ALPHA E-TİCARET LİMİTED ŞİRKETİ
KURUMSAL KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

Doküman Bilgileri	
Doküman Adı:	Kişisel Verilerin Korunması Politikası
Doküman İlgisi:	Kişisel Verilerin Korunması Politikasının amacı, ALPHA E-TİCARET LİMİTED ŞİRKETİ tarafından kişisel verilerin korunmasına yönelik süreçlerin planlanması ve bu konuya ilişkin uygulanacak esasların belirlenmesidir.
Yayınlanma Tarihi:	[04.10.2024]
Versiyon No:	00
Referans / Gerekçe:	6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuat
Onay Merci:	ALPHA E-TİCARET LİMİTED ŞİRKETİ Yönetim Kurulu

ALPHA E-TİCARET LİMİTED ŞİRKETİ
KURUMSAL KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

1. AMAÇ

Her bireyin kendisi ile ilgili kişisel verilerin korunmasını isteme hakkı Anayasa'dan doğan kutsal bir haktır. **ALPHA E-TİCARET LİMİTED ŞİRKETİ ("Humy")** olarak bu hakkın gereklerini yerine getirmeyi en değerli görevlerimizden biri olarak kabul ediyoruz. Bu nedenle kişisel verilerinizin hukuka uygun olarak işlenmesine ve korunmasına önem veriyoruz.

Kurumsal Kişisel Verilerin Korunması Politikası da kişisel verilerin korunmasına verdiğimiz önemin bir sonucu olarak kişisel verileri işlerken ve korurken temel aldığımız ilkeleri ve uyguladığımız prosedürleri belirlemek amacıyla hazırlanmıştır.

2. KAPSAM

Politika **Humy**'nin yönettiği bütün kişisel veriler 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 işlemi kapsamaktadır.
Politika **Humy**'nin ortaklarının, yetkililerinin, müşterilerinin, çalışanlarının, tedarikçi yetkililerinin ve çalışanlarının ve üçüncü kişilerin işlenen tüm kişisel verilerine ilişkindir.
Humy Politika'yı mevzuata ve Kişisel Verileri Koruma Kurumu'nun kararlarına uyum ve kişisel verilerin daha iyi korunması amaçlarıyla değiştirebilir.

3. TANIMLAR

Kısaltma	Tanım
Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.

Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
İlgili Kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun/KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Veri Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.
Kişisel Verilerin İşlenmesi	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**.**
Komisyon	**Humy** tarafından Politika'yı ve ilgili diğer prosedürleri yönetmek ve Politika'nın yürürlüğünü sağlamak amacıyla kurulan Kişisel Verileri Koruma Komisyonu.
Kurul	Kişisel Verileri Koruma Kurulu.
Kurum	Kişisel Verileri Koruma 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.
Periyodik İmha	Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Politika	Kişisel Verilerin Korunması Politikası
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.

4. GENEL İLKELER

Humy her yeni kişisel veri işlemeyi gerektiren iş akışının hazırlık aşamasında işlenecek verilerin aşağıdaki ilkelere uygunluğunu denetler. Uygun bulunmayan iş akışları hayata geçirilmez.

Humy kişisel verileri işlerken;

1. Hukuka ve dürüstlük kurallarına uyar.
2. Kişisel verilerin doğru ve gerektiğinde güncel olduğundan emin olur.
3. İşleme amacının belirli, açık ve meşru olmasına dikkat eder.
4. İşlenen verinin işlenme amacıyla bağlantılı olduğunu, işlenilmesi gerektiği kadarıyla sınırlı işlendiğini ve ölçülü olduğunu kontrol eder.
5. Verileri ancak ilgili mevzuatta öngörörülen veya işlenme amacı için gerekli olduğu kadar muhafaza eder, işlenme amacı ortadan kalktığında imha eder.

5. GÖREV VE SORUMLULUKLAR

Humy'nin bünyesinde kişisel verilerin işlenmesine ilişkin işbu Politika'yı ve ilgili diğer prosedürleri yönetmek ve Politika'nın yürürlüğünü sağlamak amacıyla Kişisel Verilerin Korunması Komisyonu kurulmuştur. Komisyon'u Genel Müdür başkan olarak temsil eder ve üyeler bölüm yöneticilerinden oluşturmaktadır. **Humy** bunun yanı sıra gerektiğinde 6698 sayılı Kişisel Verilerin Korunması Kanunu'na uyum sağlamak amacıyla KVKK danışmanlığı desteği de almaktadır. Komisyon gerek görmesi halinde toplantılarına KVKK danışmanlarını ve meslek uzmanlarını da çağırabilir.
Komisyon'un görev ve sorumlulukları aşağıda belirtilmiştir.

1. Olağan olarak 6 ayda bir toplanır. Şartların gerektirmesi halinde olağanüstü toplanılabilir (örneğin olası bir veri ihlali durumunda).
2. Politika'da değiştirilmesi/geliştirilmesi gereken hususları tartışır.
3. Kişisel verilerin hukuka uygun işlenmesi ve korunması adına yerine getirilebilecek hususları tespit eder.
4. Komisyon, şirket içi ve iş ortakları nezdinde KVKK farkındalığını artırmak için atılabilecek adımları belirler.
5. Kişisel verilerin işlenmesi ve korunması hususunda karşılaşılabilecek riskleri tespit eder, gerekli idari ve teknik tedbirleri alır.
6. Kurum ile irtibatı sağlar ve ilişkileri yönetir.
7. İlgili Kişi'den gelen talepleri değerlendirir.
8. Periyodik imha süreçlerini takip eder.
9. Veri Envanteri'ni günceller.
10. Yukarıda sayılan hususlara ilişkin görevlendirmeleri yapar.

6. VERİ GÜVENLİĞİ İÇİN ALINAN TEDBİRLER

Humy kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli hertürlü teknik ve idari tedbirleri alır.

6.1. Kişisel Verileri Koruma Kurumu Tarafından Önerilen Teknik Tedbirlerin Kapsamında;

Siber Güvenliğin Sağlanması

- Kişisel veri içeren bilgi teknoloji sistemlerinin internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında alınabilecek öncelikli tedbirler, güvenlik duvarı ve ağ geçidi uygulaması.
- Kişisel veri içeren sistemlere erişimin de sınırlı olmasının sağlanması Çalışanlara, sınırlı ölçüde erişim yetkisi tanınması ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanması,
- Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması.

Kişisel Veri Güvenliğinin Takibi

- Bilgi işleme sistemlerinin hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmasını önlemek ve bu durumun önüne geçebilmek için;
- Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi.
- Bilişim ağlarında sızma olup olmadığının belirlenmesi.
- Tüm kullanıcıların işlem hareketleri kaydının tutulması (log kayıtları gibi).
- Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması.

Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

- Kişisel veri güvenliği ihlalleri yaşanabilecek kişisel veri içeren cihazların (dizüstü bilgisayar, cep telefonu, flash disk vb.) fiziksel güvenliğinin sağlanması,

- Elektronik posta ya da posta ile aktarılacak kişisel verilerin yeterli tedbirler alınarak gönderilmesi.
- Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kağıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu giriş yetki sınırlaması olan bölümlerde/ odalarda korunması.
- Bu alanların kullanılmadığı zaman kilit altında tutulması, giriş çıkış kayıtlarının tutulması gibi önlemler de alınması.

Kişisel Verilerin Bulutta Depolanması

- Kişisel verilerin bulut depolama hizmeti sağlayıcıları tarafından işlenmesine ilişkin risklerin yönetilmesi.
- Bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının veri sorumlusunca değerlendirilmesi, onaylanması.
- Bu kapsamda, bulutta depolanan kişisel verilerin neler olduğunun detaylıca bilinmesi, yedeklenmesi, senkronizasyonun sağlanması ve kimlik doğrulama kontrolünün uygulanması.

Kişisel Verilerin Yedeklenmesi

- Yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olmasının sağlanması.
- Veri seti yedekleri mutlaka ağ dışında tutulması.
- Veri seti yedekleri üzerinde kötü amaçlı yazılım kullanımına karşı tedbirlerin alınması.
- Tüm yedeklerin fiziksel güvenliğinin sağlanması.

Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı

- Arızalandığı ya da bakım süresi geldiği için üretici, satıcı, servis gibi üçüncü kurumlara gönderilen cihazlar eğer kişisel veri içermekte ise bu cihazların bakım ve onarım işlemi için gönderilmesinden önce, kişisel verilerin güvenliğinin sağlanması.
- Cihazlardaki veri saklama ortamının sökülerek saklanması.
- Sadece arızalı parçaların gönderilmesi gibi işlemler yapılması.
- Bakım ve onarım gibi amaçlarla dışarıdan personel gelmişse kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi.

Bu Teknik Tedbirlerin Uygulanması Gereksinimine ilişkin olarak **Humy,** şu teknik tedbirleri uygular;

- Yetki Matrisi uygulaması.
- Yetki Kontrol uygulaması.
- Erişim Logları uygulaması.
- Kullanıcı Hesap Yönetimi uygulaması.
- Ağ Güvenliği uygulaması.
- Uygulama Güvenliği yönetimi.
- Şifreleme yönetimi.
- Sızma Testi uygulaması.
- Saldırı Tespit ve Önleme Sistemleri yönetimi.
- Log Kayıtları uygulaması.
- Veri Maskeleme uygulaması.
- Veri Kaybı Önleme Yazılımları uygulaması.
- Yedekleme yönetimi.

- Güvenlik Duvarları yönetimi.
- Güncel Anti-Virüs Sistemleri yönetimi.
- Silme, Yok Etme veya Anonim Hale Getirme uygulaması.
- Anahtar Yönetim uygulaması.

6.2. Kişisel Verileri Koruma Kurumu Tarafından Önerilen İdari Tedbirlerin Kapsamında;

Mevcut Risk ve Tehditlerin Belirlenmesi

- Kişisel verilerin güvenliğinin sağlanması için veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun,
- bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenmesi,
- Buna uygun tedbirlerin alınması gerekmektedir.

Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

- Kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları.
- Çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması.
- Kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olmasının sağlanması.
- Kişisel veri içeren ortamlara erişim hakkı verilirken "İzin Verilmedikçe Her Şey Yasaktır" prensibine uygun hareket edilmesi.
- Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi
- Kişisel Verilerin Mümkün Olduğunca Azaltılması
- Veri İşleyenler ile İlişkilerin Yönetimi

Bu İdari Tedbirlerin Uygulanması Gereksinimine ilişkin olarak **Humy,** şu idari tedbirleri uygular;

- Kişisel Veri İşleme Envanteri Hazırlanması
- Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
- Sözleşmeler (Veri Sorumlusu - Veri Sorumlusu, / Veri Sorumlusu - Veri İşleyen Gizlilik Taahhütnameleri
- Kurum İçi Periyodik ve/veya Rastgele Denetimler
- Risk Analizleri
- İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi)
- Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri,)
- Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)
- Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim

7. İLGİLİ KİŞİNİN KİŞİSEL VERİLERLE İLGİLİ HAKLARI

İlgili kişi, **Humy**'e başvurarak aşağıda yer alan konularda talepte bulunabilir:

1. Kişisel verilerinin işlenip işlenmediğini öğrenme,
2. Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

3. Kişisel verilerinin işlenme amacı ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
4. Kişisel verilerinin yurt içinde veya yurt dışında aktarıldığı üçüncü kişileri öğrenme,
5. Kişisel verilerinin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
6. KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerinin silinmesini, yok edilmesini veya anonim hale getirilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteme,
7. İşlenen verilerinin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle aleyhine bir sonucun ortaya çıkmasına itiraz etme,
8. Kişisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

8. İHLAL BİLDİRİMLERİ

Humy çalışanları, KVKK hükümlerini ve/veya Politika'yı ihlal ettiğini düşündüğü iş, eylem veya olguyu Komisyon'a raporlar. Komite bu ihlal bildirimi akabinde gerekli görmesi halinde toplanır ve ihlale ilişkin bir eylem planı oluşturur.

İhlal, kişisel verilerin kanuni olmayan yollarla başkaları tarafa elde edilmesi yoluyla gerçekleşmişse, Komisyon, Kurul'un 24.01.2019 tarih ve 2019/10 sayılı kararı kapsamında bu durumu **72 saat içerisinde ilgilisine ve Kurul'a bildirir.**

9. DEĞİŞİKLİKLER

Politika üzerindeki değişiklikler Komisyon tarafından hazırlanır ve **Humy** Yönetim Kurulu'nun onayına sunulur. Güncellenen Politika çalışanlara e-posta yolu ile gönderilebilir veya internet sitesi üzerinde yayınlanır.

10. YÜRÜRLÜK TARİHİ

Politika'nın işbu versiyonu **[04.10.2024]** tarihinde **Humy** Yönetim Kurulu tarafından onaylanarak yürürlüğe girmiştir.