VERIPARK KİŞİSEL VERİLERİN KORUNMASI SAKLANMASI VE İMHASI POLİTİKASI

Süreç No: VP-SEC-PL-04-01 Rev 0.1

Yayın ve Revizyon Tarihi: 04.04.2023

HAZIRLAYAN

Ad-Soyad	Pozisyon	İlk Rev. No/Tarih	İmza
Ece TÜRKMAN	Legal Counsel	00/22.03.2023	

SÜREÇ VE REVİZYON ONAY LİSTESİ

Ad-Soyad	Pozisyon	Rev. No/Tarih	İmza
Özkan ERENER	CEO	01/04.04.2023	

SÜREÇ DEĞİŞİKLİK TARİHÇESİ

Rev. No	Tarih	Değiştiren	Açıklama
00	22.03.2023	Ece TÜRKMAN	İlk Versiyon
01	04.04.2023	Gizem SURAV	Gözden geçirildi ve onaylandı

VERİPARK YAZILIM ANONİM ŞİRKETİ
KİŞİSEL VERİLERİN KORUNMASI, SAKLANMASI VE İMHASI POLİTİKASI

1 GİRİŞ

1.1 Amaç

VeriPark Yazılım Anonim Şirketi ("**Şirket**") Kişisel Verilerin Korunması, Saklanması ve İmhası Politikası ("**Politika**"), Şirket tarafından gerçekleştirilmekte olan kişisel veri işleme, saklama ve imha faaliyetlerine ilişkin olarak usul ve esasları belirlemek amacıyla hazırlanmıştır.

Şirket, iş faaliyetinin gerçekleştirilmesi amacıyla sözlü, yazılı veya elektronik ortamlar üzerinden topladığı kişisel verileri, Veri Sorumlusu sıfatıyla, hukuka uygun şekilde işlemektedir.

İşbu Politika kapsamında, Şirket'in kişisel veri işleme süreçleri ve kişisel veriler ile ilgili uygulamalar konusunda açıklamalar yer almakta ve bu vesileyle kişisel veriler hususunda şeffaflık sağlanması amaçlanmaktadır.

1.2 Kapsam

Şirket çalışanları, çalışan adayları, müşterileri, tedarikçileri, iş ortakları ve bunların çalışanları, yetkilileri ve müşterileri, ziyaretçiler ve kişisel verileri Şirket tarafından işlenen diğer üçüncü kişilerin kişisel verilerinin işlenmesi bu Politika kapsamında olup Şirket'in tüm kişisel veri işleme süreçlerine ve tüm kayıt ortamlarına ilişkin olarak bu Politika uygulanır.

1.3 Tanımlar

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
Kişisel veri:	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel veri envanteri:	Şirketin iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdığı envanter
Kişisel verileri işleme:	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 Korunması Kanunu:	7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanan 6698 sayılı Kanun ("**Kanun**")
Kişisel veri sahibi:	Kişisel verisi işlenen gerçek kişi
Kurul:	Kişisel Verileri Koruma Kurulu
Kurum:	Kişisel Verileri Koruma Kurumu
Özel nitelikli kişisel veri:	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler
Politika:	Kişisel Verilerin Korunması, Saklanması ve İmhası Politikası
Veri işleyen:	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri kayıt sistemi:	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri sorumlusu:	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi

2 SORUMLULUK VE GÖREV DAĞILIMI

Tüm Şirket birimleri ve çalışanları, sorumlu birim veya kişilerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak islenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birim veya kişilere aktif olarak destek verir.

İşbu Politika'nın uygulanması hususunda sorumlu olan veya görev alanların unvanları, birimleri ve görev tanımları aşağıdaki şekildedir:

Sorumlu	**Görev**

Yönetim Kurulu	Politika'nın onaylanması, yürütülmesi ve çalışanların Politika'ya uyumunun sağlanmasından sorumludur.
Kişisel Verilerin Korunması Komitesi ("Komite")	Politika'nın hazırlanması, yürütülmesi, ilgili ortamlarda yayımlanması, güncellenmesi ve Şirket veri işleme süreçlerinin Politika'ya uygunluğunun takip edilmesinden sorumludur. Komite'de Hukuk, Denetim ve Kalite Birimlerinden birer temsilci yer alır.
BT Birimi	Politika'nın uygulanması, özellikle teknik tedbirlerin uygulanmasından sorumludur.
Birim Yöneticileri	Politika'nın uygulanması ve yöneticisi oldukları çalışanların Politika'ya uyumunun sağlanmasından sorumludur.
Çalışanlar	Politika'ya uymaktan sorumludur.

3 KİŞİSEL VERİLERİN İŞLENMESİ

3.1 Kişisel Verilerin İşlenmesine İlişkin Genel İlkeler

Şirket, Kanun'un 4'üncü maddesi uyarınca ve kişisel verileri aşağıda yer alan ilkelere uygun olarak işlemektedir:

a. Hukuka ve dürüstlük kurallarına uygun olma.
b. Doğru ve gerektiğinde güncel olma.
c. Belirli, açık ve meşru amaçlar için işlenme.
ç. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
d. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

3.2 Kişisel Verilerin İşlenme Şartları

Kişisel veriler (özel nitelikli olmayan) aşağıdaki şartlardan birinin varlığı hâlinde, Şirket tarafından ilgili kişilerin açık rızası aranmaksızın işlenmektedir:

a. Kanunlarda açıkça öngörülmesi.
b. 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.
c. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
ç. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
d. İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
f. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Bu şartlar kapsamında olmayan hallerde kişisel veriler Şirket tarafından yalnızca ilgili kişilerin açık rızası alınarak işlenmektedir.

Özel nitelikli kişisel veriler ise aşağıdaki şartlardan birinin varlığı hâlinde, Şirket tarafından ilgili kişilerin açık rızası aranmaksızın işlenmektedir:

a. Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri bakımından; kanunlarda öngörülen hâllerde.
b. Sağlık ve cinsel hayata ilişkin kişisel veriler bakımından; ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından.

Bu şartlar kapsamında olmayan hallerde özel nitelikli kişisel veriler Şirket tarafından yalnızca ilgili kişilerin açık rızası alınarak işlenmektedir.

Şirket'in kişisel veri işleme süreçlerine ilişkin detaylar Kanun'un "Veri Sorumlusunun Aydınlatma Yükümlülüğü" başlıklı 10'uncu maddesi ile 10 Mart 2018 tarih ve 30356 sayılı Resmî Gazete'de yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ uyarınca Şirket tarafından hazırlanan Şirket Genel Aydınlatma Metni ve Çalışan Aydınlatma Metni kapsamında belirtilmektedir.

3.3. Kişisel Verilerin Yurt İçine ve Yurt Dışına Aktarılması

Yukarıdaki şartlar çerçevesinde kişiler veriler yurt içinde üçüncü kişilere aktarılabilecektir.

Kişisel veriler, iş süreçlerinin gerektirdiği hallerde KVKK'de belirlenen şartlara uygun olarak Grup Şirketleri, müşteriler ve iş ortakları başta olmak üzere yurt dışında bulunan üçüncü kişilere aktarılabilmektedir.

İş süreçlerinin gerektirdiği haller dışında kişisel veriler yurtdışına aktarılamaz. Kişisel verilerin yurt dışına aktarılacağı süreçler için Kişisel Verilerin Korunması Komitesi'nin bilgisi ve izni olması gerekmektedir.

Şirket'in kişisel veri aktarım süreçlerine ilişkin detaylar Kanun'un "Veri Sorumlusunun Aydınlatma Yükümlülüğü" başlıklı 10'uncu maddesi ile 10 Mart 2018 tarih ve 30356 sayılı Resmî Gazete'de yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ uyarınca Şirket tarafından hazırlanan Şirket Genel Aydınlatma Metni ve Çalışan Aydınlatma Metni kapsamında belirtilmektedir.

4 VERİ İHLAL BİLDİRİMİ

Kişisel veri ihlalleri, ihlal gerçekleşir gerçekleşmez Kişisel Verilerin Korunması Komitesi'ne (kvk@veripark.com) bildirilmelidir.

Söz konusu ihlal, Kişisel Verilerin Korunması Komitesi tarafından en geç 72 (yetmiş iki) saat içerisinde Kurul'a ve ihlalden etkilenen kişilere bildirilir.

5 KAYIT ORTAMLARI

Kişisel veriler, Şirket tarafından aşağıda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır:

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
- Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.) - Yazılımlar (ofis yazılımları, portal, ERP, CRM) - Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme uygulamaları, belirli süreli kayıt dosyaları, antivirüs programları vb.) - Kişisel veya kurumsal bilgisayarlar (masaüstü, dizüstü) - Mobil cihazlar (telefon, tablet vb.) - Optik diskler (CD, DVD vb.) - Taşınabilir depolama aygıtları (USB, hafıza kartı, hard disk vb.) - Yazıcı, tarayıcı, fotokopi makinesi	- Yazılı, basılı, fiziksel belgeler, kağıtlar - Manuel veri kayıt sistemleri (anket formları, ziyaretçi girişi defteri)

6 KİŞİSEL VERİLERİN GÜVENLİĞİNE İLİŞKİN TEDBİRLER

6.1 İdari Tedbirler

6.1.1 Risk ve Tehditlerin Belirlenmesi

Şirket faaliyetleri kapsamındaki kişisel veri işleme süreçlerinin belirlenmesi ve işlenmekte olan kişisel verilere ilişkin risk ve tehditlerin tespit edilmesi için "Kişisel Veri İşleme Envanteri" hazırlanmıştır. Bu envanter içerisinde yer alan kişisel veri işleme süreçleri Şirket tarafından güncel tutulacaktır.

Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında ve özel nitelikli kişisel veri güvenliğine yönelik Şirket politikaları hazırlanmış ve uygulanmaktadır. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmakta ve kişisel veri güvenliğinin takibi yapılmaktadır.

Şirket kişisel verilerin işlendiği süreçlere ve kişisel verilere ilişkin riskleri belirlerken, ilgili kişisel verilerin özel nitelikli olup olmadığını, gerektirdiği gizlilik seviyesini ve ortaya çıkabilecek bir güvenlik ihlali sonucunda oluşabilecek olumsuz sonuçları göz önünde bulundurur.

Şirket kişisel veri işleme süreçlerinin Kanun'a uygunluğunu periyodik olarak denetler.

6.1.2 Çalışanlara Eğitim Verilmesi ve Farkındalık Çalışmaları

Şirket, çalışanlarına kişisel verilerin korunması ve siber güvenlik konularında eğitimler verir ve bu konular ile ilgili farkındalık çalışmaları gerçekleştirir. Şirket içinde veya dışında kişisel veri ihtiva eden bir görev üstlendiğinde kendisine verilen bu görevi kişisel verilerin önemini de gözeterek özenle ve dikkatle yerine getirmesi beklenir.

Kişisel verilere ilişkin rol ve sorumluluklar, çalışanların iş tanımında açıkça belirlenir.

Şirket'in veri sorumlusu olduğu kişisel verilere ilişkin olarak çalışanlardan gizlilik taahhütleri alınmaktadır.

Çalışanların işbu Politika ile diğer politika ve prosedürlere uymalarının sağlanması için disiplin prosedürleri oluşturulmuştur.

6.1.3 Kişisel Verilerin Mümkün Olduğunca Azaltılması (Minimizasyonu) ve Erişimin Kısıtlanması

Kanun'da öngörülen "doğru ve gerektiğinde güncel olma", "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ve "işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkeleri doğrultusunda Şirket işlenmekte olan kişisel verileri periyodik olarak güncellemekte ve herhangi bir amaca hizmet etmeyen veya güncellenemeyen kişisel verileri silmekte, yok etmekte ya da anonim hale getirmektedir.

Yetkilendirme düzenlemeleri ile kişisel verilere yalnızca görmesi gereken birim ve kişilerin erişebilmesi sağlanmaktadır. Çalışanlar için yetki matrisi oluşturulmuştur. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

Silme, yok etme ve anonimleştirme ile ilgili prosedürlerin güncel tutulması ve sistemli olarak uygulanması sağlanmaktadır.

6.1.4 Bilgi Güvenliği ve Gizliliğe İlişkin Şirket Politika ve Prosedürleri

Çalışanlar, bilgi güvenliği ve gizliliğe ilişkin şirket politika ve prosedürlerine uymakla yükümlüdür.

Bu kapsamda, Çalışanlar Şirket nezdinde kullandıkları bilgisayar, kurumsal e-posta dahil fakat bunlarla sınırlı olmamak üzere her türlü elektronik cihazlara ve iletişim kanallarına ilişkin şifrelerini gizli tutmakla ve bunları diğer çalışanlar, tedarikçiler dahil hiç kimse ile paylaşmamakla yükümlüdür. Kişisel verilerin korunması için oluşturulan şifrelerin kolayca tahmin edilebilecek kelime veya cümlelerden oluşmaması gerekmektedir.

Şifreler, bilgi güvenliği politikalarından belirlenen kriterlere uygun olmalıdır. Şirket yazılımları, bu şekilde oluşturulan şifreler haricindeki şifrelere onay vermeyecek şekilde geliştirilmiştir.

Şifrenin unutulması halinde yeni şifre alınmasına ilişkin prosedürler izlenmelidir.

Çalışanların elektronik cihazları her zaman kilitli tutması gerekmektedir.

Şirket bilgisayarlarına yabancı yazılımların yüklenilmesine izin verilmemektedir.

6.1.5 Veri İşleyenler ile İlişkiler

Şirket, başta bilgi teknolojileri ile ilgili olmak üzere hizmet alacağı veri işleyenlerin bilgi güvenliğine en az Şirket kadar önem verdiklerinden ve sorumluluk bilinciyle hareket ettiklerinden emin olacak ve veri işleyenler ile akdedeceği sözleşmelerde bu bağlamda kişisel verilerin Kanun'a uygun olarak işlenmesi ve güvenliğine ilişkin düzenlemelere yer verecektir.

Veri işleyenler, Kanun'a uygun olarak yalnızca Şirket'in talimatları doğrultusunda, Şirket ile akdedilmiş sözleşme kapsamındaki yükümlülüklerinin yerine getirilmesi amacıyla kişisel verileri işleyebilecek ve sır saklama yükümlülüğü altında tutulacaktır.

Şirket "veri sorumlusu" olarak veri işleyenin kişisel verilerin işlendiği sistemleri üzerinde gerekli denetimleri yapacak veya yaptıracaktır.

6.2 Teknik Tedbirler

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Erişim logları düzenli olarak tutulmaktadır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Uygulamalar, işletim sistemleri dahil fakat bunlarla sınırlı olmamak üzere her türlü yazılım güncel tutulmaktadır. Özellikle güvenliği sağlayan yazılımlara ilişkin güncellemeler olması halinde bu güncellemeler makul bir süre içerisinde yapılmaktadır.
- Güncel antivirüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.

- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- Özel nitelikli kişisel veri içeren e-postalar mutlaka "*confidential*" veya "*private*" olarak işaretlenmelidir.
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişisel veriler şifrelenerek aktarılmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

7 İMHA PROSEDÜRLERİ

İlgili mevzuatta öngörülen süre ya da islendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Şirket tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak, Komisyon'un görüşü alınarak aşağıda belirtilen tekniklerle silinir, imha edilir veya anonim hale getirilir. İmhayı, ilgili kişisel verinin işlenme amacını gerçekleştiren departmandan bir kişi, tanık eşliğinde gerçekleştirir ve imhaya ilişkin olarak Kişisel Veri İmha Tutanağı ("Ek-1") söz konusu kişilerce imzalanarak kayıt altına alınır.

Dijital ve elektronik ortamlardaki kişisel verilerin imhasında aşağıdaki teknikler ve ilgili mevzuat hükümleri kapsamında "VP-SEC-PR-01 Digital Media Disposal Policy"de yer alan süreçler izlenir.

7.1 Kişisel Verilerin Silinmesi

Kayıt Ortamı	
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamlarda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamlarda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri

	okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Depolama Aygıtlarında Yer Alan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

7.2 Kişisel Verilerin Yok Edilmesi

Kayıt Ortamı	
Fiziksel Ortamlarda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik veya Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını 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.

7.3 Kişisel Verilerin Anonim Hale Getirilmesi

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

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

8 SAKLAMA VE İMHA

8.1 İmha Sebepleri

Aşağıdaki durumlarında, Şirket tarafından re'sen veya ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir:

- 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,
- Kanun'un 11'inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi veya kabul edilmemesi halinde şikâyet üzerine bu talebin Kurul tarafından uygun bulunması.

8.2 Saklama Süreleri

Süreç	**Saklama Süresi**	**İmha**
Müşteri, iş ortağı, tedarikçi sözleşme süreçleri	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan kaynakları süreçleri	İş sözleşmenin sona ermesini takiben 15 yıl Çalışan adayları için 1 yıl	
İşlem güvenliği süreçleri	1 yıl	
Kamera kayıtları	90 gün	

8.3 Periyodik İmha

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 11'inci maddesi gereğince periyodik imha süresini 6 ay olarak belirlenmiştir.

9 GÜNCELLEME VE DEĞİŞİKLİKLER

Politika, olağan olarak yılda bir defa gözden geçirilerek güncellenir. Ancak mevzuat değişiklikleri, uygulama değişiklikleri, Kişisel Verileri Koruma Kurulu'nun işlemleri ve/veya vereceği kararlar ile mahkeme kararları doğrultusunda Şirket bu Politika'yı her zaman gözden geçirebilecek ve gerekli durumlarda güncelleyecek veya değiştirecektir.

EK 1

VERİPARK YAZILIM ANONİM ŞİRKETİ
KİŞİSEL VERİ İMHA TUTANAĞI

İşbu İmha Tutanağı 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("Kanun") "Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi" başlıklı 7'nci maddesi ile 28 Ekim 2017 tarih ve 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca düzenlenmiştir.

İmha Tarihi	**:**
İmha Yeri	**:**
İmha Edilen Belge/ler (Kişisel veriler)	**:**
İmha Sebebi (Periyodik imha / ilgili kişi başvurusu / Kişisel Verileri Koruma Kurulu kararı / diğer)	**:**
İmha (Silme / Yok etme / Anonimleştirme) Yöntemi (Kağıt imha makinesi / yakma / dijital silme / diğer)	**:**

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

Yukarıda belirtilen belgeler/bilgiler geri döndürülemez şekilde imha edilmiştir.

İmha Eden	**Şahit**
Adı, Soyadı:	Adı, Soyadı:
İmza:	İmza: