca, kişisel verilerin işlenmesi, saklanması, imha edilmesi ve anonimleştirilmesi için gerekli bilgi teknolojileri sistemlerinin tesis edilmesi ve çalışır durumda olmasının sağlanması, kişisel verilerin yurt içinde ve yurt dışına aktarılması için gerekli teknik mekanizmaların oluşturulması, veri güvenliğinin sağlanması,veri güvenliği sağlayan sistemlerin önerilmesi ve bu sistemlerin uygulanması ve Komite'nin bu konularda bilgilendirilmesinden sorumludur.
Satış ve Müşteri Deneyimi Direktörü	Satış ve Müşteri Deneyimi	Şirket çağrı merkezi ve dış kaynak hizmeti tedariki esnasında kişisel verilerin Kanun ile uyumlu bir biçimde işlenmesinin, imha edilmesinin ve anonimleştirilmesinin sağlanması ve bu işlemlere ilişkin gerekli adımların atılması ve Komite'nin bu konularda bilgilendirilmesinden sorumludur.
Satış ve Müşteri Deneyimi Kıdemli Müdürü	Satış ve Müşteri Deneyimi	Şirket müşterilerine hizmet verilmesi faaliyetlerinin yürütülmesi esnasında kişisel verilerin Kanun ile uyumlu bir biçimde işlenmesinin, imha edilmesinin ve anonimleştirilmesinin sağlanması ve bu işlemlere ilişkin gerekli adımların atılması ve Komite'nin bu konularda bilgilendirilmesinden sorumludur.
İdari İşler, Satın Alma, Kalite ve Süreç Yönetimi Direktörü	İdari İşler, Satın Alma, Kalite ve Süreç Yönetimi	İdari İşlere ilişkin süreçlerin saklama sürelerine uygunluğunu sağlamak ve periyodik imha süresi uyarınca imha sürecini yönetmekle sorumludur.
Kalite ve Süreç Yönetimi Müdürü	İdari İşler, Satın Alma, Kalite ve Süreç Yönetimi	Kalite ve Süreç Yönetimi faaliyetlerinin yürütülmesi esnasında kişisel verilerin Kanun ile uyumlu bir biçimde işlenmesinin, imha edilmesinin ve anonimleştirilmesinin sağlanması ve bu işlemlere ilişkin gerekli adımların atılması ve Komite'nin bu konularda bilgilendirilmesinden sorumludur.

Kıdemli Lokasyon Müdürü	Operasyon Yönetimi	Lokasyon bazlı tüm faaliyetlerin yürütülmesi esnasında kişisel verilerin Kanun ile uyumlu bir biçimde işlenmesinin, imha edilmesinin ve anonimleştirilmesinin sağlanması ve bu işlemlere ilişkin gerekli adımların atılması ve departmanın sorumluluğunda olan süreçlerde işlenen kişisel verilerin saklama sürelerine uygunluğunu sağlamak ve periyodik imha süresi uyarınca imha sürecini yönetmek ve Komite'nin bu konularda bilgilendirilmesinden sorumludur.
Muhasebe ve Hazine Kıdemli Müdürü	Finans	Departmanın sorumluluğunda olan süreçlerde işlenen kişisel verilerin saklama sürelerine uygunluğunu sağlamak ve periyodik imha süresi uyarınca imha sürecini yönetmekle sorumludur.

9 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 Kişisel Veri Saklama ve İmha Politikası'nda

yer alır.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Sözleşmelerin hazırlanması	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kurumsal İletişim Faaliyetlerinin Yürütülmesi	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Bilgi İşlem Kayıtlarının Tutulması	Sisteme giriş tarihinden itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Ziyaretçi ve Toplantı Katılımcılarına Yönelik Faaliyetler	Ziyaretin/Etkinliğin sona ermesini takiben .... ay/yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuki İşlemler	Muhaberattan çıkış tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Operasyonel Ses Kayıtlarının Tutulması	Müşteri sözleşmesine göre değişecek şekilde en fazla 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sağlık Kayıtlarının Tutulması	İstihdam süresinin bitiminden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Muhasebe ve Finansal İşlemler	Ticari ilişkinin/faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Fiziksel Mekan Güvenliği Faaliyetleri	3 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Uzaktan Çalışmaya Fiziksel Mekan Güvenliği Faaliyetleri	Müşteri sözleşmelerine bağlı olarak en fazla 3 Ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri/Tedarikçi İşlemleri	Ticari ilişkinin/faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Potansiyel Müşteri/Tedarikçi İlişkileri Yürütülmesi	10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi İşlemleri	Silinmesi, imhası ve anonimleştirilmesinden itibaren 3 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Adayları, Stajyer Adayları ve Referanslara İlişkin Kayıtlar	Başvuru tarihinden sonra 3 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

9.1 PERİYODİK İMHA SÜRESİ

ŞİRKET, kanunlar ve ilgili mevzuatlarda belirtilen yükümlülüklere uygun olarak, kişisel verilerin imhasını gerektiren sebeplerin ortaya çıkmasını takiben ilk periyodik imha süresinde ilgili verileri siler, imha eder veya anonim hale getirir.Bu kapsamda Şirket, periyodik imha süresini 6 ay olarak belirlemiş olup, her yıl Aralık ve Haziran aylarında periyodik imha işlemini gerçekleştirir.

10 POLİTİKA'NIN YAYINLANMASI, SAKLANMASI VE GÜNCELLENMESİ

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır ve https://www.konecta-group.com/ İnternet adresinden kamuya açıklanır. Basılı kâğıt nüshası da Kalite Süreç departmanında saklanır.

Politika'nın, başta Şirketimizin tabii olduğu kanunlar ve ilgili mevzuatlarından gerçekleşebilecek düzenlemeler ve ŞİRKET'in faaliyetleri ve süreçlerinde yaşanabilecek değişiklikler doğrultusunda doğrultusunda, gerekli kısımları güncellenir. Güncellenen Politika Şirket'in https://www.konecta-group.com/internet adresinden ilan edilir.

11 POLİTİKA'NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

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