



Kişisel Verileri Saklama ve İmha Prosedürü

INTER PARTNER ASSISTANCE YARDIM VE
DESTEK HİZMETLERİ TİC. A.Ş.

AXA Partners Türkiye

Kısıklı Mah. Bosna Bulvarı No: 39 34692 Üsküdar / İstanbul
Tel: 0 216 524 36 36 | Faks: 0 216 524 36 37
info@ipaistanbul.com



İÇİNDEKİLER

1.	AMAÇ.....	3
2.	KAPSAM.....	3
3.	TANIMLAR.....	3
4.	SORUMLULUKLAR.....	4
5.	KİŞİSEL VERİLERİN SAKLANMASI.....	5
6.	SAKLAMA VE İMHA SÜRELERİ.....	6
7.	SAKLAMA USULLERİ VE TEDBİRLER.....	8
8.	KİŞİSEL VERİLERİ SİLME, İMHA ETME VE ANONİMLEŞTİRME USULLERİ.....	10
9.	YÜRÜRLÜK VE GÜNCELLENME.....	11

1. AMAÇ

İşbu prosedürün amacı 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'e uygun olarak Inter Partner Assistance Yardım ve Destek Hizmetleri Tic. A.Ş'nin ('Şirket') kişisel verilerin saklanması, silinmesi, yok edilmesi veya anonim hale getirilmesi ilişkin yükümlülüklerin Şirket içerisinde ve/veya Şirket tarafından uyulması gereken yöntem ve esasları belirlemektedir.

2. KAPSAM

Bu Prosedür, görevleri kapsamında Kişisel Verileri tamamen veya kısmen otomatik yol ve araçlarla işleyen ya da bir kayıt sisteminin bir parçasını oluşturan ya da bir kayıt sisteminin bir parçasını oluşturması amaçlanan Kişisel Verileri başka yol ve araçlarla işleyen tüm Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin işlenmesi faaliyetlerine ilişkin olarak uygulanır.

3. TANIMLAR

İşbu Politikada geçen tanımlar aşağıdaki anlamları ihtiva eder;

"Kişisel Veri" Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder

"KVKK" 6698 sayılı Kişisel Verilerin Korunması Kanununu ifade eder.

"Kişisel Veri İşleme" 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 veri üzerinde yapılan her türlü işlemi ifade eder.

"Açık Rıza" Belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.

"Elektronik Ortam" Kişisel Verilerin elektronik cihazlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamları ifade eder.

"Kurul" Kişisel Verileri Koruma Kurulunu ifade eder.

“Anonim Hale Getirme” Kişisel Verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder.

“İmha Etme” Kişisel Verilerin geri döndürülemez biçimde yok edilmesini ifade eder.

“Silme” Kişisel Verilerin geri döndürülemez biçimde temizlenmesi yahut ilgili kullanıcılar için erişilemez hale getirmeyi ifade eder.

4. SORUMLULUKLAR

- 4.1. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi Şirket tarafından bu prosedürde belirtilen teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kişisel Verileri Koruma Kurulu (“Kurul”) kararlarına uygun olarak gerçekleştirilir.
- 4.2. Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri re’sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı Şirket tarafından seçilmektedir. Ancak, ilgili Kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilecektir.
- 4.3. Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Şirket tarafından kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere işbu prosedürde açıklanan sürelerle saklanmaktadır.
- 4.4. Şirket’in faaliyetleri için Kişisel Verileri elinde tutmamasını ve Kişisel Verilerin silinmesi ve/veya arşivlenmesini sağlamak tüm çalışanların ve Veri İrtibat kişisinin sorumluluğudur.
- 4.5. Kanun’un 5. ve 6. maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Şirket tarafından periyodik imha zamanlarında re’sen veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu hususta İlgili Kişi tarafından Şirket’e başvurulması halinde;
 - 4.5.1. İletilen talepler en geç 30 (otuz) gün içerisinde sonuçlandırılmakta ve ilgili kişiye bilgi verilmektedir,
 - 4.5.2. Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilmekte ve üçüncü kişiler nezdinde gerekli işlemlerin

yapılması temin edilmektedir.

5. KİŞİSEL VERİLERİN SAKLANMASI

- 5.1. Veri Sahiplerine ait kişisel veriler, Şirket tarafından özellikle (i) ticari faaliyetlerin sürdürülebilmesi, (ii) hukuki yükümlülüklerin yerine getirilebilmesi, (iii) çalışan haklarının ve yan haklarının planlanması ve ifası ile (iv) müşteri ilişkilerinin yönetilebilmesi amacıyla yukarıda sayılan fiziki veyahut elektronik ortamlarda güvenli bir biçimde KVKK ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.
- 5.2. Bu kapsamda kişisel Verilerin saklanması gerektiren amaçlar aşağıdaki gibidir:
- Müşteri şikayet sürecini yönetmek,
 - Hasar süreçlerini yönetmek
 - Kurumsal iletişimi sağlamak,
 - Kurum güvenliğini sağlamak,
 - İşe alım ve aday başvuru süreçleri dahil olmak üzere insan kaynakları süreçlerini yönetmek,
 - Çağrı merkezi süreçlerinin yönetilmesi,
 - Risk değerlendirme süreçlerinin yönetilmesi,
 - İleride doğabilecek hukuki uyumsuzluklarda delil olarak ispat yükümlülüğü
 - Pazarlama faaliyetlerinin yönetilmesi,
- 5.3. Kişisel Verilerin saklanması gerektiren hukuki sebepler aşağıdaki gibidir:
- 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 Şirket'in meşru menfaatleri için saklanması zorunlu olması,
 - Kişisel verilerin Şirket'in 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.
- 5.4. Kişisel Veriler, Şirket bünyesinde ilgili yasal saklama ve/veya zamanaşımı süreleri müddetince bulundurulmakta olup, bu verilerle ilişkili faaliyetlerin ve işbu Prosedür'de de belirtilen amaçların gerçekleştirilmesi için gerekli süre boyunca saklanmaktadır. Kullanım amacı sonlanan ve yasal saklama süresi/zamanaşımı sona eren Kişisel Veriler ise, KVKK'nın 7'nci maddesi uyarınca Şirket tarafından

silinmekte, yok edilmekte veya anonim hale getirilmektedir.

6. SAKLAMA VE İMHA SÜRELERİ

- 6.1. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliği Şirket nezdindeki önem derecesine göre belirlenir.
- 6.2. Verinin saklanması KVKK'nın 4. maddesinde belirtilen ilkelere uygunluğu sorgulanır. Saklanması KVKK'nın 4. maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.
- 6.3. Verinin saklanması KVKK'nın 5. ve 6. maddelerinde öngörülmüş olan istisnalardan hangisi/hangileri kapsamında değerlendirilebileceği tespit edilir. Tespit edilen istisnalar çerçevesinde verilerin saklanması gereken makul süreler tespit edilir. Söz konusu sürelerin sona ermesi halinde veriler silinir, yok edilir ya da anonim hale getirilir.
- 6.4. Şirket tarafından KVKK ve diğer ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerinizin saklama ve imha işlemlerinde Mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir.
- 6.5. Saklama süresi dolan kişisel veriler, Şirket tarafından belirlenen imha süreleri çerçevesinde, 6 aylık periyodlarla her yılın ocak ve temmuz ayında işbu Prosedür'de yer verilen usullere uygun olarak imha edilir.
- 6.6. 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.
- 6.7. Mevzuatlarda öngörülen süreler hariç olmak üzere, Kişisel Veri saklama ve imha süreleri aşağıdaki gibidir;

VERİ TÜRÜ	MUHAFAZA SÜRESİ	İMHA SÜRESİ
-----------	-----------------	-------------

Kişisel Verileri Saklama ve İmha Prosedürü

Tarih: 01.03.2021

Revizyon:2

Sayfa | 7

E-postalar ve şirket içi yazışmalar	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmeler	Sözleşmenin sona ermesini takip eden 10 yıl boyunca	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri/Sigortalı Kayıtları	Müşteri ile girilen son etkileşimi takip eden 10 yıl boyunca	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Kayıtları	Çalıştıkları süre boyunca	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Eski Çalışan Kayıtları	İşten ayrılmalarını takip eden 10 yıl boyunca	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Adaylarına İlişkin Kayıtlar	Başvuruyu takip eden 2 yıl boyunca	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Muhasebe ve Finans Kayıtları	5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket İçi Şikayetler ve İlgili Belgeler	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuk Kayıtları	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Resmi Yazışmalar	Süresiz	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Vergi Kayıtları	5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Takip Sistemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

7. SAKLAMA USULLERİ VE TEDBİRLER

AXA Partners Türkiye

Kısıklı Mah. Bosna Bulvarı No: 39 34692 Üsküdar / İstanbul

Tel: 0 216 524 36 36 | Faks: 0 216 524 36 37

info@ipaistanbul.com



7.1. KAYIT ORTAMLARI

Veri sahiplerine ait kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

- EXCHANGE SERVER
- FILE SERVER
- CRYPTOLOG
- MS SQL SERVER
- DC DHCP
- Kilitli Birim Dolapları
- Arşiv
- Birimlere Kısıtlı Erişim

7.2. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla Şirket tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır:

7.2.1. Şirket'in idari tedbirler açısından yükümlülükleri aşağıdaki gibidir ;

- Kişisel Veri Envanteri hazırlar ve süreç içerisinde günceller.
- VERBIS kaydını gerçekleştirir ve herhangi bir değişiklik halinde sicildeki bilgileri günceller.
- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.
- Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırır.
- Çalışanlarla imzalanan iş sözleşmelerinde sır saklama yükümlülüğü ve gizlilik hükümlerine yer verir.
- Şirket periyodik controller gerçekleştirdiği Kontrol ve/veya denetim sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerinin giderilmesini sağlar.
- 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. Gizlilik taahhütnameleri yapar.
- Kişisel veri içeren fiziksel ortamlara (arşiv odası vb gibi) giriş çıkışlarla ilgili gerekli güvenlik önlemleri alır ve fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlar.

- İlgili departman çalışanları, Ticari sözleşmeler, Yönetim Kurulu kararları ve İnsan Kaynakları belgeleri gibi gizli belgeler bir kasada veya en azından kilitlenebilir, yangına dayanıklı bir dolapta saklayacaktır Birer kopyası ortak klasörde elektronik olarak sağlanacaktır.
- Şirket, belgelerinin yetkili bir dış kaynak fiziksel arşivleme şirketi tarafından saklanmasını tercih edebilir.
- Tüm Çalışanlar hiçbir bilginin hileli kullanımlara maruz kalmamasını sağlamak için gizli belgeleri imha etmek üzere evrak imha makinelerini kullanacaklardır.
- Kullanım dışı evrakın bir dış firma tarafından imha edilmesini sağlayabilecektir. Bu durumda dış firmadan bir teslimat ve teyit yazısı alacaktır.

7.2.2. Şirket'in teknik tedbirler açısından yükümlülükleri aşağıdaki gibidir ;

- Kurulan sistemler kapsamında bilgi teknolojileri risk değerlendirmesi ve iş etki analizinin gerçekleştirilmesi süreçlerini yürütür.
- Verilerin kurum dışına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini ve ilgili matrislerin oluşturulmasını sağlar.
- Düzenli olarak ve ihtiyaç olduğunda sızma testi hizmeti alarak sistem zafiyetlerinin kontrolünü sağlar.
- Kişisel verilerin yok edilmesi geri dönüştürülemez ve denetim izi bırakmayacak şekilde sağlar.
- Kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli yöntemler ile korur.
- Ağ güvenliği ve uygulama güvenliği sağlar.
- Bulutta depolanan kişisel verilerin güvenliği sağlar.
- Çalışanlar için yetki matrisi oluşturulmasını sağlar.
- Erişim logları düzenli olarak tutar.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırır.
- Güncel anti-virüs sistemleri kullanır.
- Güvenlik duvarları kullanır.
- İç Kontrol ile birlikte sistemler kapsamında gerekli iç kontrolleri yapar.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygular ve olup bunların takibini yapar.
- Saldırı tespit ve önleme sistemleri kullanır.
- Veri kaybı önleme yazılımları kullanır ve verilerin yedeklenmesini sağlar.
- Elektronik verinin yedeklenip arşivlenmesi Bilgi İşlem Yedekleme Prosedürü tarafından tanımlanan kurallara uygun şekilde yönetir.
- Kişisel Verilerin taşınabilir bellek, CD, DVD aracılığıyla herhangi bir şekilde aktarılması konusunda gerekli önlemleri alır. Aktarımın gerekli olması halinde ise SFTP yöntemiyle aktarım gerçekleştirir.

8. KİŞİSEL VERİLERİ SİLME, İMHA ETME VE ANONİMLEŞTİRME USULLERİ

Şirket tarafından KVKK ve diğer ilgili mevzuata uygun olarak elde edilen kişisel veriler Kanun ve Yönetmelik'te sayılan kişisel veri işleme amaçlarının ortadan kalkması halinde Şirket tarafından re'sen yahut ilgili Kişinin başvurusu üzerine yine Kanun ve ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen teknikler ile imha edilecektir.

8.1. KİŞİSEL VERİLERİN SİLİNMESİ

8.1.1. Yazılımdan Güvenli Olarak Silme: Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken; ilgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

Bulut sisteminde ilgili verilerin silme komutu verilerek silinmesi; merkezi sunucuda bulunan dosya veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi; veya taşınabilir medyada yani flash ortamında bulunan verilerin uygun yazılımlar kullanarak silinmesi bu kapsamda sayılabilecektir.

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

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

8.1.2. Uzman Tarafından Güvenli Olarak Silme: Bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşılabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından ilgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde güvenli olarak silinir.

8.1.3. Kağıt Ortamında Bulunan Kişisel Verilerin Karartılması: Kişisel verilerin amaca yönelik olmayan kullanımını önlemek veya silinmesi talep edilen verileri silmek için ilgili kişisel verilerin fiziksel olarak kesilerek belgeden

çıkartılması veya geri döndürülemez ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi, kapatılması yöntemidir.

8.2. KİŞİSEL VERİLERİN İMHA EDİLMESİ

- 8.2.1.** De-manyetize Etme: Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir. Dikkat edilmelidir ki bu yöntemle yok etme başarılı olmaz ise ancak medyanın fiziksel olarak yok edilmesi ile yok etme işlemi tamamlanmış olabilecektir.
- 8.2.2.** Fiziksel Yok Etme: Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler yok edilirken kişisel verinin sonradan kullanılmayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Kağıt ve mikrofiş ortamındaki verilerin yok edilmesi de, başka bir şekilde yok edilmeleri mümkün olmadığından bu şekilde gerçekleştirilmelidir.
- 8.2.3.** Üzerine Yazma: Üzerine yazma yöntemi, özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkânsızlaştıran veri yok etme yöntemidir

8.3. KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Şirket kayıtları çıkartma, değişken değiştirme, genelleştirme gibi yöntemlerle kişisel verilerin anonim hale getirilmesini sağlar. 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.

9. YÜRÜRLÜK VE GÜNCELLENME

İşbu Prosedür yayım tarihinde yürürlüğe girer ve ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.