İSTANBUL DİJİTAL MEDYA TİCARET ANONİM ŞİRKETİ
İş Adresi: Molla Hüsrev Mah. Cemal Yener Tosyalı Cad. No:3 Fatih/İSTANBUL
Mersis No: 0466-0645-9190-0011
Vergi Dairesi/No: Hocapaşa V.D. 466 064 5919
Telefon: 0 (212) 375 32 00 **www.medya.istanbul**

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

İSTANBUL DİJİTAL MEDYA ANONİM ŞİRKETİ
01/11/2021

İçindekiler

I. GİRİŞ

Kişisel verilerinin korunması, müşteriler, potansiyel müşteriler, Şirket çalışanları, ziyaretçiler, iş birliği içinde olunan taraf ve kurumlar açısından oldukça önemlidir. Bu bilinç ile kişisel verilerin işlenmesi ve korunması Şirket'in öncelikleri arasında yer almakta ve en üst düzeyde hassasiyet gösterilmektedir.

07.04.2016 tarihinde Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu ("**Kanun**") ve ilgili mevzuat uyarınca veri sorumlusu sıfatını haiz tüm kurumların veri işleme süreçlerini gözden geçirmesi ve gerekli organizasyonel, hukuki ve teknik önlemleri alması gerekmiştir. Bu bağlamda, İstanbul Dijital Medya Anonim Şirketi ("**Şirket**") bünyesindeki iş süreçlerinin Kanun'a uyumlu hale getirerek, Şirket nezdinde kişisel veri işleme faaliyetlerine ilişkin temel esasları içeren işbu kişisel veri saklama ve imha politikasını ("**Politika**") oluşturmuştur.

II. POLİTİKA'NIN AMACI VE KAPSAMI

İşbu Politika ile Şirket nezdinde yürütülen veri işleme faaliyetlerinin hukuka uygun ve sistematik olarak sürdürülmesi için farkındalık oluşturmak, imha periyotlarını belirlemek, imha usulünü netleştirmek, kurumsal ilkeler temelinde ortak bir dil geliştirmek, mevzuat uyumunu sağlamak, Şirket nezdinde kişisel verileri işlenen kişilerin veri işleme süreçlerine ilişkin doğru ve güncel bilgiye ulaşılabilirliğini temin etmek amaçlanmaktadır.

Politika, Şirket tarafından otomatik olan veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla gerçekleştirilen kişisel veri işleme faaliyetlerini kapsamaktadır.

Yürürlükte bulunan mevzuat ve Politika arasında uyumsuzluk bulunması durumunda, mevzuat hükümleri öncelikli olarak uygulanacaktır. Bu temel Politika'nın dışında daha özel amaçlar için aynı konuda oluşturulan başka politika veya düzenleme bulunması halinde, öncelikle özel hükümler içeren maddeler uygulanır. Diğer politika ve dokümanların bu Politika ve ilgili mevzuat ile çelişen hükümleri uygulanmaz.

Politika kapsamında, Şirket'e ait tüm yapısal ve yapısal olmayan veriler incelenmiş, fiziki ve elektronik tüm ka ortamlarına ilişkin düzenleme yapılmıştır.

III. TANIMLAR

Bu Politika'da aşağıda açıklanan kısaltma ve terimler kullanılmıştır.

Açık Rıza	Belirli bir konuya ilişkin alınmış, bilgilendirilme neticesinde özgür irade ile açıklanan rıza
Anonimleştirme	Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
Başkanlık	Kişisel Verileri Koruma Kurumu Başkanlığı
Çalışan(lar)	Şirket bünyesinde çalışan gerçek kişiler
Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
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 veriler üzerinde gerçekleştirilen her türlü işlem
Kurul	Kişisel Verileri Koruma Kurulu

Kurum	Kişisel Verileri Korunma Kurumu
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 özel nitelikli kişisel veri
Silme	Kişisel verilerin ilgili kişiler için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi
Şirket	İstanbul Dijital Medya Anonim Şirketi
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
Veri Sorumluları Sicili	Kurul ve Başkanlık gözetiminde oluşturulan kamuya açık sicil
Yok Etme	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi

IV. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN KURALLAR

07.04.2016 tarihinde Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu ile "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"nin korunmasına ilişkin usul ve esaslar belirlenmiştir. Bu esaslar uyarınca aşağıda belirtilen süreçler oluşturulmuştur.

1. Kişisel Veri İşleme İlkeleri

Şirket nezdinde kişisel veriler aşağıdaki prensipler doğrultusunda işlenmektedir.

1.1. Hukuka ve Dürüstlük Kuralına Uygun İşleme

Şirket, kişisel verilerin işlenmesi faaliyetlerinde dürüstlük kuralına uygun hareket etmektedir. Bu kapsamda Şirket, ilgili kişilere duyurulan amaçlar dışındaki amaçlarla kişisel veri işlememektedir.

1.2. Kişisel Verilerin Doğru ve Gerektiğinde Güncel Olmasını Sağlama

Şirket nezdinde işlenen kişisel verilerin doğru ve güncel olması için teknik imkânlar dâhilinde gerekli tedbirler alınmakta, imha süreçleri düzenlenmektedir. İlgili kişilerin kişiler verilerinin hatalı olması halinde düzeltilmesi ve doğruluğunun teyidi için kontrol mekanizmaları oluşturulmuştur.

1.3. Belirli, Açık ve Meşru Amaçlarla İşleme

Şirket nezdinde yürütülen veri işleme faaliyeti yalnızca meşru amaçlarla, önceden belirlenmiş kurallara ve hukuka uygun sürdürülmektedir. Veri işleme faaliyeti başlama önce kişisel veri işleme amaçları belirlenmekte ve veri sahiplerinin kişisel verilerinin elde edilmesi sırasında kendilerine bu amaçları açıkça duyurmaktadır. Şirket'in kişisel veri işleme amaçlarının değişmesi halinde Politika güncellenmekte ve değişikliğin mümkün olan farklı kanallardan da veri sahiplerine duyurulması için çaba gösterilmektedir.

1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Kişisel veriler Şirket nezdinde önceden belirlenen amaçların gerçekleştirilmesi ile sınırlı olarak işlenmekte ve amacın gerçekleştirilmesiyle bağlantılı olmayan kişisel verilerin işlenmesinden kaçınılmaktadır. İlgili kişilerden yalnızca belirlenen amaçların gerçekleştirilmesi için gerekli olan veriler toplanmaktadır.

1.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre Kadar Muhafaza Etme

Şirket, kişisel verileri ancak ilgili mevzuatta belirtildiği veya işlendikleri amaç için gerekli olan süre kadar muhafaza etmektedir. Bu kapsamda, öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülmüşse, bu süreler ile sınırlı olarak yoksa işbu Politika'da belirtilen işleme amacı uyarınca belirlenmiş süreler kapsamında kişisel veriler muhafaza edilmektedir.

2. Kişisel Veri İşleme Şartları

Şirket nezdinde işlenen kişisel veriler aşağıdaki hususların mevcudiyeti halinde işlenmektedir.

2.1 İlgili kişinin açık rızasının bulunması

2.2 Kanunlarda kişisel veri işleme yükümlülüğünün açıkça öngörülmesi

2.3 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.

2.4 Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması

2.5 Şirket'in hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması

2.6 İlgili kişinin kendisi tarafından alenileştirilmiş olması

2.7 Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması

2.8 İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Şirket'in meşru menfaatleri için veri işlenmesinin zorunlu olması

Özel nitelikli kişisel veriler ise kanunlarda açıkça işlenmesi ilişkin yükümlülük bulunmadıkça İlgili Kişi'nin açık rızası olmaksızın işlenmemektedir.

3. Kişisel Verilerin Aktarılması

3.1. Kişisel Verilerin Üçüncü Kişilere Aktarılması

Şirket, kişisel veri işleme amaçları doğrultusunda işlemekte olduğu kişisel verileri üçüncü kişilere aktarabilmektedir. Veri aktarımı yapılan veya yapılması mümkün olan üçüncü kişiler kategorik olarak

aşağıda sıralanmaktadır. Şirket, kişisel veri paylaşırken kanunda getirilen düzenlemelere uygun hareket etmektedir.

Şirket, Kurul tarafından öngörülen önlemleri ve gerekli güvenlik tedbirlerini alarak ve azami özen göstererek; özel nitelikli verileri, özel nitelikli kişisel verilerin işlenebileceği şartların bulunması halinde üçüncü kişilere aktarabilmektedir.

3.2. Kişisel Verilerin Yurtdışına Aktarılması

Şirket, gerekli güvenlik tedbirlerini alarak işlemekte olduğu kişisel verileri bulut bilişim uygulamaları kapsamında yurt dışında yerleşik üçüncü kişilere ve iştiraklerine aktarabilmektedir.

Şirket tarafından kişisel veriler; meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda, Kurul tarafından yeterli korumaya sahip olduğu ilan edilen (edilmesi halinde) yabancı ülkelere veya yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt ettiği ve Kurul'un izninin bulunduğu yabancı ülkelere aktarılmaktadır.

4. Aydınlatma Yükümlülüğü

Şirket, Kanun'da yer alan aydınlatma yükümlülüğü ile uyumlu olarak, kişisel verilerin elde edilmesi sırasında kişisel veri sahiplerini kişisel verilerinin ne şekilde işleneceği konusunda bilgilendirmektedir. Bu kapsamda Şirket, ilgili kişileri asgari olarak aşağıdaki hususlarda bilgilendirmektedir.

4.1. Şirket'in kimliği
4.2. Kişisel verilerin hangi amaçla işleneceği
4.3. Kişisel verilerin kimlere ve hangi amaçla aktarılabileceği
4.4. Kişisel veri toplamanın yöntemi ve hukuki sebepleri
4.5. Kişisel veri sahibinin sahip olduğu haklar

Bu yükümlülük, Şirket'in internet sitesi, Şirket içi duyuruları ve ticari faaliyetinde kullandığı haberleşme kanalları aracılığıyla gerçekleştirilmektedir.

5. Veri Güvenliği

Kanun'un 12. maddesi uyarınca Şirket;

(i) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
(ii) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
(iii) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almaktadır.

5.1. Kişisel Veri Güvenliğine İlişkin Alınan İdari Tedbirler

5.1.1. Mevcut Risk ve Tehditlerin Belirlenmesi

Kişisel verilerin güvenliğinin sağlanması için öncelikle Şirket, işlenen tüm kişisel verilerin ne olduğunu tespit etmekte, bunların korunmasına ilişkin ortaya çıkabilecek muhtemel risklerin gerçekleşme ihtimalini ve gerçekleşmesi halinde ortaya çıkabilecek kayıpları doğru bir şekilde saptayabilmesi gerekli olup buna ilişkin tedbirleri almaktadır. Riskler belirlenirken;

(i) Kişisel verilerin özel nitelikli kişisel veri olup olmadığı,
(ii) Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği,
(iii) Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği,

dikkate alınır.

5.1.2. Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

Kişisel veri güvenliğini ihlale yönelik saldırıların yanı sıra kişisel verilerin hukuka aykırı olarak açıklanması ya da paylaşılması gibi konular başlıca kişisel veri güvenliği ihlallerindendir. Bunlar kullanıcıların dikkatsizliği yahut tecrübesizliği sonucu kötü amaçlı yazılım içeren elektronik posta ekinin açılması veya elektronik postanın yanlış alıcıya gönderilerek kişisel verilerin üçüncü kişilerin erişimine açılması şeklinde vücut bulabilir.

Şirket nezdinde çalışan herkesin kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmektedir. Bu noktada çalışanların muhtemel durumlara yönelik eğitim almaları ve farkındalık çalışmalarına katılmaları ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması güvenliğin

sağlanması açısından önem arz eder. Aynı zamanda Çalışanlar işe alınırken görev ve yetkileri değerlendirilerek gerekli görülmesi halinde gizlilik anlaşması imzalamaları istenilmektedir. Güvenlik politika ve prosedürlerine uymamaları halinde uygulanacak disiplin süreci de çalışan kişisel verilerin korunması politikasında ayrıca belirtilmektedir.

5.1.3. Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi

Kişisel veri envanteri neticesinde tespit edilen veri kategorileri için ortaya çıkabilecek risk ve güvenlik ihlallerinin yönetilmesine ilişkin prosedürler oluşturulmaktadır. İstikrar sağlanabilmesi için bu politika ve prosedürlerin düzenli olarak kontrol edilmesi amaçlanmaktadır.

1.4. Kişisel Veri Yığılmalarının Mümkün Olduğunca Azaltılması

Kanun'un 4'üncü maddesinin ikinci fıkrasının (b) ve (d) bentleri uyarınca kişisel veriler gerektiğinde doğru ve güncel olacak şekilde öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir. Bu kapsamda, Şirket, kişisel verilere olan ihtiyacı ve verilerin doğru yerde muhafaza edilip edilmediklerini denetlemektedir. Bunun yanında işlendikleri amaca uygun olmasına karşın sıklıkla erişimine lüzum olmayan ve arşiv amaçlı tutulan kişisel veriler, yetkisiz erişimine engel olabilmek için daha güvenli ortamda muhafaza edilmektedir.

5.1.4. Veri İşleyenler ile İlişkilerin Yönetimi

Şirket, veri işleyenle imzaladığı sözleşmenin; yazılı olmasına, veri işleyenin veri sorumlusunun talimatları ışığında ilgili sözleşme hükümlerine ve mevzuata uygun hareket edeceğine ilişkin hüküm içermesine ve Politika'ya uygun olmasına dikkat etmektedir. Şirket nezdinde de Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimler yapılmakta veya yaptırılmaktadır.

5.2. Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler

5.2.1. Siber Güvenliğin Sağlanması

Şirket nezdinde aşağıda yer alan önlemler alınmaktadır:

(i) Öncelikle güvenlik duvarı ve ağ geçidinin sağlanması

(ii) Hemen hemen her yazılımın ve donanımın kurulum ve yapılandırma işlemlerine tabi tutulması (güvenlik açıkları belgelenmiş özellikle eski sürüm yazılım ve servislerinin güncel tutulması yerine cihazdan kaldırılması ve silinmesini ayrıca önermiştir)

(iii) Yama yönetimi ve yazılım güncellemelerinin yapılması

(iv) Yazılım ve donanımların düzgün bir şekilde çalışıp çalışmadığının ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli kontrolü

(v) Çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisinin tanınması

(vi) Sistemlere kullanıcı adı ve şifre kullanmak suretiyle erişim sağlanması

(vii) Şifre ve parolalar oluşturulurken kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesinin sağlanması (veri sorumlularının erişim yetki ve kontrol matrisi oluşturmasını ve ayrı bir erişim politika ve prosedürleri oluşturularak veri sorumlusu organizasyonu içinde bu politika ve prosedürlerin uygulamaya alınmasını ayrıca önermiştir)

(viii) Şifre girişi deneme sayısının sınırlandırılması

(ix) Düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması

(x) Yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması

(xi) Veri sorumlusuyla ilişkileri kesilen çalışanlar için zaman kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması

(xii) Bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması

(xiii) Yukarıda belirtilen ürünlerin güncel tutulması ve gereken dosyaların düzenli olarak tarandığından emin olunması

(xiv) Farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi gerçekleştirilmektedir.

5.2.2. Kişisel Veri Güvenliğinin Takibi

Kişisel verilerin bulunduğu sistemlere gelen saldırıların uzun süre fark edilememesinin ve geç müdahalede bulunulmasının önüne geçebilmek için;

(i) Bilişim ağlarında hangi yazılım ve servislerin çalıştığı kontrol edilmekte

(ii) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığı belirlenmekte

(iii) Tüm kullanıcıların işlem hareketleri kaydı düzenli olarak tutulmakta

(iv) Güvenlik sorunları mümkün olduğunca hızlı bir şekilde raporlanmakta

(v) Çalışanların sistem ve servislerindeki güvenlik zafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürünün oluşturulması için çalışmalar yürütülmekte

(vi) Güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçları düzenli olarak kontrol edilmekte

(vii) Sistemlerden gelen uyarılar üzerine harekete geçilmekte

(viii) Bilişim sistemlerinin bilinen zafiyetlere karşı korunması için düzenli olarak zafiyet taramaları ve sızma testleri yapılmakta

(ix) Ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılmakta

(x) Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmakta ve güvenli bir şekilde saklanmaktadır.

5.2.3. Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

Kişisel veriler Şirket'in işyerlerinde yer alan cihazlarda ya da kâğıt ortamında saklanmaktadır. Bu cihazların ve kağıtların çalınması, kaybolması gibi tehditlere karşı fiziksel önlemler alınmaktadır. Bunun dışında kişisel verilerin yer aldığı fiziksel ortamın dış risklere (yangın, sel vb.) karşı da korunması sağlanmakta ve bu ortamlara giriş / çıkışların kontrol altına alınmaktadır.

Ayrıca:

(i) Kâğıt ortamındaki evrak, sunucu, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınmakta

(ii) Kişisel veri içeren kâğıt ortamındaki evrak, kilitli bir şekilde ve sadece yetkili kişilerin erişebileceği ortamlarda saklanmakta ve bu evraka yetkisiz erişim önlenmekte

(iii) Kişisel veri içeren cihazların kaybolması veya çalınması gibi durumlara karşı erişim kontrol yetkilendirme ve/veya şifreleme yöntemleri kullanılmakta

(iv) Şifre anahtarı sadece yetkili kişilerin erişebileceği ortamda saklanmakta ve bunlara yetkisiz erişim önlenmekte

(v) Hangi şifreleme yöntemleri kullanılırsa kullanılsın kişisel verilerin tam olarak korunduğundan emin olunması amacıyla uluslararası kabul gören şifreleme programları kullanılmakta

(vi) Asimetrik şifreleme yöntemi uyarınca anahtar yönetimi süreçlerine önem gösterilmekte

(vii) Çalışanların şahsi elektronik cihazlarının bilgi sistem ağına erişim sağladığı durumlar için yeterli güvenlik tedbirleri alınmaktadır.

5.2.4. Kişisel Verilerin Bulutta Depolanması

Şirket nezdinde bulut depolama hizmeti sağlayıcısı tarafından sağlanan güvenlik tedbirlerini değerlendirmektedir. Bu kapsamda:

(i) Bulutta depolanan kişisel verilerin neler olduğunun detaylıca bilinmekte,

(ii) İlgili kişisel verilerin yedeklenmesi ve senkronizasyonu sağlanmakta,

(iii) İlgili kişisel verilere gerektiği hallerde uzaktan erişilebilmesi için iki kademeli kimlik doğrulama kontrolü uygulanmakta,

(iv) Kişisel verilerin depolanması ve kullanımı sırasında verilerin kriptografik yöntemlerle şifrelenmesi bulut ortamlarına şifrelenerek atılmakta,

(v) Kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılmaktadır.

Bulut depolama hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmeye yarayabilecek şifreleme anahtarlarının tüm kopyalarının da yok edilmesi esastır.

5.2.5. Bilgi Teknolojileri Sistemleri Tedariki, Geliştirme ve Bakımı

Yeni sistemlerin tedariki, geliştirilmesi veya bakımı ile ilgili eylemler gerçekleştirilirken veri sorumlusu birtakım güvenlik önlemleri alınmaktadır.

İşlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmış uygulama sistemlerinin girdilerinin doğru ve uygun olduğunun kontrolü yapılmalı ve bu

uygulamalara doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı kontrol istemi halinde bozulup bozulmadığını denetlemek maksadıyla kontrol mekanizması yerleştirilmesi öngörülmektedir.

Bakım veya teknik destek için üçüncü kişilere gönderilen cihazlar kişisel veri içeriyorsa gönderilmeden önce veri saklama ortamı sökülerek saklanmakta ya da sadece arızalı parçası gönderilmektedir. Dışarıdan bir çalışan bakım ve onarım için gelmişse kişisel veriler kopyalanmaktadır.

5.2.6. Kişisel Verilerin Yedeklenmesi

Kişisel veriler herhangi bir sebeple zarar görebilir, yok olabilir, çalınabilir, kaybolabilir yahut verilere kötü amaçlı yazılımlar yüzünden erişilemeyebilir. Bu durumlara maruz kalmamak için veriler düzenli olarak yedeklenmektedir.

Yedeklenen kişisel verilere erişilebilirlik sistem yöneticisiyle sınırlanmakta, veri seti yedekleri mutlaka ağ dışında tutulmaktadır.

6. İlgili Kişinin Hakları ve Şikâyet Yönetimi

İlgili Kişinin hakları ise kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme olarak belirlenmektedir. Bu kapsamda Şirket nezdinde İlgili Kişi'nin taleplerini yönetecek sistemler oluşturulmaktadır.

İlgili Kişi'nin, Şirket'e başvuruda bulunması halinde ilgili talep, mümkün olan en kısa sürede ve en geç otuz

gün içinde yanıtlandırmaktadır. Başvuruda bulunan ilgili kişinin talebi, talebin Kanun ile uyumluluğu ve Şirket'in mevzuat gereği uyması gereken yükümlülükler bakımından değerlendirilerek mümkün olduğu ölçüde yerine getirilmektedir. Değerlendirme sonucu talebin yerine getirilmesinin mümkün olmadığına karar verilirse, ilgili kişinin başvurusu gerekçeli olarak yanıtlandırılmaktadır. İlgili Kişi, Kanun'un 14. maddesi gereğince başvurusunun reddedilmesi, verilen cevabı yetersiz bulması veya süresinde başvurusuna cevap verilmemesi hâllerinde; Şirket'in cevabını öğrendiği tarihten itibaren otuz ve her hâlükârda başvuru tarihinden itibaren altmış gün içinde Kurul'a şikâyette bulunabilir.

V. ŞİRKET NEZDİNDE İŞLENEN VERİ KATEGORİLERİ ve İMHA

Şirket nezdindeki veri işleme faaliyetleri aşağıda yer alan kategoriler bazında sürdürülmektedir. Bahse konu kişisel veri kategorilerinin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan azami muhafaza edilme süreleri aşağıda yer alan tabloda belirtilmiştir. Aşağıda belirtilen istisnalar dışındaki kişisel veriler 10 yıl süreyle saklanmakta ve yıllık periyodik imha tarihinde imha edilmektedir.

KİŞİSEL VERİ KATEGORİZASYONU	AÇIKLAMA	İMHA SÜRESİ
Kimlik Bilgisi	Ehliyet, nüfus cüzdanı, ikametgâh, pasaport, avukatlık kimliği, evlilik cüzdanı gibi dokümanlarda yer alan kişinin kimliğine dair tüm bilgiler.	İşlenme amacının tamamlanmasından itibaren 10 yıl
İletişim Bilgisi	Telefon numarası, adres, e-mail gibi veri sahibiyle iletişim kurulmasına yönelik bilgiler.	İşlenme amacının tamamlanmasından itibaren 10 yıl
Müşteri Bilgisi	Ticari faaliyetlerimiz ve bu çerçevede iş birimlerimizin yürüttüğü operasyonlar neticesinde ilgili kişi hakkında elde edilen ve üretilen bilgiler.	İşlenme amacının tamamlanmasından itibaren 10 yıl
Aile Bireyleri ve Yakın Bilgisi	Sunduğumuz ürün ve hizmetlerle ilgili veya Şirketin ve veri sahibinin hukuki menfaatlerini korumak amacıyla işlenen kişisel veri sahibinin aile bireyleri ve yakınları hakkındaki bilgiler.	İşlenme amacının tamamlanmasından itibaren 10 yıl
Müşteri İşlem Bilgisi	Ürün ve hizmetlerimizin kullanımına yönelik kayıtlar ile müşterinin ürün ve hizmetleri kullanımı için gerekli olan talimatları ve talepleri gibi bilgiler.	İşlenme amacının tamamlanmasından itibaren 10 yıl
Fiziksel Mekân Güvenlik Bilgisi	Fiziksel mekâna girişte, fiziksel mekânın içerisinde kalış sırasında alınan kamera kayıtları, parmak izi kayıtları gibi kayıtlar ve belgelere ilişkin kişisel veriler.	Kamera kaydının tamamlanmasından itibaren 60 gün
İşlem Güvenliği Bilgisi	Ticari faaliyetlerimizi yürütürken teknik, idari, hukuki ve ticari güvenliğimizi sağlamamız için işlenen kişisel veriler.	İşlenme amacının tamamlanmasından itibaren 10 yıl

Finansal Bilgi	Şirketimizin kişisel veri sahibi ile kurmuş olduğu hukuki ilişkinin tipine göre yaratılan her türlü finansal sonucu gösteren bilgi, belge ve kayıtlara ilişkin işlenen kişisel veriler.	İşlenme amacının tamamlanmasından itibaren 10 yıl
Çalışan Adayı Bilgisi	Şirketimizin çalışanı olmak için başvuruda bulunmuş veya ticari teamül ve dürüstlük kuralları gereği şirketimizin insan kaynakları ihtiyaçları doğrultusunda çalışan adayı olarak değerlendirilmiş veya Şirketimizle çalışma ilişkisi içerisinde olan bireylerle ilgili işlenen kişisel veriler.	Çalışanın işe alınmama kararı alınmasından itibaren 3 yıl
Hukuki İşlem ve Uyum Bilgisi	Hukuki alacak ve haklarımızın tespiti, takibi ve borçlarımızın ifası ile kanuni yükümlülüklerimiz ve şirketimizin politikalarına uyum kapsamında işlenen kişisel veriler.	İşlenme amacının tamamlanmasından itibaren 10 yıl
Denetim ve Teftiş Bilgisi	Şirketimizin kanuni yükümlülükleri ve şirket politikalarına uyumu kapsamında işlenen kişisel veriler.	İşlenme amacının tamamlanmasından itibaren 10 yıl
Özel Nitelikli 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 özel nitelikli kişisel veridir.	İşlenme amacının tamamlanmasından itibaren 10 yıl (Sağlık raporlarında 15 yıl)
Çalışanların Sağlık Verileri	İş sağlığı ve güvenliği kapsamında saklanır.	Fesihten itibaren 15 yıl
Pazarlama Bilgisi	Ürün ve hizmetlerimizin kişisel veri sahibinin kullanım alışkanlıkları, beğenisi ve ihtiyaçları doğrultusunda özelleştirilerek pazarlamasının yapılmasına yönelik işlenen kişisel veriler ve bu işleme sonuçları neticesinde yaratılan rapor ve değerlendirmeler.	İşlenme amacının tamamlanmasından itibaren 10 yıl
Talep/Şikâyet Yönetimi Bilgisi	Şirketimize yöneltilmiş olan her türlü talep veya şikâyetin alınması ve değerlendirilmesine ilişkin kişisel veriler.	İşlenme amacının tamamlanmasından itibaren 3 yıl
İtibar Yönetimi Bilgisi	Şirketimizin ticari itibarını korumak maksatlı toplanan bilgiler ve buna ilişkin oluşturulan değerlendirme raporları ile alınan aksiyonlarla ilgili bilgiler.	İşlenme amacının tamamlanmasından itibaren 10 yıl

Azami muhafaza sürelerinin sona ermesi neticesinde ilgili kişisel verinin saklanması için mevcut olan hukuki veya teknik sebeplerin ortadan kalkması neticesinde Silme, Yok Etme ve Anonimleştirme yollarından biri seçilerek kişisel verinin imhası gerçekleştirilir. İmha süreçlerinde veri kaybı oluşmaması adına tüm teknik ve idari tedbirler alınır, yetkisiz kişilerin sürece dahil edilmemesi sağlanır. Periyodik imha tarihi olarak her yılın Ocak ve Ağustos ayı belirlenmiştir.

VI. KİŞİSEL VERİ İŞLEME AMAÇLARI

Şirket nezdindeki veri işleme faaliyetleri aşağıda yer alan amaçlar doğrultusunda sürdürülmektedir. Bu amaçlar zaman zaman değişebilecektir.

- Şirket faaliyetlerinin Şirket prosedürleri ve/veya ilgili mevzuata uygun olarak yürütülmesinin temini için gerekli operasyonel faaliyetlerinin planlanması ve icrası
- İş faaliyetlerinin planlanması ve icrası
- Kurumsal yönetim faaliyetlerin planlanması ve icrası
- İş sürekliğinin sağlanması faaliyetlerinin planlanması ve icrası
- İnsan kaynakları süreçlerinin ve ihtiyaçlarının planlanması ve icrası
- Sözleşme süreçlerinin ve/veya hukuki taleplerin takibi
- Şirket'in finansal risk süreçlerinin planlanması ve/veya icrası
- Finans ve/veya muhasebe işlerinin takibi
- Risk yönetiminin gerçekleştirilmesi
- Ücret yönetimi
- Şirket denetim faaliyetlerinin planlanması ve icrası
- Yetkili kişi ve/veya kuruluşlara mevzuattan kaynaklı bilgi verilmesi
- Hukuk işlerinin takibi
- Kurumsal iletişim faaliyetlerinin planlanması ve icrası
- Tedarikçi veya iş ortağı yönetimi süreçlerinin planlanması ve icrası
- Operasyon süreçlerinin planlanması ve icrası
- Bilgi güvenliği süreçlerinin planlanması, denetimi ve icrası
- Bilgi teknolojileri alt yapısının oluşturulması ve yönetilmesi
- Çalışan istihdamına ilişkin süreçlerinin yürütülmesi
- Mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi
- Çalışanlar için yan haklar ve menfaatlerin planlanması ve icrası
- Çalışanların performans değerlendirme süreçlerinin planlanması ve takibi
- Yetenek- kariyer gelişimi faaliyetlerinin planlanması ve icrası
- Çalışanlara yönelik kurumsal iletişim/sorumluluk/etkinlik projelerinin planlanması ve/veya icrası

- Çalışanların iş faaliyetlerinin takibi ve/veya denetimi
- Şirket dışı veya Şirket içi eğitim faaliyetlerinin planlanması ve icrası
- Çalışan memnuniyetinin ve/veya bağlılığı süreçlerinin planlanması ve icrası
- Ziyaretçi kayıtlarının oluşturulması ve takibi
- Acil durum yönetimi süreçlerinin planlanması ve icrası
- Şirket mevzuatı işlemlerinin gerçekleştirilmesi
- Şirket işyerlerinin, demirbaşlarının ve kaynaklarının güvenliğinin temini
- Şirket'in operasyonel risk süreçlerinin planlanması

Bu amaçlar, somut olayın özelliklerine göre açık rıza gerektiren süreçler olabilmektedir. Bu durumda ilgili kişilerden, Kanun'a uygun açık rızaların alınması süreçleri uygulanmaktadır. İlgili kişinin açık rızasını vermemesi durumunda, ilgili kişinin verileri ancak Kanun'da sayılan açık rıza alınmadan kişisel verilerin işlenebileceği şartlar kapsamında ve bu şartlara uygun amaçlarla işlenebilmektedir.

VII. KİŞİSEL VERİLERİN TOPLANMASI VE AKTARIMI

Perakende ticareti mevzuatı ve diğer sair mevzuat hükümleri çerçevesinde toplanan kişisel veriler, hizmetlerin sağlanabilmesi için ilgili kişi ve/veya kurumlara, iş ortaklarına ve bağlı bulunulan şirketler topluluğuna aktarılabilmekte olup; ayrıca bu veriler anonim hale getirildikten sonra sağlanılan hizmetlere yönelik istatistiksel analizler yapılmak üzere Şirket içerisinde yer alan merkezlere ve iştiraklere aktarılabilmektedir.

İnternet sitesine üye olma ve internet sitesi aracılığı ile elektronik ortamda alışveriş yapılması halinde otomatik toplanan ve/veya işlenen kişisel veri ve/veya özel nitelikli kişisel verilere ilişkin açık rızalar elektronik ortamda alınmaktadır. Bu doğrultuda açık rıza beyanlarının toplanması üzerine, internet sitesi vasıtası ile elde edilen kişisel veri ve/veya özel nitelikli kişisel veriler işlenmekte, hizmetlerin amaçları doğrultusunda yasal sürelerde saklanmakta ve gerekli görülmesi halinde 3. kişilere aktarılmaktadır. Bu doğrultuda çerezler içerisinde kişisel veriler saklanmamakta olup başka uygulamalar veya kişiler ile paylaşılmamaktadır.

Yukarıda belirtilen amaçlarla, kişisel verilerin aktarılabileceği kişi/kuruluşlar; Türk Ticaret Kanunu, Vergi Usul Kanunu ve diğer mevzuat hükümlerinin izin verdiği kurum veya kuruluşların yanı sıra adli makamlardır.

VIII. KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK ORGANİZASYONEL TEDBİRLER

Teknik Tedbirler

5.2.1. maddede belirtilen siber güvenlik önlemlerinin yanı sıra aşağıdaki önlemler alınmaktadır.

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Alınan teknik önlemlerin uygulamasının belirli aralıklarla denetim sürecine tabidir ve denetim sonuçları ilgili birimlere raporlanmaktadır.
- Şirketimiz bünyesinde teknik konularda uzman personel istihdam edilmektedir.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- 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.
- Mevcut risk ve tehditler belirlenmiştir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

İdari Tedbirler

- İş birimlerimizce yürütülen kişisel veri işleme faaliyetlerinin tespiti, hukuka uygunluk analizi ve bu doğrultuda iş birimlerinin yükümlülüklerinin ortaya konulması gerçekleştirilmektedir.

- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- İş birimlerinin mevcut çalışanlarının ve iş birimi bünyesine yeni dâhil olmuş çalışanların kişisel verilerin korunması konusunda farkındalığının oluşması için eğitim düzenlenmesi, eğitim sonuçlarının değerlendirilmesi ve gerektiğinde bu eğitimlerin tekrarlanması veya iş birimine özgü eğitim programlarının kurgulanması sağlanmaktadır.
- Şirketimiz ile çalışanlar arasında akdedilen sözleşmelere, Şirketimizin talimatları ve kanunlarla getirilen istisnalar dışında, kişisel verileri işlememe, ifşa etmeme ve kullanmama yükümlülüğü getiren kayıtlar konulmaktadır.
- İşlenme amacına paralel olarak kişisel verilere erişim sınırlandırması yapılmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- 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.

YÜRÜRLÜK VE GÜNCELLENEBİLİRLİK

Şirket tarafından düzenlenen bu Politika 01.11.2021 tarihlidir.

Politikanın tamamında veya bir kısmına ilişkin olarak güncellemeler yapılabilir.

Politika, yönetim onayından sonra 10.11.2021 tarihinde yayımlanarak yürürlüğe girer.