



Sertrans Holding A.Ş.

Kişisel Veri Saklama ve İmha Politikası

ÖNSÖZ

Sertrans Holding A.Ş., ("Şirket") Ömerli Mah. İstanbul Cad. No:260 Hadımköy,Arnavutköy-İstanbul adresinde mukim, 610265 Ticaret sicil numarası ile Büyükçekmece Vergi Dairesi'ne kayıtlı bir şirkettir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("**Kanun**") 16'ncı maddesi kapsamında Veri Sorumluları Sicili'ne ("**VERBİS**") kayıt yükümlülüğü bulunan veri sorumluları, hazırlamış oldukları kişisel veri işleme envanterlerine uygun olarak, işlenen verilerin saklanması ve imhasına ilişkin sürecin belirlenmesi adına saklama ve imha politikası oluşturmakla yükümlü kılınmıştır. Bu kapsamda Kanun çerçevesinde veri sorumlusu sıfatına haiz Şirket de uyum süreci çerçevesinde VERBİS'e kayıt yükümlülüğünü yerine getirmiş olmakla birlikte Kanun'dan doğan diğer yükümlülüklerini de eksiksiz yerine getirmek amacıyla kişisel veri işleme faaliyetlerinin tümünü hukuka uygun olarak yerine getirmeyi ve kişisel verilerin güvenliğini en yüksek düzeyde sağlamayı hedeflemektedir. İşbu Kişisel Verileri Saklama ve İmha Politikası ("**Politika**") Kanun ve 28.10.2017 tarihli 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("**Yönetmelik**") hükümleri doğrultusunda hazırlanmış olup Şirket içerisinde fiilen uygulanmakta olan mevcut yöntemlerde veya mevzuat düzenlemelerinde değişiklik olması halinde Politika üzerinde ilgili güncellemeler yapılmaktadır.

1. AMAÇ, KAPSAM VE KULLANICILAR

Şirket, hukuki ve sosyal sorumluluğunun bir parçası olarak öncelikle Kanun'dan doğan yükümlülüklerini yerine getirmek amacıyla gerekli tüm çalışmaları yapmakta ve veri işleme faaliyetlerini mevzuat hükümleri çerçevesinde gerçekleştirmektedir. Bu doğrultuda Yönetmelik'in 5'inci ve 6'ncı maddeleri kapsamında kişisel verilerin saklanması ve imhasına ilişkin yükümlülüklerin ve Yönetmelik'te belirtilen sair yükümlülüklerin yerine getirilmesi ve kişisel veri koruma, işleme ve imha düzenlemelerine ilişkin bu mevzuata dayanılarak çıkarılan Yönetmelik/Tebliğlere uymayı da taahhüt etmektedir.

İşbu Politika, yürürlükteki mevzuat çerçevesinde kişisel veri korumasının sağlanması ve Kanun ile diğer ilgili mevzuat kapsamında kişisel verilerin ve özel nitelikli kişisel verilerin saklanma sürelerine riayet edilerek muhafaza edilmesi ve gerekli veri imha çalışmalarının yapılması için uygulanmakta olan çerçeve koşulları içermekte olup Şirket tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

İşbu Politika, Şirket nezdinde www.sertransholding.com alan adlı internet sitesi aracılığıyla söz konusu faaliyetleri gerçekleştirmek amacıyla elde edilen müşteri, müşteri adayı, tedarikçi, tedarikçi adayı ve ziyaretçi sıfatına haiz gerçek veya tüzel kişilere ait kişisel verileri kapsamaktadır.

Politika Kanun’da belirtildiği şekilde, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla verilerin işlendiği sistemlerde yer alan kişisel verileri ve özel nitelikli kişisel verileri içermektedir.

İstatistiki değerlendirmeler, anket çalışmaları veya çalışmalar için elde edilen veriler gibi anonim hale gelmiş, tanımlanamayan veri veya tüzel kişilere ilişkin veriler, Kanun’un 28 inci maddesi kapsamında kişisel veri olarak kabul edilmemektedir ve işbu Politika’ya tabi değildir.

İşbu Politika Kanun ve ilgili düzenlemeler doğrultusunda ve Şirket prosedürleri gereğince güncellenmekte olup, yapılan değişiklikler güncellenmenin KVK Kurulu tarafından kabul edilmesiyle birlikte yürürlüğe girecektir.

2. TANIMLAR

İşbu Politika’da yer alan hukuki ve teknik terimlerin tanımları aşağıdaki tabloda gösterilmiştir:

5651 sayılı Kanun	5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
6563 sayılı Kanun	6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
6098 sayılı Kanun	6098 sayılı Türk Borçlar Kanunu
6102 sayılı Kanun	6102 sayılı Türk Ticaret Kanunu
6502 sayılı Kanun	6502 sayılı Tüketicini Korunması Hakkında Kanun
6698 sayılı Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek ve/veya birleştirilerek dahi hiçbir suretle kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemi
Elektronik Ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar
Elektronik Olmayan Ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar
İlgili Kişi	Kişisel verisi işlenen gerçek kişi, veri sahibi
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
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 ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter

Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem
Kişisel Verilerin Silinmesi	Kişisel verilerin hiçbir surette tekrar erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hardware ve software (yani fiziki ve elektronik ortamda) hiçbir kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi. (Örneğin; bir CD veya flash diskin imha edilmesi, parçalanması veya yakılması, personel özlük dosyasının yakılması, yeniden kâğıt haline getirilmesi vs.)
KVKK/Kanun	7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete’de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
Özel Nitelikli Kişisel Veri	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri
Periyodik İmha	Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda tekrar eden aralıklarla re’ sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Politika	Kişisel Verileri Saklama ve İmha Politikası
Şirket/Şirket	Sertrans Holding Anonim Şirketi
Şirket KVK Birimi	Şirket nezdinde kurulmuş olan ve işbu Politika’nın yürütülmesinden ve takibinden sorumlu olan Kurul
Sicil/VERBİS	Veri Sorumluları Sicili
Silme	Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi
Veri İşleyen	Veri sorumlusunun vermiş olduğu yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişi
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri Sahibi/İlgili Kişi/İlgili Kişiler	Kişisel verisi işlenen gerçek kişi
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, (İşbu Politika içerisinde Şirket olarak ifade edilecektir.)
Yok Etme	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi
Yönetmelik	28 Ekim 2017 tarihli 30224 sayılı Resmî Gazete’ de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

3. SORUMLULUK VE GÖREV DAĞILIMLARI

Kanun, Yönetmelik ve Politika ile belirtilen verinin saklanması ve imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar, danışmanlar, iş ortakları ve sair surette Şirket nezdinde kişisel veri saklayan ve işleyen herkes sorumludur.

Her iş birimi kendi iş süreçlerinde ürettiği veriyi saklamak ve korumakla yükümlüdür; ancak üretilen verinin iş biriminin kontrolü ve yetkisi dışında sadece bilgi güvenliği sisteminde bulunması durumunda, söz konusu veri bilgi güvenliği sistemlerinden sorumlu birimler tarafından saklanacaktır. İş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına veya yasal düzenlemelere aykırı sonuçlar doğmasına neden olacak periyodik imhalar, ilgili kişisel verinin türü, içinde yer aldığı sistemler ve veri sahibi iş birimi dikkate alınarak kural olarak bilgi güvenliği sistemleri bölümlerince ve aşağıda görev dağılımları verilen KVK Kurulu tarafından yapılacaktır.

Verilerin fiziksel ortamlarda tutulması durumunda Şirket içerisinde ilgili departman tarafından periyodik imha sürelerine veya ilgili kişinin talebi dahilinde iletilecek veri imha süreçlerine bağlı kalınarak kişisel verilerin imhası sağlanacaktır. Şirket, her departman özelinde veri imha süreçleri ve işbu Politika'da belirtilen usul ve esaslar hakkında tüm çalışanlarını, iş ortaklarını veya sair Şirket nezdinde kişisel veri saklayan kişileri bilgilendirdiğini taahhüt etmektedir.

Tablo 1: Saklama ve imha süreçleri görev dağılımı

Personel	Unvan	Birim	Görev Tanımı
Akif Erdem KARATAŞ	Bilgi Teknolojileri Müdürü	Arge ve Bilgi Teknolojileri	Verilerin fiziksel ortamda toplanması, saklanması ve imha edilmesinin denetlenmesi
Ebru İNÇE	İnsan Kaynakları Müdür Yardımcısı	İnsan Kaynakları	Verilerin dijital ortamda toplanması, saklanması ve imha edilmesinin denetlenmesi
Meltem CÖMERT	Muhasebe Yöneticisi	Mali İşler	Verilerin dijital ortamda toplanması, saklanması ve imha edilmesi

4. DOKÜMAN İÇERİĞİ

4.1. Kayıt Ortamları

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. Bu kapsamda kişisel veriler, Şirket tarafından aşağıda sıralanan ortamlarda hukuka uygun olarak saklanmaktadır.

Tablo 2: Verilerin muhafaza edildiği kayıt ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Personel Bilgisayarları	Kağıt Ortamları
Sunucu Sistemleri	Manuel Veri Kayıt Sistemleri
Dijital Arşiv (İK Dijital Arşiv, Muhasebe Micro Program Yedekleri)	Arşiv (İnsan Kaynakları, Muhasebe)
PDKS Sistemleri	Kilitli Birim Dolapları

E-mail	Arşiv (İnsan Kaynakları, Muhasebe)
Bulut Bilişim Sistemleri	
Çıkarılabilir bellekler (USB, Hafıza Kartı vb.)	
Mobil Cihazlar (Telefon, Tablet vb.)	

4.2. Kişisel Verilerin Saklanması

4.2.1. Saklamaya İlişkin Açıklamalar

Kanunun 3'üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4'üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı, ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiştir. Buna ek olarak Kanun'un 5 ve 6'ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır. Şirket tarafından işlenmekte olan kişisel veriler, Kanun kapsamında oluşturulan envanter ve Kişisel Veri İşleme Politikası'nda detayları belirtildiği üzere çeşitli hukuki sebepler ile ve kanuni yükümlülükler gereğince belirlenen süreler kadar Şirket nezdinde saklanmaktadır.

4.2.2. Saklamayı Gerektiren Hukuki Sebepler

Şirket nezdinde gerçekleştirilen faaliyetler kapsamında işlenen kişisel veriler, işbu Politika ilgili maddelerinde belirtilen süreler kadar yukarıda açıklanan kayıt ortamlarında muhafaza edilmektedir.

Kişisel verilerin saklanmasına ilişkin dayanılabilecek hukuki sebepler aşağıdaki gibidir:

- Açık Rıza
- Fiili İmkansızlık Nedeni ile Açık Rıza Alınamaması
- Sözleşmenin Kurulması veya İfası İçin Veri İşlemenin Gerekli Olması
- Hukuki Yükümlülük
- Kanunlarda Açıkça Öngörülmesi
- Hakkın Tesisi, Kullanılması ve Korunması,
- Meşru Menfaat
- İlgili Kişi'nin Kendisi Tarafından Alenileştirilmesi

Tarafımızca kişisel verileri saklama süreçlerinde hukuki sebep olarak "kanunlarda öngörülme"ye dayanıldığı hallerde aşağıda yer alan kanunlar esas alınmıştır:

- 6698 sayılı Kişisel Verileri Koruma Kanunu
- 6098 sayılı Türk Borçlar Kanunu
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 6102 sayılı Türk Ticaret Kanunu
- İnternet Toplu Kullanım Sağlayıcıları Yönetmelik
- Ticari Defterlere İlişkin Tebliğ
- 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi

- 213 sayılı Vergi Usul Kanunu
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
- Posta Gönderilerine İlişkin Güvenlik Tedbirleri Usul ve Esasları

Bu kanunlar uyarınca ve yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.2.3. Saklamayı Gerektiren Veri İşleme Amaçları

Şirket tarafından işlenmekte olan kişisel veriler; aşağıdaki tabloda sayılan amaçlar dahilinde mevzuatlarda öngörülen süreler kadar Şirket nezdinde saklanmaktadır.

Veri Kategorisi/Özel Nitelikli Veri Kategorisi	Veri Türü	İşleme Amacı
Kimlik	Ad Soyad	• İnsan kaynakları süreçlerinin planlanması
	Anne Baba Adı	• Kurumsal iletişim faaliyetlerinin planlanması ve icrası
	Nüfus Cüzdanı Seri Sıra No	• Çalışan için gerekli olan kurumsal bildirimlerin sağlanması
	Cüzdanın Verildiği Yer	• Çalışan ile ilgili iş organizasyonunun sağlanması
	T.C. Kimlik Numarası	• Görevlendirme süreçlerinin yürütülmesi
	Cüzdanın Veriliş Nedeni	• Şirket içi faaliyetlerde çalışanın görev ve yetkilerinin belirlenmesi
	Cüzdanın Veriliş Tarihi	• Personelin etkin yönetilmesi
	Evlilik tarihi	• Erişim yetkilerinin yürütülmesi,
	Pasaport No	• Çalışanın özlük dosyasının tutulması ve bununla ilgili işlemlerin düzenlenmesi
	Doğum Tarihi	• Şirket tarafından yürütülen iş ve faaliyetlerin gerçekleştirilmesi ve ilgili iş birimleri tarafından gerekli çalışmaların yapılması
	Sürücü Belgesi Sınıfı	• Çalışanların maaş ödemelerinin sağlanması
	Medeni Durum	• Kanuni gerekçelerle sgk bildirimlerinin yapılması
	İmza	• GSS, 4a vb. ödemelerinin yapılması
	Doğum Yeri	• Şirketin kamu kurum ve kuruluşlarına olan yükümlülüklerini yerine getirebilmesi ve bu kapsamda buna bağlı iş süreçlerinin yürütülmesi
	Cinsiyet	• Zorunlu BES bildirimi ve ödemelerinin yapılması
	Uyruk	• Çalışanın hak ve yükümlülüklerinin somut olarak belirlenmesi • Çalışanın şirket bünyesinde prim, teşvik, yol, araç tesisi, yemek gibi yan haklarının belirlenmesi ve yöneltmesi • Çalışana tekin ekipmanların sağlanması • Kurumsal iletişim faaliyetlerinin planlanması ve icrası • Faaliyetlerin mevzuata uygun yürütülmesi • Hukuk işlerinin takibi ve yürütülmesi • İletişim faaliyetlerinin yürütülmesi

		• İş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi • Mal/hizmet satış süreçlerinin yürütülmesi • Bilgi güvenliği süreçlerinin yürütülmesi • Denetim/etik faaliyetlerinin yürütülmesi • Erişim yetkilerinin yürütülmesi • Finans ve muhasebe işlerinin yürütülmesi • İş sürekliliğinin sağlanması • Mal/hizmet üretim ve operasyon süreçlerinin yürütülmesi • Sözleşme süreçlerinin yürütülmesi • Tedarik zinciri yönetimi süreçlerinin yürütülmesi • Yetkili kişi, kurum ve kuruluşlara bilgi verilmesi • Acil durum yönetimi süreçlerinin yürütülmesi • Fiziksel mekan güvenliğinin temini • Ziyaretçi kayıtlarının oluşturulması ve takibi • Çalışan aday ve stajyer adaylarının şirketimize yapmış olduğu başvurularda süreç yönetiminin sağlanması • İşe alım süreçleri için gerekli olan bildirimlerin sağlanması • Sürecin yönetilmesi ve çalışan aday ile ilgili toplantı ve görüşme organizasyonun sağlanması • İnsan kaynakları departmanının işe alım süreci ile ilgili gerekli faaliyetleri gerçekleştirebilmesi
İletişim	Telefon Numarası	• Acil durum yönetimi süreçlerinin yürütülmesi • Bilgi güvenliği süreçlerinin yürütülmesi • Erişim yetkilerinin yürütülmesi
	E-Posta Adresi	• Faaliyetlerin mevzuata uygun yürütülmesi • Fiziksel mekan güvenliğinin temin • Denetim/etik faaliyetlerinin yürütülmesi, • İş faaliyetlerinin yürütülmesi/denetimi • Taşınır mal ve kaynakların güvenliğinin temini
	İkametgah Adresi	• Veri sorumlusu operasyonlarının güvenliğinin temini • Ziyaretçi kayıtlarının oluşturulması • Hukuk işlerinin takibi ve yürütülmesi • İletişim faaliyetlerinin yürütülmesi
	Posta Kodu	• Mal/hizmet satış süreçlerinin yürütülmesi • Sözleşme süreçlerinin yürütülmesi • Ürün/hizmetlerin pazarlama süreçlerinin yürütülmesi • Yetkili kişi, kurum ve kuruluşlara bilgi verilmesi

	Adres	• İnsan kaynakları süreçlerinin planlanması • Kurumsal iletişim faaliyetlerinin planlanması ve icrası • Çalışan için gerekli olan kurumsal bildirimlerin sağlanması
	KEP adres bilgisi	• Çalışan ile ilgili iş organizasyonun sağlanması • Görevlendirme süreçlerinin yürütülmesi • Şirket içi faaliyetlerde çalışanın görev ve yetkilerinin belirlenmesi • Personelin etkin yönetilmesi • Çalışanın özlük dosyasının tutulması ve bununla ilgili işlemlerin düzenlenmesi • Finans ve muhasebe işlerinin yürütülmesi • İletişim faaliyetlerinin yürütülmesi • İş sürekliliğinin sağlanması • Tedarik zinciri yönetimi süreçlerinin yürütülmesi • Çalışan aday ve stajyer adaylarının şirketimize yapmış olduğu başvurularda süreç yönetiminin sağlanması • İşe alım süreçleri için gerekli olan bildirimlerin sağlanması • İşe alım sürecinde çalışan adayının başvurmuş olduğu pozisyon için değerlendirilebilmesi • Şirketimizin ve şirketimizle iş ilişkisi içerisinde bulunan ilgili kişilerle teknik, hukuki ticari ve iş süreçlerindeki güvenliğin temini
Özlük	Bordro bilgileri	• Çalışan memnuniyeti ve bağlılığı süreçlerinin yürütülmesi
	Disiplin soruşturması	• Çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi
	İşe giriş belgesi kayıtları	• Denetim / etik faaliyetlerinin yürütülmesi
	Mal bildirim bilgileri	• Faaliyetlerin mevzuata uygun yürütülmesi
	Özgeçmiş bilgileri	• Görevlendirme süreçlerinin yürütülmesi
	Performans değerlendirme raporları	• İnsan kaynakları süreçlerinin planlanması • İş faaliyetlerinin yürütülmesi / denetimi • İç denetim/ soruşturma / istihbarat faaliyetlerinin yürütülmesi • Saklama ve arşiv faaliyetlerinin yürütülmesi • Sözleşme süreçlerinin yürütülmesi
Görsel ve İşitsel Veri	Kapalı devre güvenlik kamerası görüntüleri	• Acil durum yönetimi süreçlerinin yürütülmesi • Bilgi güvenliği süreçlerinin yürütülmesi
	Fotoğraf	• Erişim yetkilerinin yürütülmesi • Faaliyetlerin mevzuata uygun yürütülmesi • Fiziksel mekan güvenliğinin temini • İş faaliyetlerinin yürütülmesi/denetimi
	Şirket içi etkinliklerde elde edilen ses ve görüntü verileri	• Taşınır mal ve kaynakların güvenliğinin temini • Yeri sorumlusu operasyonlarının güvenliğinin temini • Ziyaretçi kayıtlarının oluşturulması ve takibi

		• İnsan kaynakları faaliyetlerinin yürütülmesi ve süreçlerin planlanması • Faaliyetlerin mevzuata uygun yürütülmesi • Yetkili kurum ve kuruluşlara bilgilendirmede bulunulması • Çalışanların giriş çıkış kayıtlarının tutulması • Denetim ve güvenliğin sağlanması
Finans	Kart Bilgileri	• Faaliyetlerin mevzuata uygun yürütülmesi • Hukuk işlerinin takibi ve yürütülmesi
	İBAN	• Mal/hizmet satış süreçlerinin yürütülmesi
	Müşteri Numarası	• Sözleşme süreçlerinin yürütülmesi • Ürün/hizmetlerin pazarlama süreçlerinin yürütülmesi • Yetkili kişi, kurum ve kuruluşlara bilgi verilmesi
Müşteri İşlem	Çağrı merkezi kayıtları	• Faaliyetlerin mevzuata uygun yürütülmesi
	Çek/Senet bilgileri	• Hukuk işlerinin takibi ve yürütülmesi
	Fatura	• İletişim faaliyetlerinin yürütülmesi
	Gişe dekontlarındaki bilgiler	• İş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi
	Müşteri Başvuru Formları	• Mal/hizmet satış süreçlerinin yürütülmesi • Sözleşme süreçlerinin yürütülmesi
	Müşteri Talepleri	• Ürün/hizmetlerin pazarlama süreçlerinin yürütülmesi
	Müşteri Talimatları	• Finans ve muhasebe işlerinin yürütülmesi,
	Sipariş bilgisi	• Talep / şikayetlerin takibi • Yetkili kişi, kurum ve kuruluşlara bilgi verilmesi
İşlem Güvenliği	IP Adresi Bilgileri	• Denetim ve güvenliğin sağlanması
	İnternet Sitesi Giriş Çıkış Bilgileri	• Acil durum yönetimi süreçlerinin yürütülmesi
	İnternet Erişim Kayıt Log'ları	• Bilgi güvenliği süreçlerinin yürütülmesi
	Sistem ve Uygulama Kullanıcı Hesap Bilgileri	• Erişim yetkilerinin yürütülmesi
	Şifre ve Parola Bilgileri	• Fiziksel mekan güvenliğinin temini
	Gezilen sayfa ve incelenen ürün bilgileri	• İş faaliyetlerinin yürütülmesi/denetimi
		• Taşınır mal ve kaynakların güvenliğinin temini • Ziyaretçi kayıtlarının oluşturulması ve takibi
Fiziksel Mekan Güvenliği	İlgili kişilerin giriş çıkış kayıt bilgileri	• Denetim ve güvenliğin sağlanması
	Kamera Kayıtları	• Acil durum yönetimi süreçlerinin yürütülmesi
	Ziyaret edilen kişi bilgisi	• Bilgi güvenliği süreçlerinin yürütülmesi • Erişim yetkilerinin yürütülmesi • Fiziksel mekan güvenliğinin temini • İş faaliyetlerinin yürütülmesi/denetimi • Taşınır mal ve kaynakların güvenliğinin temini • Ziyaretçi kayıtlarının oluşturulması ve takibi
Mesleki Deneyim	Diploma Bilgileri	• Çalışan ile ilgili iş organizasyonun sağlanması
	Gidilen Kurslar Bilgisi	• Şirket içi faaliyetlerde çalışanın görev ve yetkilerinin belirlenmesi
	Meslek İçi Eğitim Bilgileri	• Personelin etkin yönetilmesi

	Sertifika Bilgisi	• Çalışanın özlük dosyasının tutulması ve bununla ilgili işlemlerin düzenlenmesi
	Öğrenim Durumu Bilgisi	• Çalışanın hak ve yükümlülüklerinin somut olarak belirlenebilmesi
	Eğitim ve Beceriler	• Çalışanın, firma bünyesinde prim, teşvik, yol, araç tesisi, yemek gibi yan haklarının belirlenmesi ve yönetilmesi
	Özgeçmiş	• Çalışanlar için iş akdi ve mevzuattan kaynaklanan yükümlülüklerin yerine getirilmesi • Ücret politikasının yürütülmesi • Eğitim faaliyetlerini yürütülmesi • Çalışanların çalışma durumunun kontrolü • İnsan kaynakları faaliyetlerinin yürütülmesi ve süreçlerin planlanması • Faaliyetlerin mevzuata uygun yürütülmesi
Sağlık Bilgileri,Ceza Mahkumiyeti ve Güvenlik Tedbirleri Bilgisi	Sağlık Bilgisi	• Faaliyetlerin mevzuata uygun yürütülmesi
	Ceza Mahkumiyeti	• Çalışanın, firma bünyesinde prim, teşvik, yol, araç tesisi, yemek gibi yan haklarının belirlenmesi ve yönetilmesi
	Güvenlik Tedbiri Bilgisi	• Çalışanın hak ve yükümlülüklerinin belirlenmesi • Görevlendirme süreçlerinin yürütülmesi • Çalışanın pozisyon uygunluk değerlendirmesinin yürütülmesi
Diğer	Banka Hesap Bilgileri	• Çalışan memnuniyeti ve bağlılığı süreçlerinin yürütülmesi • Çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi
	Bakmakla yükümlü olduğu kişi özlük bilgileri	• Çalışanlar için yan haklar ve menfaatleri süreçlerinin yürütülmesi • Finans ve muhasebe işlerinin yürütülmesi • Hukuk işlerinin takibi ve yürütülmesi • İş sağlığı / güvenliği faaliyetlerinin yürütülmesi • Mal / hizmet satın alım süreçlerinin yürütülmesi • Mal / hizmet satış sonrası destek hizmetlerinin yürütülmesi
	Mail order için kredi kartı bilgileri	• Yetkili kişi, kurum ve kuruluşlara bilgi verilmesi
	Araç Plakası	• Müşteri ilişkileri yönetimi süreçlerinin yürütülmesi • Müşteri memnuniyetine yönelik aktivitelerin yürütülmesi

4.2.4. Kişisel Verilerin Saklanma Süreleri

Şirket, faaliyetleri kapsamında işlemekte olduğu kişisel verileri Kanun'un 4'üncü maddesinde yer alan veri işleme ilkelerine uygun olarak aşağıda belirtilen süreler kadar muhafaza etmektedir.

Tablo 3: Kişisel verilerin saklanma süreleri

Veri Kategorisi	Saklama Süresi
Kimlik	İlgili sözleşmenin/hukuki ilişkinin/faaliyetin sona ermesini takiben 10 yıl + 6 ay
İletişim	İlgili sözleşmenin/hukuki ilişkinin/faaliyetin sona ermesini takiben 10 yıl+6 ay
Özlük	İlgili sözleşmenin/hukuki ilişkinin/faaliyetin sona ermesini takiben 10 yıl+6 ay
Görsel ve İşitsel Veri	İlgili sözleşmenin/hukuki ilişkinin sona ermesini takiben 10 yıl + 6 ay
Finans	İlgili sözleşmenin/hukuki ilişkinin sona ermesini takiben 10 yıl + 6 ay
Müşteri İşlem	İlgili sözleşmenin/hukuki ilişkinin sona ermesini takiben 10 yıl + 6 ay
İşlem Güvenliği	İlgili sözleşmenin/hukuki ilişkinin/faaliyetin sona ermesini takiben 2 yıl
Fiziksel Mekan Güvenliği	İlgili sözleşmenin/hukuki ilişkinin sona ermesini takiben 10 yıl + 6 ay
Mesleki Deneyim	İlgili sözleşmenin/hukuki ilişkinin sona ermesini takiben 10 yıl + 6 ay
Ceza Mahkumiyeti ve Güvenlik Tedbiri Bilgisi	İlgili sözleşmenin/hukuki ilişkinin sona ermesini takiben 10 yıl + 3 ay
Sağlık Bilgileri	İlgili sözleşmenin/hukuki ilişkinin sona ermesini takiben 15 yıl + 3 ay
Diğer	İlgili sözleşmenin/hukuki ilişkinin sona ermesini takiben 10 yıl + 6 ay

4857 sayılı İş Kanunu’nda ve ilgili mevzuatta yapılan düzenlemeler ile birlikte iş sözleşmesinden doğan yükümlülükler kapsamında Çalışan’a ait kişisel verilerin saklama sürelerinde birtakım değişiklikler meydana gelmiştir. Bu değişiklikler kapsamında kıdem, ihbar ve kötü niyet tazminatları veya yıllık izin ücretleri bakımından saklama süreleri aşağıdaki gibidir:

Tarih	Tür	Saklama Süresi
25.10.2017 tarihinden önce sona eren iş sözleşmeleri	Kıdem, İhbar ve Kötü Niyet Tazminatları	10 Yıl
01.07.2012 tarihinden önce muaccel olan	Yıllık İzin Ücreti	5 Yıl
01.07.2012-25.10.2017 tarihleri arasında muaccel olan	Yıllık İzin Ücreti	10 yıl
25.10.2017 tarihinden itibaren sona eren iş sözleşmeleri	Kıdem, İhbar ve Kötü Niyet Tazminatları, Yıllık İzin Ücreti	5 Yıl

Tüm bunlara ek olarak 4857 sayılı İş Kanunu’nun ek madde 8/2 düzenlemesi uyarınca “*Ek 3 üncü maddede belirtilen yıllık izin ücreti ve tazminatlar için bu maddenin yürürlüğe girmesinden önce işlemeye başlamış bulunan zamanaşımı süreleri, değişiklikten önceki hükümlere tabi olmaya devam eder. Ancak, zamanaşımı süresinin henüz dolmamış kısmı, ek 3 üncü maddede öngörülen süreden uzun ise, ek 3 üncü maddede öngörülen sürenin geçmesiyle zamanaşımı süresi dolmuş olur.*” olarak belirtilmiştir.

4.3. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi

Kanun'un 7'nci maddesi uyarınca, Kanun ve diğer ilgili mevzuatta yer alan düzenlemelere uygun olarak işlenmiş olmasına rağmen işlenme sebeplerinin ortadan kalkması halinde kişisel verilerin, re'sen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir. İşbu düzenleme kapsamında Şirket, aşağıda açıklanacak usul ve yöntemler ile kişisel verilerin imhasını gerçekleştirmekte ve Kanun'dan doğan yükümlülüklerini yerine getirmektedir.

Şirket, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemleri esnasında gerekli tüm idari ve teknik tedbirleri almaktadır. Bu kapsamda kişisel verilerin saklanması esnasında kişisel hukuka aykırı erişimleri engellemek üzere Şirket tarafından alınmış ve aşağıda açıklamalarına yer verilen teknik ve idari tedbirler kişisel verilerin imhası süreçlerinde de uygulanmaktadır. Bununla birlikte, fiziki ortamda bulunan verilerin imhası esnasında; veriler, yukarıda görev dağılımı verilen kişiler dışındaki birisi tarafından erişilmesinin engellenmesi için kapalı kutular ile imha edilecek ortama getirilmekte ve imha görevli kişiler tarafından gerçekleştirildikten sonra imha tutanağı oluşturulmaktadır. Elektronik ortamdaki veriler bakımından ise öncelikle yetki sınırlandırması yapılarak imha edilecek verilere erişimler kısıtlanmakta akabinde imha edilecek verilerin elektronik ortamda bulunduğu konumlar tespit edilerek aşağıda detayları açıklandığı şekilde verilerin imhası gerçekleştirilmektedir. Elektronik ortamda verilerin imha işlemi Bilgi Teknolojileri departmanı çalışanlarından imha sürecinde görev almış kişiler tarafından yerine getirilmektedir. Ayrıca bu kişilerden bilgi güvenliği taahhütnamesi de alınmış olup verilerin imhası sürecinde gerekli tüm idari ve teknik tedbirlerin uygulanması amaçlanmıştır.

4.3.1. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesini Gerektiren Sebepler

İlgili kişilerin kişisel verileri, yukarıda sayılmış olan kişisel veri işleme nedenlerinin ortadan kalkması, işlemeye esas teşkil eden mevzuatın değişmesi veya mülga hale gelmesi, Kanun'un 11'inci maddesi uyarınca ilgili kişinin kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi, Şirket'in, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanun'da öngörülen süre içinde cevaplamaması ihtimallerinde; ilgili kişinin Kurul'a şikayette bulunması ve bu talebin Kurul tarafından uygun görülmesi durumlarında gerçekleştirilecek ilk periyodik imha süresinde imha edilmektedir.

4.3.2. Kişisel Verilerin Silinme Yöntemleri

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirket, verilerin muhafaza edildiği kayıt ortamlarına göre verilerin silinmesi için ayrı yöntemler uygulamaktadır.

Kişisel verilerin silinmesi sürecinde öncelikle silme işlemine konu edilecek kişisel veriler ve erişim yetki/kontrol matrisi kullanılmak suretiyle ilgili veriye erişim yetkisi bulunan kullanıcılar belirlenmekte, ilgili kullanıcıların kişisel veriler üzerindeki erişim, geri getirme, tekrar kullanma gibi yetkileri kaldırılmakta ve aşağıda yer alan yöntemler ile veriler silinmektedir.

Tablo 4: Kişisel verilerin silinmesi yöntemleri

Kayıt Ortamı	Silme Yöntemi
Bulut Bilişim Sistemleri	Sunucularda bulunan veriler ' <i>Delete</i> ' komutu ile silinmektedir. Ayrıca ilgili kullanıcının erişim ve geri getirme hakları yetki matrisi doğrultusunda kaldırılmaktadır.
E-mail Ortamı	E-mail ortamında bulunan veriler silme komutu verilerek suretiyle silinmektedir. Ayrıca ilgili kullanıcının silinmiş verileri geri getirme yetkisi de kaldırılmaktadır.
Merkezi Sunucular	Merkez sunucularda bulunan veriler ' <i>Delete</i> ' komutu ile silinmekte ve yeniden geri getirilememektedir. Ayrıca ilgili kullanıcının erişim hakları kaldırılmaktadır.
Personel Bilgisayarları	Personel bilgisayarında bulunan veriler tespit edilerek ' <i>Delete</i> ' komutu ile silinmekte ve yeniden geri getirilememektedir.
Fiziksel Ortamlar	Kağıt ortamında bulunan veriler kağıt öğütme makinası ile imha edilecektir. Arşivde bulunan kişisel veriler bakımından silme ve imha işlemi arşive erişim yetkisi bulunan kişi tarafından diğer kullanıcılar için tekrar kullanılamaz hale getirilmesi yöntemi ile uygulanmakta, kilitli birim dolaplarında bulunan kişisel veriler için de yine erişim yetkisi bulunan kullanıcı tarafından aynı yöntem uygulanmaktadır.
PDKS Sistemleri	' <i>Delete</i> ' komutu ile silinmekte ve yeniden geri getirilememektedir. Çalışanın işten ayrılması durumunda talep olmaksızın otomatik olarak imha edilmektedir.
Kamera Kayıt Sistemleri	' <i>Delete</i> ' komutu ile silinmekte ve yeniden geri getirilememektedir.

Ancak, kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır.

- Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması,
- Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.

Bulut bilişim hizmeti alınan üçüncü taraf uygulamasından sağlanan hizmet nedeniyle silinen veriler 30 gün süre ile geri getirilebilir şekilde tutulmaktadır. Bulut bilişim sistemi üzerinde bulunan verilerin silinmesi halinde bu geri getirme yetkisi yalnızca yetki matrisinde belirtilen kişiler tarafından sağlanmaktadır. İlgili kişilerden ayrıca Bilgi Güvenliği Taahhütnamesi alınmış olup bu kişiler dışında silinen verilerin geri getirilmesi veya erişilmesi mümkün olmamaktadır.

4.3.3. Kişisel Verilerin Yok Edilmesi Yöntemleri

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

Kişisel verilerin yok edilmesi için verilerin bulunduğu ortamlar ile tüm kopyaları tespit edilmekte ve tüm veriler için aşağıda belirtilen yöntemler uygulanmak suretiyle kişisel veriler yok edilmektedir.

Kayıt Ortamı	Yok Etme Yöntemi
Bulut Bilişim Sistemleri	Üzerine Yazma
E-mail ortamı	Üzerine Yazma
Merkezi Sunucular	Üzerine Yazma
Personel Bilgisayarları	Üzerine Yazma
Fiziksel Ortamlar	Fiziksel Yok Etme
PDKS Sistemleri	Üzerine Yazma
Kamera Kayıt Sistemleri	Üzerine Yazma

Fiziksel Yok Etme: Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler yok edilirken kişisel verinin sonradan kullanılamayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Kâğıt ve mikrofiş ortamındaki verilerin yok edilmesi de başka bir şekilde yok edilmeleri mümkün olmadığından bu şekilde gerçekleştirilmelidir.

Üzerine Yazma: Üzerine yazma yöntemi, özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkânsızlaştıran veri yok etme yöntemidir.

4.3.4. 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.

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya alıcı grupları 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 gerekmektedir.

Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan grupta, maskeleye, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilmekte olup Şirket tarafından kişisel verilerin anonim hale getirilmesinde aşağıda belirtilen yöntemler kullanılmakta ve veriler ilgili kişi ile ilişkilendirilemeyecek hale getirilmektedir.

Tablo 6: Kişisel verilerin anonim hale getirilmesi yöntemleri

Anonim Hale Getirme Yöntemleri	Uygulama
Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemi	• Değişkenleri Çıkartma • Kayıtları Çıkartma • Bölgesel Gizleme • Genelleştirme • Alt ve Üst Sınır Kodlama • Global Kodlama • Örneklem
Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemi	• Mikro Birleştirme • Veri Değiş Tokuşu • Gürültü Ekleme
Anonim Hale Getirmeyi Kuvvetlendirici İstatistiksel Yöntemi	• K-Anonimlik • L-Çeşitlilik • T-Yatkınlık

4.4. PERİYODİK İMHA SİSTEMİ

Yönetmelik'in 5'inci maddesi uyarınca saklama ve imha politikası hazırlamış olan veri sorumlusunun, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri silme, yok etme veya anonim hale getirme işlemlerini yerine getirme yükümlülüğü bulunmaktadır.

Şirket, ilgili mevzuat düzenlemelerinde öngörülen yükümlülüklerle uygun olarak, yukarıda açıklanmış bulunan kişisel verilerin imhasını gerektiren sebeplerin ortaya çıkması halinde ilk periyodik imha sürecinde bu verileri silmekte, yok etmekte veya anonim hale getirmektedir.

Şirket nezdinde belirlenen periyodik imha süresi 6 ay olup periyodik imha işlemleri her yıl Haziran ve Aralık aylarında gerçekleştirilmektedir. Kişisel verilerin özel nitelikli kişisel veriler kapsamında olması halinde periyodik imha süresi 3 aydır.

Periyodik imha süresine ek olarak, ilgili kişinin veri sorumlusuna başvurusunun uygun görülmesi halinde en geç 30 gün içinde talep doğrultusunda imha işlemi gerçekleştirilecektir.

İmhası Gerçekleştirilen Kayıtlara Ait Bilgilerin Muhafazası

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler tutanak ile kayıt altına alınmakta ve söz konusu kayıtlar imha tarihinden itibaren en az 3 yıl süreyle saklanmaktadır.

Talep üzerine imha edilen veriler için tüm talep bilgileri ve ilgili kişi ile gerçekleştirilen iletişim detayları (yazılı form ve Kanun'da bahsi geçen kimlik doğrulama bilgileri, Şirket tarafından oluşturulmuş olan başvuru formu ve Kanun'da bahsi geçen kimlik doğrulama bilgileri, başvuru cevap formu, mail iletileri, ses kayıtları ve imha tarihi vb. gibi), kanunlara delil teşkil etmesi nedeniyle 3 yıl süre muhafaza edilmektedir.

Periyodik olarak gerçekleştirilen imha verileri, kanunlara delil teşkil etmesi nedeniyle 3 yıl süre ile muhafaza edilmektedir.

Veri imha kayıtlarına sadece KVK Kurulu Üyeleri erişebilmektedir.

Basılı ortamda bir imha gerçekleşti ise,

- İmhası gerçekleştirilen evrakların veri kategorisi belirlenerek, birden fazla veri kategorisinin imhası gerçekleştirilmiş ise imha edilen kategoriler ardışık halde tutanakta belirtilir,
- Periyodik imha gerçekleştiriliyor ise evrakları ayırt etmeye yarayan bir numara imha tutanağında belirtilir,
- Talep üzerine imha gerçekleştiriliyorsa imha edilen evrakların bilgileri tutanağa işlenir (özlük numarası, fatura numarası vs.),
- Evrakın oluşma tarihi ya da bir sözleşmenin ifası ile imha gerçekleşiyor ise sözleşme tarihi (periyodik imha ise tarih aralığı) ile
- İmha tarihine kadar saklanması gerektiren sebepler (kanunlar/iş gerekçeleri) tutanağa yazılır.

Basılı ortam için gerçekleştirilen imhaların kayıtları işbu Politika'da belirtilen imha sürecinde görev alan kişilerce imza edilerek imha tutanakları Şirket merkezinde 3 yıl süre ile muhafaza edilmektedir.

Basılı ortamlar dışındaki ortamlarda yapılacak silme, yok etme veya anonim hale getirme işlemlerinde, oluşturulacak otomatik imha kayıtları içerisinde asgari olarak isim, soyisim, telefon, vb. bilgileri yer alır. Ayrıca elektronik ortamlarda gerçekleştirilen veri imha işlemlerinde log kayıtları da tutulmakta ve Bilgi Teknolojileri Departmanı'nda 3 yıl süre ile muhafaza edilmektedir.

4.5. TEKNİK VE İDARİ TEDBİRLER

Kanun'un 12 inci maddesi uyarınca veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini veya verilere hukuka aykırı erişilmesini önlemek ve verilerin güvenli şekilde muhafazasını sağlamak ile yükümlü kılınmıştır. Bununla birlikte veri sorumlusu nezdinde özel nitelikli kişisel verilerin işlenmesi durumunda Kurul tarafından belirlenmiş olan Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler'e uygun şekilde veri işleme faaliyetinin gerçekleştirilmesi gerekmektedir. Bu kapsamda Şirket, alınması gereken tüm idari ve teknik tedbirleri almakta veri güvenliğinin sağlanması bakımından azami gayret ve özeni göstermektedir.

4.5.1. Teknik Tedbirler

Sertrans Holding tarafından uygulanmakta olan teknik tedbirler ařağıdaki gibidir:

- Ağ güvenliğı ve uygulama güvenliğı saėlanmaktadır,
- Bilgi teknolojileri sistemleri tedarik, geliřtirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır,
- Bulutta depolanan kiřisel verilerin güvenliğı saėlanmaktadır,
- Eriřim logları düzenli olarak tutulmaktadır,
- Eriřim, bilgi güvenliğı, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır,
- Güvenlik duvarları kullanılmaktadır,
- Kiřisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır,
- Kağıt yoluyla aktarılan kiřisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir,
- Kiřisel veri içeren ortamların güvenliğı saėlanmaktadır,
- Kiřisel veriler yedeklenmekte ve yedeklenen kiřisel verilerin güvenliğı de saėlanmaktadır,
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi yapılmaktadır,
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır,
- Sızma testi uygulanmaktadır,
- Çalışanlar için yetki matrisi oluşturulmuştur,
- Görev deėiřikliğı olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır,
- Güncel anti-virüs sistemleri kullanılmaktadır,
- Kiřisel veri içeren ortamların güvenliğı saėlanmaktadır,
- Kiřisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliğı saėlanmaktadır,
- Şifreleme yapılmaktadır.

4.5.2. İdari Tedbirler

Şirket tarafından uygulanmakta olan idari tedbirler ařağıdaki gibidir:

- Çalışanlar için veri güvenliğı hükümleri içeren disiplin düzenlemeleri mevcuttur,
- Çalışanlar için veri güvenliğı konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır,
- Gizlilik taahhütleri yapılmaktadır,
- Kiřisel veri güvenliğı politika ve prosedürleri belirlenmiştir,
- Kiřisel veri güvenliğı sorunları hızlı bir şekilde raporlanmaktadır,

- Kişisel veriler mümkün olduğunca azaltılmaktadır,
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır,
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir,
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yapılmaktadır,
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır,
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır,
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

4.6. GEÇERLİLİK VE DOKÜMAN YÖNETİMİ

Şirket tarafından, fiilen uygulanmakta olan mevcut yöntemlerde veya mevzuat düzenlemelerinde değişiklik olması halinde Politika üzerinde ilgili güncellemeler yapılabilmektedir. Ancak her halükârda kişisel veri güvenliğinin azami düzeyde sağlanması bakımından Politika en az yılda bir kez kontrol edilmekte ve gerekli görülen düzenlemeler yapılmaktadır.

İşbu Politika'nın etkinliği ve yeterliliği değerlendirilirken, ayrıca periyodik imha sırasında yaşanan aksaklıklar ile hakkında hiçbir kayıt tutulmayan veya Kanun'a ve Politika'da belirtilen yöntemlere uygun şekilde imha edilmeyen dokümanların sayısı göz önünde bulundurulmaktadır.

5. YÜRÜRLÜK VE REVİZYON

İşbu Politika 15.09.2020 tarihinde yürürlüğe girmiştir. Şirket'in Politika üzerinde değişiklik yapma hakkı saklı olup Politika'nın tamamının veya belirli maddelerinin yenilenmesi durumunda Politika'nın yürürlük tarihi güncellenecektir. Politika'nın revize edilmesi halinde yeni Politika örneği ilgili yerlerde ilan edilecektir.

6. VERİ SORUMLUSUNA BAŞVURU

İşbu Politika kapsamında ilgili kişi sıfatına haiz veri sahiplerinin, Kanun'un 11. maddesine göre veri sorumlusuna başvurarak; kendileriyle ilgili kişisel verilerin işlenip işlenmediğini öğrenme, işlenmişse bunlara ilişkin bilgi talep etme, verinin içeriğinin eksik veya yanlış olması halinde bunların düzeltilmesini, hukuka aykırı olması halinde ise silinmesini, yok edilmesini ve buna göre yapılacak işlemlerin verilerin açıklandığı üçüncü kişilere bildirilmesini ve verilerin kanuna aykırı olarak işlenmesi sebebiyle zararlarının giderilmesini talep etme hakları bulunmaktadır.

İlgili kişi sıfatına haiz olmanız halinde taleplerinizi, kimliğinizi tespit edecek bilgi ve belgeler ile yazılı ve ıslak imzalı olarak Şirket merkezinin bulunduğu taleplerinizi Ömerli Mah. İstanbul Cad. No:260 Hadımköy,Arnavutköy-İstanbul adresine bizzat elden iletebilir, noter kanalıyla

gönderebilir, Şirketimize ait olan **sertrans@hs02.kep.tr** KEP adresi üzerinden elektronik imzalı olarak gönderebilir.

Şirket tarafından, taleplerinizin 30 günden fazla olmamak üzere en kısa sürede ve işlemin maliyeti olmadığı sürece ücret talep edilmeksizin cevaplanacağı taahhüt edilmektedir.

İlgili Dokümanlar:

SRT-FORM-16 Kişisel Veri imha tutanağı