

İçindekiler

1	GİRİŞ	2
1.1	Amaç.....	2
1.2	Kapsam.....	2
2	TANIMLAR VE KISALTMALAR	2
3	SORUMLULUK VE GÖREV DAĞILIMLARI.....	4
4	KAYIT ORTAMLARI	7
5	SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR	7
5.1	Saklamayı Gerektiren Hukuki Sebepler	8
5.2	Saklamayı Gerektiren İşleme Amaçları.....	9
5.3	İmhayı Gerektiren Sebepler.....	9
6	TEKNİK VE İDARİ TEDBİRLER	10
6.1	Teknik Tedbirler	10
6.2	İdari Tedbirler	11
7	KİŞİSEL VERİLERİ İMHA TEKNİKLERİ	13
7.1	Kişisel Verilerin Silinmesi.....	13
7.2	Kişisel Verilerin Yok Edilmesi	13
7.3	Kişisel Verilerin Anonimleştirilmesi	14
8	SAKLAMA VE İMHA SÜRELERİ	15
9	PERİYODİK İMHA SÜRESİ.....	17
10	POLİTİKANIN YAYINLANMASI VE SAKLANMASI.....	17
11	POLİTİKANIN GÜNCELLENME PERİYODU.....	17
12	POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI	17
13	REVİZYON TAKİP ÇİZELGESİ	18

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

1 GİRİŞ

1.1 Amaç

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

Şirketimiz, kişisel verileri işlendikleri amaç için gerekli olan süre ve ilgili faaliyetin tabi olduğu yasal mevzuatta öngörülen minimum sürelerle uygun olarak muhafaza etmektedir. Bu kapsamda, Şirketimiz öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini tespit etmekte, bir süre belirlenmişse bu süreye uygun davranmaktadır. Yasal bir süre mevcut değil ise kişisel veriler işlendikleri amaç için gerekli olan süre kadar saklanmaktadır. Kişisel veriler belirlenen saklama sürelerinin sonunda periyodik imha sürelerine veya veri sahibi başvurusuna uygun olarak ve belirlenen imha yöntemleri (silme ve/veya yok etme ve/veya anonimleştirme) ile imha edilmektedir.

1.2 Kapsam

Bu Politika kapsamında, herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik veya otomatik olmayan yollarla işlenen gerçek kişiler olarak müşteriler, müşteri adayları, çalışan adayları, çalışanlar, stajyerler, tedarikçiler, IAS Business Academy eğitimleri katılımcıları, şirket yetkilileri, ziyaretçiler, iş ortakları, iş birliği içinde olunan kişi ve şirketlerin çalışanları, pay sahipleri, yetkilileri ve üçüncü kişiler bulunmaktadır. Politika, Şirketimizce yönetilen, tüm kişisel verilerin işlenmesi ve korunmasına yönelik yürütülen faaliyetlerde uygulanmaktadır.

2 TANIMLAR VE KISALTMALAR

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.
------------------	--

Hazırlayan Kalite Yönetim Sistemleri Uzmanı Onay	Gözden Geçiren Kalite Sistemleri Yöneticisi Onay	Onaylayan Genel Müdür Onay
---	--	----------------------------------

Aydınlatma Yükümlülüğü	Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi, Kanun'un 11 inci maddesinde sayılan diğer hakları, konusunda bilgi vermektir.
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 kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir.
Kanun veya KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu'dur.
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 ortamdır.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.
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 işlemdir.
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
Kurul	Kişisel Verileri Koruma Kurulu'dur.

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

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 verileridir.
Periyodik İmha	Kanun'da yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemidir.
Veri Sahibi/ İlgili Kişi	Kişisel verisi işlenen gerçek kişidir.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişidir.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.
Yönetmelik	28 Ekim 2017 tarihinde Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'tir.

3 SORUMLULUK VE GÖREV DAĞILIMLARI

Şirket'in tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanması 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.

Hazırlayan Kalite Yönetim Sistemleri Uzmanı Onay	Gözden Geçiren Kalite Sistemleri Yöneticisi Onay	Onaylayan Genel Müdür Onay
---	--	----------------------------------

Birim	GÖREV	SORUMLULUK
İnsan Kaynakları Birimi	Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Sistem Destek Birimi	Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Muhasebe & Finans Birimi	Kişisel veri saklama ve imha politikası saklama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Satış Birimi	Kişisel veri saklama ve imha politikası saklama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
İdari İşler ve Satın alma Birimi	Kişisel veri saklama ve imha politikası saklama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Pazarlama Birimi	Kişisel veri saklama ve imha politikası saklama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

IBA Birimi	Kişisel veri saklama ve imha politikası saklama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Danışmanlık Birimi	Kişisel veri saklama ve imha politikası saklama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Proje Yönetim ve Kontrolü Birimi	Kişisel veri saklama ve imha politikası saklama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Kalite Yönetim Sistemleri Birimi	Kişisel veri saklama ve imha politikası saklama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
BGYS-KVKK	Kişisel veri saklama ve imha politikası saklama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

Tablo 1: Saklama ve imha süreçleri görev dağılımı

Hazırlayan Kalite Yönetim Sistemleri Uzmanı Onay	Gözden Geçiren Kalite Sistemleri Yöneticisi Onay	Onaylayan Genel Müdür Onay
---	--	----------------------------------

4 KAYIT ORTAMLARI

Şirket tarafından işlenen Kişisel Veriler, aşağıda yer alan kayıt ortamlarında saklanmaktadır.

Elektronik Ortamlar	Fiziksel Ortamlar
Sunucular (Etki alanı, yedekleme, e-posta, Veri tabanı, web) Yazılımlar (Ofis Yazılımları) Bilgi güvenliği cihazları (güvenlik duvarı, antivirüs vb.) Mobil cihazlar (telefon, tablet vb.) Şirket Bilgisayarları (Masaüstü, Dizüstü)	Kâğıt (yazılı, basılı, görsel ortamlar) Arşiv Dosyaları

5 SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; müşteriler, müşteri adayları, çalışan adayları, çalışanlar, stajyerler, tedarikçiler, IAS Business Academy eğitimleri katılımcıları, şirket yetkilileri, ziyaretçiler, iş ortakları, iş birliği içinde olunan kişi ve şirketlerin çalışanları, pay sahipleri, yetkilileri ve üçüncü kişilere ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

Şirket tarafından toplanan kişisel veriler Kanun'un ilgili maddeleri doğrultusunda hukuka ve dürüstlük kurallarına uygun, doğru ve gerektiğinde güncel olacak şekilde, belirli, açık ve meşru amaçlar için işlenmekte, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak kullanılmakta ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan ve Şirketçe işbu Politika'da belirlenen süreler kadar muhafaza edilmektedir.

Şirket tarafından işlenen kişisel verilere ilişkin Veri Sahibi'nden açık rıza alınmaktadır. Ancak Kanun'un 5. Maddesi kapsamında aşağıda sayılan hallerde Veri Sahibi'nin açık rızası olmaksızın kişisel verinin işlenmesi mümkündür. Bu haller şöyle sayılmaktadır:

- Kanunlarda açıkça öngörülmesi,
- 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,

Hazırlayan Kalite Yönetim Sistemleri Uzmanı Onay	Gözden Geçiren Kalite Sistemleri Yöneticisi Onay	Onaylayan Genel Müdür Onay
---	--	----------------------------------

- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hali.

5.1 Saklamayı Gerektiren Hukuki Sebepler

Şirket faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler.

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 4857 Sayılı İş Kanunu,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun,
- 6102 sayılı Türk Ticaret Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 6502 sayılı Tüketicinin Korunması Hakkında Kanun,
- 6183 sayılı Amme Alacaklarının Tahsili Kanunu
- 4632 Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu,
- 213 sayılı Vergi Usul Kanunu,
- 27579 sayılı Sosyal Sigorta İşlemleri Yönetmeliği,
- 29417 Sayılı Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik,
- 29029 Sayılı Resmî Gazetede Yayınlanan Satış Sonrası Hizmetler Yönetmeliği,
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

5.2 Saklamayı Gerektiren İşleme Amaçları

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

- Şirketin mevzuattan kaynaklanan yükümlülükleri yerine getirmesi,
- Şirketin iş sağlığı ve güvenliğine ilişkin gerekli ve yeterli önlemleri alabilmesi,
- Şirket faaliyetlerinin hukuka ve faaliyet konusuna ilişkin mevzuat ve içtihat hükümlerine uygun olarak yürütülmesi,
- Şirketin taraf olduğu sözleşmelerin mevcut hukuk kuralları çerçevesinde, amacına uygun, eksiksiz ve doğru olarak akdedilmesi,
- Verileri kaydedilen kişiler ile doğru iletişimin sağlanabilmesi,
- Şirketin finans, muhasebe ve hukuk işlerinin ve denetimlerinin yürütülmesi,
- Gerekli hallerde, kanun tarafından yetkili kılınmış makam, mercii ve kurumlar tarafından talep edilen bilgilerin paylaşılması ve/veya kanun hükümleri uyarınca Şirketin bildirim yapma yükümlülüğünün bulunduğu hallerde doğru bilgilendirmenin yapılabilmesi,
- Şirketin insan kaynakları süreçlerinin ve yönetim faaliyetlerinin yürütülmesi,
- Şirketin ticari faaliyetlerinden ve Şirket içi personel, ortak, yönetim kurulu üyeleri arasında doğabilecek her türlü uyuşmazlığa ilişkin delil olarak kullanılabilmesi,
- Kurumsal iletişimi sağlamak ve Şirket'in pazarlama faaliyetlerinin yürütülmesi,
- Şirket güvenliğini sağlamak,
- Yasal raporlamalar yapmak,
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek,
- Çağrı merkezi süreçlerini yönetmek.

5.3 İmhayı Gerektiren Sebepler

Şirket, aşağıdaki hallerin varlığı halinde işlediği kişisel verileri yok etmektedir. Bu haller şöyle sıralanabilir.

- 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,

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine 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 Kanunda öngörülen süre içinde cevap vermemesi hallerinde; ilgili kişinin Kurum'a şikâyette bulunması ve bu talebin Kurum tarafından uygun bulunması,
- Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

6 TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanun'un 12. maddesiyle Kanunun 6. maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde, Şirket tarafından aşağıda sayılan teknik ve idari tedbirler alınmaktadır.

6.1 Teknik Tedbirler

- Mevcut sistemler kapsamında gerekli iç kontroller yapılır.
- Düzenli olarak ve ihtiyaç olduğunda sızma testi yaptırarak sistem zafiyetlerinin kontrolünü sağlar varsa bilişim sistemlerine yönelik risk, tehdit, zafiyet ve açıklıkları ortaya çıkararak gerekli önlemleri alır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile güvenlik politikaları aracılığı ile yapılmaktadır.
- Şirketin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınır.

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenir, bu risklere uygun teknik tedbirlerin alınması sağlanır ve alınan tedbirlere yönelik teknik kontroller yapılır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulur.
- Silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri alınır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Kurum tarafından IS FR 03 Bilgi Güvenliği İhlal Olayı Bildirim Formu ile kayıt altına alınır. Hukuk Birimi sürece dahil edilir.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Şirket internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.

6.2 İdari Tedbirler

- Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırılır. Bu personel ile Şirket arasında verilerin güvenliğine ilişkin gerekli sözleşme ve protokoller düzenlenir.
- Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam edilir ve personele kişisel verilerin korunması mevzuatı ve bilgi güvenliği kapsamında gerekli eğitimler verilir.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

- Şirket içerisinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla ISO 27001 denetimi ile birlikte periyodik denetimler yapılır veya yaptırılır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetleri giderilir.
- Kişisel veri işleme envanteri hazırlanmıştır.

Kanunu'nun 6. maddesinde, hukuka aykırı olarak işlendiğinde kişilerin mağduriyetine veya ayrımcılığa sebep olma riski taşıyan kişisel veriler "Özel Nitelikli" olarak belirlenmiştir. Bu veriler; ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir. Özel Nitelikli Kişisel Veriler, otomatik ya da otomatik olmayan yöntemler ile sözlü, yazılı ya da elektronik olarak toplanabilmektedir. Bu veriler, elektronik ve/veya fiziksel ortamlarda saklanmaktadır.

"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı uyarınca, Özel nitelikli kişisel verilerin güvenliğine yönelik uygulamalar aşağıdaki şekildedir:

- Özel nitelikli kişisel veri işleyen personele, veri güvenliğine ilişkin gerekli eğitim verilmiş, bilgilendirme yapılmıştır.
- Özel nitelikli kişisel veri işleyen personel ve bu verilerin paylaşıldığı kişiler ile gizlilik hükümleri imzalanmıştır.
- Özel nitelikli kişisel verilere erişimi olan kullanıcıların yetki kapsamı ve süreleri kendilerine bildirilmiştir.
- Periyodik olarak yetki kontrolleri gerçekleştirilmektedir.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri derhal kaldırılmaktadır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlarda, verilerin kriptografik yöntemler kullanılarak muhafaza edilmektedir. Kriptografik anahtarlar güvenli ve farklı ortamlarda tutulmaktadır. Veriler üzerinde gerçekleştirilen tüm hareketler güvenli olarak loglanmaktadır. Gerekli program güncellemeleri düzenli aralıklarla kontrol edilmektedir.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamlarda verilerin bulunduğu ortamda yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınmaktadır. Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmektedir.

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

- Özel nitelikli kişisel veriler, verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılmaktadır. Veriler, taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarıldığında kriptografik yöntemlerle şifrelenmektedir.
- Özel nitelikli kişisel veriler kâğıt ortamı yoluyla aktarıldığında, evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınmaktadır ve evrak "gizlilik dereceli belgeler" formatında gönderilmektedir.

7 KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Şirket tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

7.1 Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin kayıt ortamlarına göre silme yöntemleri aşağıda belirtilmiştir:

- Bulut sisteminde yer alan kişisel veriler, geri getirme yetkisi olmaksızın silme komutu verilerek silinir.
- Merkezi sunucuda yer alan ofis dosyalarında yer alan kişisel veriler, işletim sistemindeki silme komutu ile ya da dosyanın bulunduğu dizin üzerinde erişim haklarının kaldırılması suretiyle silinir.
- Taşınabilir medyada bulunan kişisel veriler şifreli olarak saklanır ve uygun yazılımlar kullanılarak silinir. Kişisel verilerin veri tabanlarında bulunması halinde ilgili satırlar veri tabanı komutları ile silinir.

7.2 Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılmaz hale getirilmesi işlemidir. Kişisel verilerin kayıt ortamlarına göre yok etme yöntemleri aşağıda belirtilmiştir:

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

- Yerel sistemler üzerinde yer kişisel veriler de-manyetize etme, üzerine yazma ya da fiziksel yok etme yöntemlerinden biri ile yok edilir.
- Ağ cihazları (içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. De-manyetize etme, fiziksel yok etme ya da üzerine yazma yöntemlerinden bir ya da birkaçı kullanılmak suretiyle yok edilir.
- Flash tabanlı ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da de-manyetize etme, fiziksel yok etme ya da üzerine yazma yöntemlerinden bir ya da birkaçı kullanılmak suretiyle yok edilir.
- Manyetik disk gibi ünitelerde, yer alan veriler çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.
- Optik diskler, yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilir.
- Kâğıt ortamında bulunan kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kâğıt imha veya kırma makinaları ile anlaşılabilir boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünür.
- Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre de-manyetize etme, fiziksel yok etme ya da üzerine yazma yöntemlerinden bir ya da birkaçı kullanılmak suretiyle yok edilir.
- Bulut Ortamında yer alan kişisel veriler, kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılır. Bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilir.

7.3 Kişisel Verilerin Anonimleştirilmesi

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

Hazırlayan Kalite Yönetim Sistemleri Uzmanı Onay	Gözden Geçiren Kalite Sistemleri Yöneticisi Onay	Onaylayan Genel Müdür Onay
---	--	----------------------------------

İlgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir. Anonimleştirme işlemi BAST90 KVKK uygulamasıyla gerçekleştirilir.

8 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 kayıta;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikası'nda yer alır.
- Söz konusu saklama süreleri üzerinde, gerekmesi halinde Kalite Yönetim Sistemleri Departmanı tarafından güncellemeler yapılır.
- Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi varlık sahibi ilgili birim tarafından yerine getirilir.

Süreç	Saklama Süresi	İmha Süresi
İş Kanunu kapsamında saklanan veriler (örn. Performans kayıtları, özlük dosyasına ilişkin bilgiler, mesleki deneyim bilgisi vs.)	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
İş sağlığı ve güvenliği mevzuatı kapsamında toplanan veriler (özlük dosyasına ilişkin bilgiler, sağlık raporları, özel sağlık sigortasına ilişkin bilgiler, bordro işlemleri vs.)	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
SGK mevzuatı kapsamında tutulan veriler	İş ilişkisinin sona ermesine müteakip 15 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
İş kazası/meslek hastalığına ilişkin bir talepte/davada kullanılabilecek dokümanlar	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Sair ilgili mevzuat gereği toplanan veriler	İlgili mevzuatta öngörülen süre kadar	Saklama süresinin bitimini takiben ilk periyodik imha süresinde

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

Süreç	Saklama Süresi	İmha Süresi
İlgili kişisel verinin Türk Ceza Kanunu veya sair ceza hükmü getiren mevzuat kapsamında bir suça konu olması	Dava zaman aşımı müddetince/Hukuki ilişki sona erdikten sonra 10 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Zimmet Formu	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Tedarikçi verileri	Sözleşme devam ettiği müddetçe	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Şirket ortağı/ yönetim kurulu üyelerine ilişkin veriler	Görevleri devam ettiği müddetçe	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Sözleşmelerin hazırlanması ve imzalanması	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Şirket İletişim Faaliyetlerinin İcrası	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Kamera Kayıtları	30 gün	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Çerez ve Log Kayıtları	6 ay - En fazla 2 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Çevrimiçi Ziyaretçilere İlişkin Trafik Bilgileri	2 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
IBA Eğitim Katılımcılarının Kaydı	Etkinliğin sona ermesini takiben 2 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
SLA Raporları	2 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Pazarlama Bilgileri	Müşteri ilişkisinin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

Süreç	Saklama Süresi	İmha Süresi
Finans Bilgileri	Hukuki ilişki sona erdikten sonra 10 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde
Ziyaretçi İnternet Girişlerine İlişkin Aydınlatma Metni	Etkinliğin sona ermesinden itibaren 2 yıl	Saklama süresinin bitimini takiben ilk periyodik imha süresinde

İşbu Kişisel Veri Saklama ve İmha Politikası içerisinde mevzuat değişiklikleri, güncel içtihat hükümleri ile yargı kararlarındaki yenilikler ve sair sebeplerden dolayı değişiklik yapılabilecektir.

9 PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir.

10 POLİTİKANIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. IAS Personeline e-posta ile duyurusu yapılarak, caniasERP DOCT01 Doküman Yönetimi uygulamasında saklanır.

11 POLİTİKANIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

12 POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, caniasERP DOCT01 Doküman Yönetimi uygulamasına yüklendikten ve IAS personeline e-posta ile duyurulduktan sonra yürürlüğe girmiş kabul edilir. Politika, Şirket'in internet sitesinde yayınlanır. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları Kalite Yönetim Sistemleri Departmanı tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 2 yıl süre ile Kalite Yönetim Sistemleri Departmanı tarafından saklanır.

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay

13 REVİZYON TAKİP ÇİZELGESİ

Revizyon No	Revizyon Tarihi	Güncelleme Yapan	Açıklamalar

Hazırlayan
Kalite Yönetim Sistemleri
Uzmanı
Onay

Gözden Geçiren
Kalite Sistemleri Yöneticisi
Onay

Onaylayan
Genel Müdür
Onay