

SPACE SOLUTIONS FOR TOMORROW

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Date: 07.01.2025

Rev: AA

İçindekiler

1 AMAÇ.....	4
2 KAPSAM	4
3 TANIMLAR	4
4 SORUMLULUK VE GÖREVLER	5
5 KAYIT ORTAMLARI	6
6 SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER	6
7 SAKLAMAYI GEREKTİREN İŞLEME ARAÇLARI	6
8 İMHAYI GEREKTİREN HUKUKİ SEBEPLER	6
9 TEKNİK TEDBİRLER	7
10 İDARİ TEDBİRLER	7
11 KİŞİSEL VERİLERİN SİLİNMESİ YÖNTEMLERİ	7
12 KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ	8
13 SAKLAMA VE İMHA SÜRELERİ	8
14 PERİYODİK İMHA SÜRESİ.....	8
15 POLİTİKANIN YAYIMLANMASI SAKLANMASI VE GÜNCELLENMESİ...	9
16 YÜRÜRLÜK.....	10
17 EKLER	10

Tablo Listesi

EK TABLO 1 Saklama ve imha süreçleri görev dağılımı	10
EK TABLO 2 Kişisel Veri Saklama Ortamları	10
EK TABLO 3 Kişisel Verilerin Silinmesi Yöntemleri	10
EK TABLO 4 Kişisel Verilerin Yok Edilmesi Yöntemleri	11
EK TABLO 5 Saklama ve İmha Süresi Tablosu	11

1 AMAÇ

Kişisel Veri Saklama ve İmha Politikası ("Politika"), Plan S Uydu ve Uzay Teknolojileri Anonim Şirketi ("Şirket") tarafından işlenen kişisel verilerin saklanması ve imhasına ilişkin usul ve esasları belirlemek amacıyla hazırlanmıştır.

Bu Politika, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ile 28.10.2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") hükümleri esas alınarak hazırlanmıştır.

2 KAPSAM

Şirket çalışanlarına, çalışan adaylarına, stajyerlere, ürün ve hizmet alanlara, potansiyel müşterilere, ortaklara, ziyaretçilere, tedarikçilere ve diğer üçüncü kişilere ait kişisel veriler bu politika kapsamındadır.

Şirketin sahip olduğu ya da şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu politika uygulanır.

3 TANIMLAR

Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.

Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye 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: Şirket personeli

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.

Hizmet sağlayıcı: Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.

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.

İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.

Kanun: 6698 Sayılı Kişisel Verilerin Korunması Kanunu.

Kayıt ortam: 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 işleme 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 işlenmesi: 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 ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.

Periyodik imha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.

Politika: Kişisel Verileri Saklama ve İmha Politikası.

Şirket: PLAN S Uydu ve Uzay Teknolojileri A.Ş.

Veri işleyen: 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 kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.

Veri sorumluları sicil bilgi sistemi: Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.

VERBİS: Veri Sorumluları Sicil Bilgi Sistemi.

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

4 SORUMLULUKLUK VE GÖREVLER

Şirketin tüm çalışanları ve birimleri; kişisel verilerin hukuka uygun olarak elde edilmesi, işlenmesi ve saklanması konusunda sorumlu birimlere tam ve aktif destek verir. Politika kapsamında alınan idari ve teknik tedbirlerin uygulanmasında, birim çalışanlarının eğitilmesinde, çalışanların farkındalığının sağlanmasında, artırılmasında ve izlenmesinde, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesinde ve kişisel verilerin hukuka uygun olarak muhafazasında tüm çalışanlar ve birimler, sorumlu birimlere destek olur.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım EK TABLO: 1’de gösterilmiştir.

5 KAYIT ORTAMLARI

Kişisel veriler, şirket tarafından EK TABLO: 2’de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde muhafaza edilir.

6 SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

Şirkette, faaliyetler çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar ve kanun ile ilgili mevzuat kapsamında muhafaza edilir. Bu kapsamda saklamayı gerektiren sebepler şunlardır:

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

7 SAKLAMAYI GEREKTİREN İŞLEME ARAÇLARI

Şirket aşağıdakiler dahil olmak ancak bununla sınırlı olmamak üzere, ilgili kişinin veya ilgili kişi tarafından belirtilen üçüncü tarafların kişisel verilerini çeşitli amaçlarla işleyebilir:

- İnsan kaynakları süreçlerini yürütmek
- Kurumsal iletişimi sağlamak
- Şirket güvenliğini sağlamak
- İstatistiksel çalışmalar yapabilmek
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak
- Şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak
- Yasal raporlamalar yapmak
- Çağrı merkezi süreçlerini yönetmek
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü yerine getirmek
- Şirket hukuk işlerinin icrası/takibini yapmak

8 İMHAYI GEREKTİREN HUKUKİ SEBEPLER

Kişisel veriler, aşağıdaki durumların varlığı halinde ilgili kişinin talebi üzerine veya re’sen şirket tarafından silinir ya da yok edilir:

- Kişisel verinin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya kaldırılması
- Kişisel verinin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması

- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi
- Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması

9 TEKNİK TEDBİRLER

- Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıdadır:
- Kurulan sistemler kapsamında gerekli iç kontrolleri yapar
- Kurulan sistemler kapsamında bilgi teknolojileri risk değerlendirmesi ve iş etki analizinin gerçekleştirilmesi süreçlerini yürütür
- Verilerin şirket dışına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini ve ilgili matrislerin oluşturulmasını sağlar
- Düzenli olarak ve ihtiyaç oluştuğunda sızma testi hizmeti alarak sistem zafiyetlerinin kontrolünü sağlar
- Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlar
- Kişisel verilerin yok edilmesi geri dönüştürülemez ve denetim izi bırakmayacak şekilde sağlanır
- Kanun'un 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli veyahut kriptografik yöntemler ile korunur

10 İDARİ TEDBİRLER

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıdadır:

- Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgisine ve Kurul'a bildirir.
- Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar.
- Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.
- Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.

11 KİŞİSEL VERİLERİN SİLİNMESİ YÖNTEMLERİ

Kişisel veriler EK TABLO: 3'te belirtilen yöntemlerle silinir.

12 KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ

Kişisel veriler EK TABLO: 4'te belirtilen yöntemlerle yok edilir.

13 SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından kişisel verilerin saklama süresi belirlenirken; öncelikle yasal mevzuatta söz konusu kişisel verinin saklanması ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Bunun haricinde; EK TABLO: 5'te yer alan saklama ve imha süresi tablosu esas alınır.

14 PERİYODİK İMHA SÜRESİ

Şirket tarafından işlenen kişisel verilere ilişkin saklama süreleri belirlenirken öncelikle ilgili mevzuatta öngörülen süreler esas alınır. Mevzuatta süre öngörülmemiş olması halinde, kişisel veriler işlendikleri amaç için gerekli olan süre boyunca ve her hâlükârda Türk Borçlar Kanunu'nda öngörülen zamanaşımı süreleri gözetilerek saklanır.

Süreç bazında saklama süreleri işbu Politika'da, veri kategorisi bazında süreler VERBİS kaydında, kişisel veri bazında süreler ise Kişisel Veri İşleme Envanteri'nde yer almaktadır.

Saklama süresi sona eren kişisel veriler, ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.

Şirketin periyodik imha süresi 6 aydır. Saklama süresi dolan kişisel veriler, işbu Politikada belirtilen imha süreleri çerçevesinde, 6 aylık periyodlarla işbu Politika'da yer verilen usullere uygun olarak imha edilir. Söz konusu sistemlerde bilgilerin tekrar geri getirilmeyecek şekilde, verilerin kaydedildiği varsa evrak, dosya, CD, disket, hard disk gibi araçlardan geri dönüştürülmeyecek şekilde silinecektir.

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

Periyodik imha sürecinin takibi konusunda şirket verileri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak, süreç boyunca tüm idari ve teknik önlemleri almakla yükümlüdür.

Kayıt Türü	Açıklama	Saklama Süresi	İmha Süresi
Kimlik Bilgisi	Ad-soyad, T.C. kimlik no, doğum tarihi, uyruk vb.	10 yıl	İlk periyodik imhada
İletişim Bilgisi	Telefon, adres, e-posta vb.	10 yıl	İlk periyodik imhada
Finansal Bilgiler	Banka bilgileri, ödeme kayıtları, fatura verileri vb.	10 yıl	İlk periyodik imhada

Çalışan Özlük Dosyası	İş Sözleşmesi, izinler, bordro, performans kayıtları vb.	İş ilişkisi süresi +10 yıl	İlk periyodik imhada
İşe Alınmayan Aday Verileri	CV, başvuru formları vb.	2 yıl	İlk periyodik imhada
Sözleşmeler ve İletişimler	Tedarikçi, müşteri, iş ortağı sözleşmeleri	Sözleşme süresi + 10 yıl	İlk periyodik imhada
Alt İşveren/Tedarikçi Çalışan Bilgileri	SGK bildirimi, görev kayıtları vb	10 yıl	İlk periyodik imhada
CCTV Kayıtları	Kamera Görüntüleri	45 gün	İlk periyodik imhada
Görsel/İşitsel Verileri	Etkinlik fotoğrafı, tanıtım videosu vb.	5 yıl	İlk periyodik imhada
Ziyaretçi Kayıtları	Ziyaretçi giriş kayıtları	2 yıl	İlk periyodik imhada
İşlem Güvenliği Verileri	IP adresi, erişim logları, oturum kayıtları vb.	1 ay	İlk periyodik imhada
Hukuki İşlem ve Uyum Verileri	Dava dosyaları, icra kayıtları, resmi yazışmalar	10 yıl	İlk periyodik imhada
Talep / Şikayet Kayıtları	Müşteri talepleri, şikayet başvuruları	10 yıl	İlk periyodik imhada
Özel Nitelikli Kişisel Veriler	Sağlık verisi, biyometrik veri vb.	Mevzuatta öngörülen süre kadar ve amaçla sınırlı	İlk periyodik imhada
Araç Bilgileri (Plaka vb.)	Ziyaretçi veya çalışan araç bilgisi	5 yıl	İlk periyodik imhada
Müşteri İşlem Verileri	Kullanım kayıtları, hizmet talepleri	10 yıl	İlk periyodik imhada

15 POLİTİKANIN YAYIMLANMASI SAKLANMASI VE GÜNCELLENMESİ

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuoyuna ilan edilir. Basılı kâğıt nüshası şirket bünyesinde saklanır. Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümler güncellenir.

16 YÜRÜRLÜK

Politika, şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, politikanın ıslak imzalı eski nüshaları iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile şirket tarafından saklanır.

17 EKLER

EK TABLO 1 Saklama ve imha süreçleri görev dağılımı

UNVANI	BİRİMİ	GÖREVİ
Finans ve Operasyon Direktörü	Finans ve Operasyon	Komite Başkanı- yönetim ve iletişimden sorumlu
İnsan ve Kültür Direktörü	İnsan ve Kültür	KVKK Risk Yönetimi, Politika ve Prosedürlerden Sorumlu, iş süreçlerinin planlanması, raporlama sorumlusu
Bilgi Teknolojileri Müdürü	IT	Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
Diğer Tüm Birimler	İlgili Birimler	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

EK TABLO 2 Kişisel Veri Saklama Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Kişisel bilgisayarlar Mobil Cihazlar Optik diskler Yazıcılar, tarayıcılar, fotokopi makineleri Çıkarılabilir ve taşınabilir bellekler Sunucular Yazılımlar Bilgi güvenliği cihazları	Kağıtlar Yazılı ve basılı ortamlar Görsel kayıtlar Manuel veri kayıt sistemleri

EK TABLO 3 Kişisel Verilerin Silinmesi Yöntemleri

Veri Kayıt Ortamı	Silinme Yöntemi
Sunucular	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik ortam	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel ortam	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç

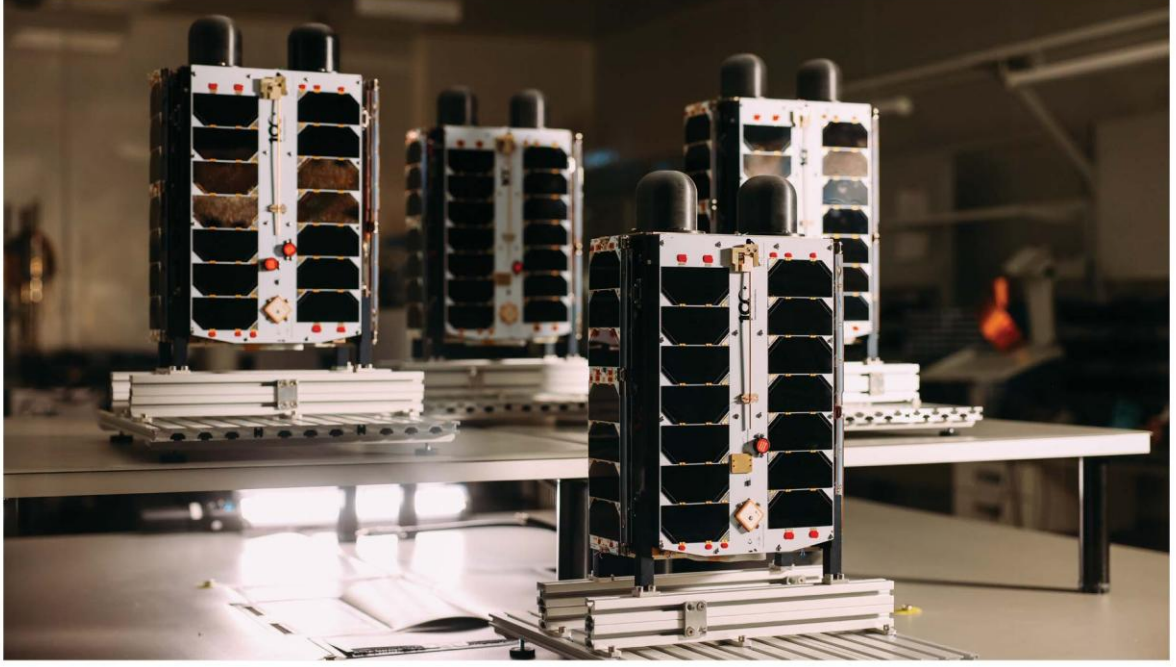
	diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir medya	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanması gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

EK TABLO 4 Kişisel Verilerin Yok Edilmesi Yöntemleri

Veri Kayıt Ortamı	Yok Edilme Yöntemi
Fiziksel ortam	Kâğıt ortamında yer alan kişisel verilerden saklanması gerektiren süre sona erenler, evrak imha makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik ya da manyetik medya	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanması gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir

EK TABLO 5 Saklama ve İmha Süresi Tablosu

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
İş sağlığı ve güvenliği uygulamalar	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Bordrolama	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Personel mahkeme/adliye taleplerinin cevaplandırılması	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Eğitim kayıtlarının dosyalanması	Eğitimin düzenlenmesinin ardından 10 yıl	Saklama süresinin bitimini takiben 180 gün
Acil durum hazırlıkları	Hazırlığın yapılmasını takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Log kayıt takip sistemleri	Oluşturulmasından itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün
Kamera kayıtları	Kaydedilmesinden itibaren 1 yıl	Saklama süresinin bitimini takiben 180 gün



www.plan.space • info@plan.space