

Kişisel Veri Saklama ve İmha Politikası

OTOVİM TEKNOLOJİ A.Ş. · Yürürlük tarihi: 26.10.2026 · Sürüm 2 · Kanıt: b0b2fb2bf7da3281...

YEDEKNOKTA.COM

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

MADDE 1 - AMAÇ

İşbu Kişisel Veri Saklama ve İmha Politikası'nın ("Politika") amacı; OTOVİM Teknoloji Anonim Şirketi ("Yedeknokta") tarafından işlenen kişisel verilerin;

- hangi esaslarla saklanacağını,
- saklama sürelerinin nasıl belirleneceğini,
- işleme şartlarının ortadan kalkması halinde hangi yöntemlerle silineceğini, yok edileceğini veya anonim hale getirileceğini,
- periyodik imha süreçlerinin nasıl yürütüleceğini,
- ilgili birimlerin görev ve sorumluluklarını

belirlemektir.

MADDE 2 - KAPSAM

İşbu Politika;

- kullanıcılar,
- üyeler,
- alıcılar,
- satıcılar ve satıcı adayları,
- ziyaretçiler,
- çalışanlar ve çalışan adayları,
- tedarikçiler,
- iş ortakları,
- yetkili kişiler,
- diğer ilgili kişiler

hakkında Yedeknokta tarafından tamamen veya kısmen otomatik yollarla ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verileri kapsar.

MADDE 3 - DAYANAK VE İLGİLİ DOKÜMANLAR

İşbu Politika;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin uygulanabilir mevzuat,
- Yedeknokta Kişisel Verilerin Korunması Aydınlatma ve Gizlilik Metni,
- Veri İşleme Envanteri,
- Bilgi Güvenliği ve Kişisel Veri Güvenliği Politikası,
- Veri İhlali Müdahale düzenlemeleri

ile birlikte uygulanır.

MADDE 4 - TANIMLAR

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Özel Nitelikli Kişisel Veri: İlgili mevzuat kapsamında özel koruma öngörülen kişisel veri kategorilerini,

İlgili Kişi: Kişisel verisi işlenen gerçek kişiyi,

Veri Sorumlusu: Kişisel verilerin işleme amaç ve vasıtalarını belirleyen Yedeknokta'yı,

Saklama: Kişisel verilerin belirli sürelerle muhafaza edilmesini,

Silme: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesini,

Yok Etme: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesini,

Anonim Hale Getirme: Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

Periyodik İmha: Kişisel verilerin işlenmesini gerektiren şartların tamamının ortadan kalkması halinde belirli aralıklarla gerçekleştirilen silme, yok etme veya anonim hale getirme işlemini, ifade eder.

MADDE 5 - TEMEL İLKELER

Kişisel verilerin saklanması ve imhasında aşağıdaki ilkeler esas alınır:

1. Hukuka ve dürüstlük kurallarına uygunluk,
2. Doğruluk ve güncellik,
3. Belirli, açık ve meşru amaçlarla işleme,

4. İşleme amacıyla bağlantılı, sınırlı ve ölçülü olma,
5. Gereğinden uzun süre saklamama,
6. Güvenli saklama,
7. Yetkisiz erişimi önleme,
8. Saklama süresi sona erdiğinde uygun imha yöntemini uygulama,
9. Yapılan imha işlemlerini kayıt altına alma,
10. Kişisel verilerin yalnızca görev gereği erişmesi gereken kişilerce erişilebilir olmasını sağlama.

MADDE 6 - KİŞİSEL VERİLERİN SAKLANMA SEBEPLERİ

Kişisel veriler, somut veri işleme faaliyetinin niteliğine göre aşağıdaki nedenlerle saklanabilir:

- sözleşmenin kurulması veya ifası,
- üyelik ve hesap yönetimi,
- sipariş ve teslimat işlemleri,
- satıcı ilişkilerinin yürütülmesi,
- faturalama ve muhasebe,
- ödeme ve hakediş işlemleri,
- tüketici taleplerinin yönetilmesi,
- hukuki uyumazlıkların yürütülmesi,
- mevzuattan doğan saklama yükümlülüklerinin yerine getirilmesi,
- bilgi ve işlem güvenliğinin sağlanması,
- dolandırıcılık ve kötüye kullanımın önlenmesi,
- bir hakkın tesisi, kullanılması veya korunması,
- gerekli hukuki şartların bulunması halinde pazarlama ve iletişim süreçlerinin yürütülmesi.

MADDE 7 - SAKLAMA SÜRELERİNİN BELİRLENMESİ

Her kişisel veri kategorisi için saklama süresi;

- ilgili mevzuatta öngörülen süre,
- sözleşme ilişkisinin devamı,
- zamanaşımı ve hak düşürücü süreler,
- hukuki uyumazlık ihtimali,
- veri işleme amacı,
- ilgili kişinin makul beklentileri,

- veri güvenliği riski

dikkate alınarak belirlenir.

Kişisel veri, yalnızca “ileride gerekebilir” gerekçesiyle belirsiz süreyle saklanamaz.

MADDE 8 - SAKLAMA SÜRESİNİN BAŞLANGICI

Saklama süresinin başlangıcı veri kategorisine göre;

- verinin ilk elde edildiği tarih,
- üyeliğin sona erdiği tarih,
- siparişin tamamlandığı tarih,
- sözleşmenin sona erdiği tarih,
- hukuki uyumsuzluğun kesin olarak sona erdiği tarih,
- çalışan ilişkisinin sona erdiği tarih,
- ilgili işlemin tamamlandığı tarih

esas alınarak belirlenebilir.

MADDE 9 - SAKLAMA SÜRESİNİN SONA ERMESİ

Bir kişisel verinin işlenmesini gerektiren hukuki ve fiili sebepler ortadan kalktığında;

- başka bir kanuni saklama yükümlülüğü bulunup bulunmadığı,
- devam eden bir hukuki uyumsuzluk olup olmadığı,
- bir hakkın tesisi, kullanılması veya korunması için saklamanın gerekli olup olmadığı

kontrol edilir.

Saklamayı gerektiren başka bir hukuki neden bulunmaması halinde veri silinir, yok edilir veya anonim hale getirilir.

MADDE 10 - KİŞİSEL VERİ SAKLAMA SÜRELERİ TABLOSU

Aşağıdaki tablo, Veri İşleme Envanteri ile uyumlu olarak her veri kategorisi bakımından azami saklama süresini, süre başlangıcını ve süre sonunda uygulanacak imha yöntemini gösterecek şekilde doldurulur; mevzuat, faaliyet veya sistem değişiklikleri üzerine derhal güncellenir.

Veri / Süreç	İlgili Kişi	Saklama Nedeni	Saklama Süresi	Süre Başlangıcı	Süre Sonunda İşlem
--------------	-------------	----------------	----------------	-----------------	--------------------

Üyelik bilgileri	Kullanıcı	Üyelik ilişkisi / hukuki yükümlülük	[●]	Üyeliğin sona ermesi	Silme/Yok etme/Anonimleştirme
Sipariş kayıtları	Alıcı	Sözleşme / mali yükümlülük	[●]	Siparişin tamamlanması	[●]
Fatura ve muhasebe kayıtları	Alıcı/Satıcı	Vergi ve mali mevzuat	[●]	İlgili mali dönem	[●]
Satıcı sözleşmeleri	Satıcı	Sözleşme / hakların korunması	[●]	Sözleşmenin sona ermesi	[●]
Satıcı doğrulama kayıtları	Satıcı	Güvenlik / mevzuat	[●]	İlişkinin sona ermesi	[●]
Ödeme kayıtları	Alıcı/Satıcı	Finans ve uyumsuzluk	[●]	İşlem tarihi	[●]
Müşteri hizmetleri kayıtları	Kullanıcı	Talep ve şikayet yönetimi	[●]	Talebin kapanması	[●]
İade/şikayet kayıtları	Alıcı	Tüketici süreçleri	[●]	Sürecin kapanması	[●]
Sistem/log kayıtları	Kullanıcı/Satıcı	Bilgi güvenliği	[●]	Kayıt tarihi	[●]
Ticari ileti onay/ret kayıtları	Kullanıcı	Mevzuat / ispat	[●]	Onay/ret tarihi	[●]

KVKK başvuru kayıtları	İlgili kişi	Hukuki yükümlölük	[●]	Başvurunun sonuçlanması	[●]
Çalışan verileri	Çalışan	İş ilişkisi / mevzuat	[●]	İş ilişkisinin sona ermesi	[●]
Çalışan aday verileri	Aday	İşe alım süreci	[●]	Sürecin kapanması	[●]
Tedarikçi kayıtları	Tedarikçi	Ticari ilişki	[●]	Sözleşmenin sona ermesi	[●]
Hukuki uyuşmazlık dosyaları	İlgili kişi	Hakların korunması	[●]	Uyuşmazlığın kesin sona ermesi	[●]

MADDE 11 - VERİLERİN SAKLANDIĞI ORTAMLAR

Kişisel veriler aşağıdaki ortamlarda saklanabilir:

Elektronik Ortamlar

- sunucular,
- bulut sistemleri,
- veri tabanları,
- CRM sistemleri,
- e-posta sistemleri,
- muhasebe sistemleri,
- müşteri hizmetleri sistemleri,
- log sistemleri,
- yedekleme sistemleri,
- çalışan cihazları,
- yetkili üçüncü taraf hizmet sağlayıcı sistemleri.

Fiziksel Ortamlar

- sözleşme dosyaları,

- personel dosyaları,
- arşiv klasörleri,
- basılı başvuru ve bildirimler.

MADDE 12 - SAKLAMA ORTAMLARININ GÜVENLİĞİ

Elektronik ve fiziksel saklama ortamlarında uygun teknik ve idari tedbirler uygulanır.

Özellikle;

- rol bazlı erişim,
- güçlü kimlik doğrulama,
- şifreleme,
- loglama,
- yedekleme,
- antivirüs ve güvenlik yazılımları,
- fiziksel arşiv erişim kontrolü,
- erişim yetkilerinin düzenli gözden geçirilmesi

uygulanır.

MADDE 13 - SİLME YÖNTEMLERİ

Kişisel verilerin silinmesi gerektiğinde, veriler ilgili kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

Silme yöntemleri veri ortamına göre değişebilir.

Örneğin:

- kullanıcı hesabından erişimin kaldırılması,
- veri tabanı kayıtlarının erişime kapatılması,
- uygulama kullanıcılarının erişim yetkisinin kaldırılması,
- dosyanın aktif sistemlerden silinmesi,
- ilgili kayıtların yalnızca zorunlu saklama erişimine alınması.

Silinen veriye sistem yöneticisi veya özel yetkili kullanıcıların teknik zorunluluk nedeniyle sınırlı erişimi bulunuyorsa bu erişim ayrıca korunur ve amacı dışında kullanılamaz.

MADDE 14 - YOK ETME YÖNTEMLERİ

Kişisel verilerin yok edilmesinde verinin tekrar elde edilmesini teknik olarak engelleyen yöntemler uygulanır.

Elektronik veriler bakımından örneğin;

- güvenli silme,
- üzerine yazma,
- kriptografik silme,
- veri taşıyıcının fiziksel olarak imha edilmesi

yöntemleri kullanılabilir.

Fiziksel evrak bakımından;

- kağıt öğütücü,
- güvenli imha hizmeti,
- geri döndürülemez fiziksel imha

yöntemleri kullanılabilir.

MADDE 15 - ANONİMLEŞTİRME

Kişisel veriler, işleme amacı bakımından kişiyi tanımlamaya artık ihtiyaç bulunmaması ancak istatistiksel veya analitik değerin korunmasının gerekli olması halinde anonim hale getirilebilir.

Anonimleştirme sonucunda verinin, başka verilerle eşleştirilmesi dahil olmak üzere, kimliği belirli veya belirlenebilir gerçek kişiyle ilişkilendirilememesi gerekir.

MADDE 16 - ANONİMLEŞTİRME YÖNTEMLERİ

Verinin niteliğine göre örneğin;

- toplulaştırma,
- genelleştirme,
- maskeleyme,
- kategorileştirme,
- veri azaltma,
- değişken çıkarma,
- istatistiksel yöntemler

kullanılabilir.

Uygulanan yöntem sonucunda, kayıt ortamı ve faaliyet alanı bakımından uygun teknikler kullanılsa dahi verinin kimliği belirli veya belirlenebilir bir gerçek kişiyle yeniden ilişkilendirilememesi gerekir.

MADDE 17 - TAKMA ADLANDIRMA İLE ANONİMLEŐTİRMENİN AYRIMI

Bir veri setindeki doğrudan tanımlayıcıların kodla değıştirilmesi veya takma adlandırılması, tek başına verinin anonim hale geldiğı anlamına gelmez.

Ek bilgi kullanılarak kişinin yeniden belirlenebilmesi mümkünse veri kişisel veri niteliğini korur.

MADDE 18 - PERİYODİK İMHA

Kişisel verilerin işlenmesini gerektiren şartların tamamı ortadan kalktığında, veriler belirlenen periyodik imha dönemlerinde silinir, yok edilir veya anonim hale getirilir.

Periyodik imha aralığı:

6 AY

olarak belirlenir.

Periyodik imha, işleme şartlarının ortadan kalktığı tarihi takip eden ilk periyodik imha işleminde gerçekleştirilir.

MADDE 19 - PERİYODİK İMHA TAKVİMİ

Periyodik imha süreci aşağıdaki takvim uyarınca yürütölür:

Ocak ve Temmuz: Saklama süresi dolan kayıtların belirlenmesi Takip eden ay: İlgili birim ve Hukuk/Uyum kontrolü Takip eden ayın son iş günü: İmha işlemlerinin gerçekleştirilme ve kayıt altına alınması

Takvimdeki değışiklikler, altı aylık azami periyodik imha aralığı aşılmamak kaydıyla Hukuk/Uyum ve Bilgi Teknolojileri tarafından kayıt altına alınır.

Her periyotta yapılacak işlemler ayrıca kayıt altına alınır.

MADDE 20 - İLGİLİ KİŐİ TALEBİ ÜZERİNE İMHA

İlgili kişinin kişisel verilerinin silinmesi veya yok edilmesi yönünde başvuruda bulunması halinde;

1. Talebin kimlik doğrulaması yapılır.
2. İlgili veri kategorileri belirlenir.
3. Veri işleme şartlarının devam edip etmediğı incelenir.
4. Saklama yükümlölüğü varsa ilgili kişiye gerekçesi açıklanır.
5. Saklama şartı kalmamışsa uygun imha işlemi gerçekleştirilir; talebe konu veriler üçüncü kişilere aktarılmışsa bu durum ilgili üçüncü kişilere bildirilir ve gerekli işlemlerin

yapılması temin edilir.

6. Başvuru sonucu, talebin alınmasından itibaren en geç otuz gün içinde ilgili kişiye yazılı veya elektronik ortamda bildirilir.

MADDE 21 - KANUNİ SAKLAMA YÜKÜMLÜLÜĞÜ BULUNAN VERİLER

İlgili kişinin silme talebinde bulunması, başka bir kanun gereği saklanması zorunlu olan verilerin derhal yok edilmesini gerektirmez.

Bu durumda veri;

- yalnızca kanuni saklama amacıyla,
- erişimi sınırlandırılmış biçimde,
- yeni amaçlarla kullanılmaksızın

saklanmaya devam edebilir.

MADDE 22 - HUKUKİ UYUŞMAZLIK BULUNAN VERİLER

Devam eden;

- dava,
- icra,
- arabuluculuk,
- idari inceleme,
- tüketici uyuşmazlığı,
- sözleşmesel talep

bulunması halinde ilgili kişisel veriler, bir hakkın tesisi, kullanılması veya korunması için gerekli olduğu süre boyunca muhafaza edilebilir.

Uyuşmazlığın sona ermesinden sonra saklama ihtiyacı yeniden değerlendirilir.

MADDE 23 - YEDEKLERDE BULUNAN VERİLER

Aktif sistemlerden silinen kişisel verilerin teknik yedeklerde belirli sürelerle bulunması mümkündür.

Yedeklerde bulunan veriler;

- olağan operasyon için yeniden kullanılamaz,
- yalnızca felaket kurtarma ve iş sürekliliği amacıyla erişilebilir,

- yalnızca tanımlı yedekleme saklama süresinin sonunda, geri yükleme erişimi kapatılarak otomatik veya kontrollü şekilde silinir ya da yok edilir.

Bir yedeğin geri yüklenmesi halinde daha önce silinmiş verilerin yeniden aktif sisteme alınmasını önleyecek gerekli kontroller uygulanır.

MADDE 24 - ÜÇÜNCÜ TARAF HİZMET SAĞLAYICILAR

Kişisel verilerin veri işleyen veya diğer hizmet sağlayıcılarda tutulduğu durumlarda, saklama ve imha gereklilikleri ilgili sözleşmelere yansıtılır.

Sözleşme sona erdiğinde hizmet sağlayıcıdan;

- verilerin iadesi,
- silinmesi,
- yok edilmesi,
- yedeklerden kaldırılması

konusunda sözleşmede belirlenen süre ve usule uygun olarak işlem yapılması istenir; işlemin tamamlandığı yazılı olarak teyit edilir.

MADDE 25 - YURT DIŞINDA SAKLANAN VERİLER

Kişisel verilerin yurt dışındaki sistemlerde saklanması halinde;

- veri aktarımının hukuki dayanağı,
- saklama süresi,
- hizmet sağlayıcının imha uygulamaları,
- yedekleme yapısı

ayrıca değerlendirilir.

MADDE 26 - ÖZEL NİTELİKLİ KİŞİSEL VERİLER

Özel nitelikli kişisel veriler işleniyorsa;

- erişim yetkileri kişi, rol, kapsam ve süre bakımından yazılı olarak tanımlanır ve düzenli olarak gözden geçirilir,
- veriler kriptografik yöntemlerle korunur; işlem hareketleri güvenli biçimde loglanır ve uzaktan erişimde en az iki kademeli kimlik doğrulama uygulanır,
- gereksiz kopyalama engellenir; görev değişikliği veya işten ayrılma hâlinde erişim yetkileri derhal kaldırılır,
- imha işlemi daha kontrollü yürütülür.

MADDE 27 - ÇALIŞAN DOSYALARI

Çalışan ve eski çalışanlara ilişkin kişisel veriler;

- iş mevzuatı,
- sosyal güvenlik,
- ücret ve bordro,
- iş sağlığı ve güvenliği,
- hukuki uyuşmazlıklar,
- şirket varlıklarının teslimi

gibi amaçlar bakımından uygulanabilir saklama süreleri dikkate alınarak muhafaza edilir.

Çalışan dosyalarındaki her belgenin aynı süreyle saklanması zorunlu değildir.

MADDE 28 - ÇALIŞAN ADAYI VERİLERİ

İşe alınmayan adaylara ilişkin kişisel veriler, işe alım süreci sona erdikten sonra devam eden meşru bir işleme sebebi bulunmuyorsa silinir veya yok edilir.

Adayın gelecekteki pozisyonlar için ayrıca değerlendirilmesi isteniyorsa bu işlem için uygun hukuki işleme şartı ayrıca belirlenir.

MADDE 29 - ÜYELİĞİ KAPATILAN KULLANICILAR

Üyeliğin sona ermesiyle;

- pazarlama amaçlı aktif profil kullanımı sona erdirilir,
- üyelik nedeniyle tutulması gerekmeyen veriler imha sürecine alınır,
- ancak sipariş, fatura ve hukuki işlem kayıtları gerekli sürelerle saklanabilir.

MADDE 30 - SATICI HESABI KAPATILDIĞINDA

Satıcı mağazasının kapatılması halinde;

- ticari işlem kayıtları,
- fatura ve hakediş kayıtları,
- tüketici uyuşmazlıkları,
- sahte ürün veya güvenlik incelemeleri,
- hukuki talepler

için gerekli veriler ilgili sürelerle saklanabilir.

Artık işlenmesine gerek bulunmayan doğrulama ve operasyon verileri imha programına alınır.

MADDE 31 - LOG KAYITLARI

Log kayıtlarının saklama süresi;

- bilgi güvenliği,
- olay inceleme,
- yasal yükümlülük,
- sistem bütünlüğü

amaçları dikkate alınarak belirlenir.

Log kayıtlarının gereğinden uzun süre tutulmaması esastır.

MADDE 32 - TİCARİ İLETİ ONAY VE RET KAYITLARI

Ticari elektronik ileti onayı veya ret kayıtları, ilgili elektronik ticaret mevzuatı ve ispat ihtiyacı dikkate alınarak saklanır.

Ret talebi sonrasında aktif pazarlama listelerinde ilgili iletişim adresinin kullanılmaması sağlanır.

MADDE 33 - İMHA İŞLEMİNİN KAYIT ALTINA ALINMASI

Gerçekleştirilen silme, yok etme ve anonimleştirme işlemleri kayıt altına alınır.

İmha kaydında asgari olarak;

- veri kategorisi,
- imha yöntemi,
- imha tarihi,
- işlemi gerçekleştiren birim,
- onaylayan kişi,
- imha gerekçesi

yer alır.

MADDE 34 - İMHA KAYITLARININ SAKLANMASI

İmha işlemlerine ilişkin kayıtlar, diğer hukuki yükümlülükler saklı kalmak kaydıyla en az üç yıl süreyle saklanır.

Bu kayıtların kendisi kişisel veri içeriyorsa ilgili güvenlik tedbirlerine tabi tutulur.

MADDE 35 - SORUMLU BİRİMLER

Hukuk/Uyum

- saklama sürelerinin hukuki dayanaklarını değerlendirir,
- mevzuat değişikliklerini takip eder,
- ilgili kişi silme taleplerini değerlendirir.

Bilgi Teknolojileri

- elektronik imha işlemlerini gerçekleştirir,
- yedek ve erişim sistemlerini yönetir,
- teknik imha kayıtlarını tutar.

İnsan Kaynakları

- çalışan ve aday verilerinin saklama sürelerini takip eder.

Finans/Muhasebe

- mali kayıtların yasal saklama sürelerini takip eder.

Operasyon

- kullanıcı ve Satıcı işlem verilerinin operasyonel gerekliliğini takip eder.

MADDE 36 - VERİ SAHİBİ BİRİMLERİN SORUMLULUĞU

Her birim kendi sisteminde bulunan kişisel veriler bakımından;

- gereksiz veri tutmamak,
- saklama süresi dolan verileri bildirmek,
- kopya dosyaları azaltmak,
- yerel cihazlarda kontrolsüz veri bulundurmamak

ile sorumludur.

MADDE 37 - YETKİLENDİRME

Silme veya imha işlemleri yalnızca yetkili personel tarafından gerçekleştirilir.

Kritik veri setlerinde;

- işlemi başlatan,

- kontrol eden,
- onaylayan

kişiler arasında görevler ayrılığı uygulanır; teknik veya organizasyonel olarak bunun mümkün olmadığı hâllerde işlem, yetkili ikinci kişi tarafından sonradan kontrol edilerek kayıt altına alınır.

MADDE 38 - VERİ İMHA TALEP FORMU

Bir birim tarafından veri imhası talep edildiğinde aşağıdaki bilgiler kaydedilebilir:

Veri Kategorisi: [●]

Sistem/Dosya: [●]

İlgili Kişi Grubu: [●]

Saklama Süresi: [●]

Saklama Süresi Doldu mu?: [●]

Devam Eden Hukuki Sebep Var mı?: [●]

Önerilen İşlem: Silme / Yok Etme / Anonimleştirme

Talep Eden: [●]

Hukuk/Uyum Kontrolü: [●]

İşlem Tarihi: [●]

İşlemi Yapan: [●]

MADDE 39 - PERİYODİK İMHA KONTROL LİSTESİ

- Saklama süresi dolan veri setleri belirlendi.
- Devam eden hukuki yükümlülükler kontrol edildi.
- Açık uyumsuzluklar kontrol edildi.
- İlgili iş biriminin görüşü alındı.
- İmha yöntemi belirlendi.
- Aktif sistemler kontrol edildi.
- Yedekleme sistemi değerlendirildi.
- Üçüncü taraf hizmet sağlayıcılar kontrol edildi.
- İmha işlemi gerçekleştirildi.
- İmha kaydı oluşturuldu.
- Yetkili onayı tamamlandı.

MADDE 40 - VERİ SAKLAMA ENVANTERİNİN GÖZDEN GEÇİRİLMESİ

Saklama süreleri tablosu yılda en az bir kez ve ayrıca;

- yeni veri işleme faaliyeti,
- yeni mevzuat,
- yeni sistem,
- yeni tedarikçi,
- faaliyet modelinde esaslı değişiklik

olması halinde gözden geçirilir.

MADDE 41 - YENİ SİSTEMLERDE SAKLAMA SÜRESİ

Yeni bir yazılım veya veri tabanı kullanılmaya başlanmadan önce mümkün olduğu ölçüde;

- hangi kişisel verilerin tutulacağı,
- saklama süresi,
- otomatik silme fonksiyonu,
- yedekleme yapısı,
- erişim yetkileri

belirlenir.

Saklama süresinin sonradan manuel olarak takip edilmesine ihtiyaç bırakmayacak otomatik mekanizmalar tercih edilir.

MADDE 42 - GEREKSİZ KOPYALAR

Aynı kişisel verinin;

- e-posta,
- masaüstü,
- ortak klasör,
- mesajlaşma sistemi,
- taşınabilir bellek

gibi farklı ortamlarda gereksiz kopyalarının oluşturulmasından kaçınılır.

İmha işlemi yapılırken bilinen kopyalar da kapsam dahilinde değerlendirilir.

MADDE 43 - VERİ TAŞIYICILARININ ELDEN ÇIKARILMASI

Bilgisayar, disk, telefon veya diğer veri taşıyıcılar;

- satılmadan,
- devredilmeden,

- hurdaya ayrılmadan

önce üzerindeki kişisel verilerin geri getirilemeyecek şekilde temizlenmesi sağlanır.

MADDE 44 - FİZİKSEL ARŞİVLER

Fiziksel kişisel veri içeren evrak;

- kilitli ve kontrollü alanlarda saklanır,
- yetkisiz kişilerce erişilemez,
- saklama süresi dolduğunda güvenli şekilde imha edilir.

Normal çöp kutusuna atılmak suretiyle imha yapılmaz.

MADDE 45 - İMHA HİZMETİ ALINMASI

Üçüncü kişiden fiziksel veya elektronik imha hizmeti alınması halinde;

- hizmet sağlayıcının güvenilirliği,
- gizlilik yükümlülüğü,
- veri güvenliği tedbirleri,
- imhanın doğrulanabilirliği

kontrol edilir.

Gerekli görülürse imha tutanağı veya sertifikası alınır.

MADDE 46 - DENETİM

Politikanın uygulanması iç denetim veya uyum kontrolleri kapsamında incelenebilir.

Denetimde özellikle;

- süresi dolmuş veri bulunup bulunmadığı,
- imha kayıtlarının mevcut olup olmadığı,
- birimlerin yerel kopyaları,
- yedekleme sistemleri,
- erişim yetkileri

kontrol edilir.

MADDE 47 - UYGUNSUZLUKLAR

Aşağıdaki durumlar uygunsuzluk olarak değerlendirilir:

- saklama süresi dolmuş verinin sebepsiz tutulması,

- imha kayıtlarının bulunmaması,
- kişisel verinin güvenli olmayan yöntemle silinmesi,
- yetkisiz personelin imha işlemi yapması,
- anonim hale getirildiği belirtilen verinin kolaylıkla yeniden kimliklendirilebilir olması.

Tespit edilen uygunsuzluklar için düzeltici tedbir alınır.

MADDE 48 - EĞİTİM

Kişisel veri işleyen personele;

- saklama süreleri,
- veri minimizasyonu,
- silme ve imha yöntemleri,
- gereksiz kopya oluşturulmaması,
- fiziksel belge güvenliği

konularında gerekli eğitim verilir.

MADDE 49 - POLİTİKANIN GÜNCELLENMESİ

İşbu Politika;

- mevzuat değişiklikleri,
- veri işleme faaliyetlerindeki değişiklikler,
- yeni teknoloji veya sistem kullanımı,
- denetim sonuçları

dikkate alınarak güncellenir.

MADDE 50 - YÜRÜRLÜK

İşbu Kişisel Veri Saklama ve İmha Politikası [●] tarihinde yürürlüğe girer.

Doküman Sahibi: [●]

Onaylayan: [●]

Versiyon: 1.0

Yürürlük Tarihi: [●]

Son Gözden Geçirme Tarihi: [●]