

Es Uluslararası Tařımacılık ve Denizcilik Ticaret Anonim Őirketi

KiŐisel Veri Politikası



İÇİNDEKİLER

A. GENEL İLKELER

- A.1 Giriş
- A.2 Tanımlar
- A.3 Politikanın Amacı
- A.4 Politikanın Kapsamı
- A.5 Politikanın ve İlgili Mevzuatın Uygulanması

B. KİŞİSEL VERİLERİN İŞLENMESİ VE KORUNMASI

- B.1 Temel İlkeler
- B.2 Kişisel Verilerin İşlenme Şartları
- B.3 Özel Nitelikli Kişisel Verilerin İşlenme Şartları
- B.4 Veri Güvenliğine İlişkin Yükümlülükler
- B.5 Veri Sahibi İlgili Kişinin Hakları
- B.6 Veri Sahibinin Aydınlatılması ve Bilgilendirilmesi
- B.7 Kişisel Verilerin Aktarılması

C. KİŞİSEL VERİ SAKLAMA VE İMHA SÜRECİ

- C.1 Amaç
- C.2 Tanımlar
- C.3. Temel İlkeler
- C.4 Saklama Ortamları
- C.5 Saklamayı Gerektiren Hukuki Sebeplere İlişkin Açıklamalar
- C.6 Teknik ve İdari Tedbirler
- C.7 İmha Nedenleri
- C.8 İmha Yöntemleri
- C.9 Saklanma Süreleri
- C.10 Periyodik İmha Süreleri
- C.11 Kişisel Veri İmha Kurulu
- C.12 Politikanın Yayınlanması ve Saklanması
- C.13 Politikanın Güncellenme Periyodu
- C.14 Politikanın Yürürlüğü ve Yürürlükten Kaldırılması

D. VERİ İHLALİ

E. VERİ GÜVENLİĞİNE İLİŞKİN BİLDİRİ

A.1 GİRİŞ

“Anayasa 20. Madde : (Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir. “

Anayasal bir hak olan kişisel verilerin korunması hususu şirketimizin önem verdiği konular arasında yer almaktadır.

Politika içeriğinde; müşterilerimizin, potansiyel müşterilerimizin, çalışanlarımızın, çalışan adaylarımızın, şirket hissedarlarının, şirket yetkililerinin, şahıs firma yetkililerinin, veri işleyen kurumunda olan firma yetkililerinin, ziyaretçilerimizin, işbirliği içinde olduğumuz kurumların, kara nakliyecilerin, gümrük müşavirlerin ve üçüncü kişilerin kişisel verilerinin işlenmesi ve korunması düzenlenmektedir.

Şirketimizin kişisel verilerin korunması ile ilgili hassasiyeti gereğince yönetilen İşbu Politika'da 6698 sayılı Kişisel Verilerin Korunması Kanunu (“KVKK”) ve ilgili yönetmelikler uyarınca kişisel verilerin korunması için gerekli özen ve yükümlülüklerin yerine getirilerek gerekli idari ve teknik tedbirler alınmaktadır.

A . 2 T A N I M L A R

Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

Anonim hale getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

Başkan: Kişisel Verileri Koruma Kurumu Başkanını,

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi ve Politika kapsamında müşteriler, potansiyel müşteriler, çalışanlar, çalışan adayları, şirket hissedarları, şirket yetkilileri, şahıs firma yetkilileri, veri işleyen kurumunda olan firma yetkilileri, ziyaretçiler, işbirliği içinde olduğumuz kurumlar, kara nakliyecileri, gümrük müşavirleri

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

Kişisel verilerin işlenmesi: 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 işlemi,

Kurul: Kişisel Verileri Koruma Kurulunu,

Kurum: Kişisel Verileri Koruma Kurumunu,

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, ifade eder.

Kanun : 6698 sayılı kişisel verilerin korunması kanunu anlaşılabacaktır

A.3 POLİTİKANIN AMACI

Politikanın temel amacı Kanuna ve ilgili yönetmeliklere uygun olarak

Kişisel verilerin temin edilmesine, işlenmesine, saklanmasına, imhasına ve verilerin korunmasına ilişkin yürütülen süreç ile ilgili açıklamaları,

Veri koruma hukuku bağlamında benimsenen ilkelerini,

İlgili kişinin haklarını,

Açık rızanın alınma şeklini,

Şirketimiz tarafından alınan idari ve teknik tedbirleri, içermektedir.

Ayrıca Politika kişisel verileri işlenen ilgili kişileri verilerinin işlenmesi, korunması, saklanması ve imhası konusunda bilgilendirmekte ve Şirket tarafından belirlenen usulleri içermektedir.

A.4 POLİTİKANIN KAPSAMI

Politika, Şirketimiz tarafından hangi kişisel verilerin ne şekilde temin edilebileceğini, temin yöntemlerini, hangi amaçlarla işlenebileceğini, aktarımın hangi durumlarda hangi kurallara göre yapılacağını, ilgili kişinin haklarının neler olduğu ve nasıl kullanılacağını, verilerin saklama sürelerinin belirlenmesindeki esasları, sürenin sonunda nasıl bir imha yöntemi izleneceğini ve hangi güvenlik önlemlerinin alınacağını içermektedir.

Politikanın uygulama kapsamı ilgili kişiler için tamamiyle uygulanabileceği gibi yalnızca bir kısım hükümleri de uygulanabilecektir.

A.5 POLİTİKANIN VE İLGİLİ MEVZUATIN UYGULANMASI

Politika, Anayasal bir hak olan kişisel verilerin korunmasında ulusal mevzuat olan 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik tarafından ortaya konulan kuralların Şirket iş süreci ve faaliyetleri kapsamında somutlaştırılarak düzenlenmesinden oluşturulmuştur.

Politikada düzenlenmeyen hususlara ilişkin yürürlükteki ulusal mevzuat ve ilgili yönetmelikler uygulanacaktır.

B.1 TEMEL İLKELER

Politika çerçevesinde kişisel verilerin korunmasına ve işlenmesine ilişkin Kanun uyarınca Şirketimiz tarafından aşağıdaki ilkeler benimsenmiştir. (KVKK m.4)

- I. Hukuka ve dürüstlük kurallarına uygun olma
Kişisel veriler ancak Kanunda ve diğer Kanunlarda öngörülen usul ve esaslar çerçevesinde işlenmektedir. Dürüstlük kuralı gereği şirket iş süreci faaliyeti ile alınan veri arasındaki ölçülülük/orantılılık ilkesi dikkate alınarak işlenmektedir.
- II. Doğru ve gerektiğinde güncel olma
Şirketimiz tarafından veri işleme amacına uygun olmayan, yanlış olan verilerin, gecikmeden silinmesi veya düzeltilmesi için gerekli her makul adım gecikmeksizin atılmaktadır. Kişisel verilerin değişmiş veya güncelliğini yitirmiş olması durumlarında hem Şirketimizin hem de veri sahibinin çıkarlarına uygun olarak güncel haliyle değiştirilmektedir.
- III. Belirli, açık ve meşru amaçlar için işlenme
Belirli, açık ve meşru amaçlar için işlenme ilkesi gereğince Şirketimiz veri işlenmesini iş süreci ve sunmuş olduğu hizmetle bağlantılı olarak açık ve kesin olarak belirlemektedir. İşlenen veriler sadece amacın gerçekleştirilmesi için gerekli olanla sınırlı tutulmaktadır.

IV. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma
Şirketimiz veri işleme amacının gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmaktadır. Sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik ise Kanunun 5. maddesinde düzenlenmiş olan şartlardan birinin gerçekleşmesi gerekmektedir.

V. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

Verilerin işlenmesi sadece amacın gerçekleştirilmesi için gerekli olan ile sınırlı tutulacaktır. Alınan veriler, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilecektir. Bir verinin daha fazla saklanması için geçerli bir sebep olmaması durumunda verinin boyutu ve niteliğine göre silinecek veya anonim hale getirilecektir. Bu bende ilişkin detaylı düzenleme Politikanın C.8 ve C.9 maddelerinde yapılmıştır.

B.2 KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

T.C ANAYASASI "Temel Hak ve Hürriyetlerin Sınırlanması" madde 13:

Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir.

Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçünlülük ilkesine aykırı olamaz.

Kişisel verilerin Anayasa 20. madde hükmü gereğince ilgili kişinin açık rızası veya aşağıda yer verileceği üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu madde 5 uyarınca sayılan istisnalar dışında işlenmesi yasaktır.

95/46 EC sayılı Avrupa Birliği Direktifine göre rıza, ilgili kişinin kendisiyle ilgili veri işlenmesine, özgür iradesiyle, konu hakkında yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işleme sınırlı olarak verdiği onay beyanıdır.

6698 sayılı Kişisel Verilerin Korunması Kanunu 5. maddesinde kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğini söylediği gibi aynı Kanunun ikinci maddesinde ilgili kişinin açık rızası olmasa dahi bazı hallerde kişisel verilerin işlenebileceğini öngörmektedir.

İşbu Politika ile Şirketimiz kişisel verilerin korunması ve işlenmesi sürecini anayasal güvenceye sahip Kişisel Verilerin Korunması hususunda TC Anayasası ile doğrudan bağlantılı olarak yürütmektedir.

Daha öncesinde "Temel İlkeler" bölümünde bahsettiğimiz gibi Şirketimiz ilgili mevzuat kapsamında benimsediği ilkeler çerçevesinde kişisel verileri ancak kanunun öngördüğü hallerle sınırlı olarak veya kişinin açık rızasını alarak işlemektedir.

*Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (KVKK md.5)

Kişisel Veri Sahibinin Açık Rıza Var ise	Aşağıdaki şartlardan birinin varlığı halinde, Şirketimiz tarafından ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesi mümkündür:
--	--

	<p>Kanunlarda açıkça öngörülmesi (Örneğin: Kolluk tarafından bir suç soruşturması sebebiyle, 2559 sayılı Polis Vazife ve Salahiyet Kanununun 5'inci maddesi uyarınca şüphelilerin parmak izinin alınması.)</p>
	<p>Fili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için gerekli olması (Örneğin: Veri sahibinin şuurunun yerinde olmadığı veya hayat veya beden bütünlüğünün korunması amacıyla, tıbbi müdahale yapılması sırasında kişisel verileri işlenebilecektir.)</p>
	<p>Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması</p>
	<p>Şirketin hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması (Örneğin: Şirketin çalışanına çalışanına maaş ödeyebilmesi için banka hesap numarası, evli olup olmadığı, bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi verileri işlemesi bu bendin verdiği yetkiye istinaden gerçekleşmektedir.)</p>
	<p>İlgili kişinin kendisi tarafından alenileştirilmiş olması İlgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinebilecek hale gelen bu tür verilerin işlenmesinde korunan hukuki yarının ortadan kalktığı kabul edilmektedir.</p>
	<p>Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması (Örneğin: Şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması bu bent gereğince hukuka uygun sayılacaktır.)</p>
	<p>İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Şirketimizin meşru menfaatleri için veri işlenmesinin zorunlu olması Kişisel verilerin işlenmesine ilişkin temel ilkeler ve Şirketimiz ile ilgili kişinin menfaat dengesi gözetilmektedir.</p>

B.3 ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

Politikada aşağıda yer verileceği üzere özel nitelikli kişisel veri; başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olmasına veya ayrımcılığa maruz kalmasına neden olabilecek nitelikte verilerdir.

Bu sebeple 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, biyometrik verisi veya haklarında verilen ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler özel nitelikli(hassas) veri olarak kabul edilmektedir.

Özel nitelikli kişisel verileriniz Şirketimiz tarafından hassasiyetle 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik ve Kurul tarafından belirlenen yeterli önlemlere uygun olarak aşağıdaki tabloda gösterildiği hallerde işlenmektedir:

(KVKK md.6)

Kişisel Veri Sahibinin Açık Rızası Var ise	Kişisel Veri Sahibinin Açık Rızası Yok ise
	Sağlık ve cinsel hayat <u>dışındaki</u> kişisel veriler kanunda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir.
	Sağlık ve cinsel hayata <u>ilişkin</u> kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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 ilgilinin açık rızası aranmaksızın işlenebilir. Örneğin: Askerlik yapacak kişilerin bazı özel sağlık bilgilerinin ilgili kanun hükümleri uyarınca işlenmesi, yine hastanelerin, eczanelerin ya da Sosyal Güvenlik Kurumunun hastalarla ilgili veri işleme bu kapsamda değerlendirilecektir. Sağlık Bakanlığı ile her türlü sağlık kuruluşunun ve Sosyal Güvenlik Kurumunun bu amaçlar çerçevesinde yazılı tuttukları veriler ve kayıtlar bu kapsamda değerlendirilecektir.

B.4 VERİ GÜVENLİĞİNE İLİŞLİN YÜKÜMLÜLÜKLER

Kişisel verilerin korunmasında ve işlenmesinde güvenliğin sağlanması belli bir aşama veya veriye özgü olmayıp sürekli olan bir sorumluluktur. Bundan dolayı Şirketimiz veri güvenliğine ilişkin önlemlerin bir defa saptanması ve gerçekleştirilmesiyle yetinmemektedir. Tarafımızca alınan önlemler, değişen ve gelişen teknoloji ve güvenlik uygulamaları dikkate alınarak yenilenmektedir.

Veri güvenliğine ilişkin alınan idari ve teknik tedbirler Politika'nın C.6. maddesinde ayrıntılı olarak düzenlenmiştir.

Şirket çalışanlarının Politika'ya uymaması halinde İş Yeri İç Yönetmeliği'nde belirtilen idari yaptırımlar uygulanacaktır.

B.2 VERİ SAHİBİ İLGİLİ KİŞİNİN HAKLARI

İlgili Kişi;

Kişisel verilerinin işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgi talep etme, işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında aktarıldığı üçüncü kişileri bilme, eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, KVKK ve ilgili mevzuat hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde 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, kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme, haklarına sahiptir.

İlgili kişinin haklarını ve bu haklarını kullanabileceği yöntemlerin anlaşılması Şirketimiz tarafından üzerinde durulan önemli konulardan birisidir.

Bu haklar Şirketimiz tarafından yapılan veri işleme, saklama, aktarım, silme, anonimleştirme ve yok etme faaliyetlerinin her aşamasına ilişkindir.

Kişisel veri sahipleri Kanununun 11. maddesinde belirtilen hakları ile ilgili taleplerini öncelikle Şirketimize iletmeleri zorunludur.

Şirketimiz alınan talebi ücretsiz olarak veya işlemin ayrıca bir maliyeti gerektirmesi halinde, Kişisel Verileri Koruma Kurul'u tarafından belirlenen tarifeye göre alacağı ücret mukabilinde en kısa sürede ve en geç otuz gün içerisinde sonuçlandıracak ve ilgili veri sahibini bilgilendirecektir.

Şirketimiz konu edilen hususta hatalı ise alınan ücret ilgiliye iade edilecektir.

Kanununun 11. maddesinde belirtilen haklardan ilgili veri sahibi kullanmayı talep ettiği hakkına yönelik açıklamalarını içeren talebini <https://www.esitr.com> adresindeki formu doldurarak web sayfası üzerinden veya formun imzalı bir nüshasını Kaya Sultan Sokak, Hayriye İş Merkezi, No:83 Kat:5 Kozyatağı / İstanbul adresine kimliğini tespit edici belgeler ile bizzat elden iletebilir, noter kanalıyla gönderebilir veya ilgili formu info@esitr.com adresine güvenli elektronik imzalı olarak iletebilir.

B.6 VERİ SAHİBİNİN AYDINLATILMASI VE BİLGİLENDİRİLMESİ

Şirketimiz, anayasal bir hak olan kişisel verilerin korunması konusunda, veri sahibinin haklarının kullanımına ilişkin Anayasa madde 20 ve KVK Kanunu 11. Maddesine uygun olarak şeffaf bilgilendirme yapmaktadır.

İlgili kişinin kanun maddesinde aşağıda belirtilen konular dışında bilgilendirilmesi gerektiği durumlarda göz önüne alınarak (kişisel verilerin işlendiği her durumda açık rıza olsun ya da olmasın, kişisel veri amacı değiştiğinde) işleme faaliyetine ilişkin olarak aydınlatma yükümlülüğü yerine getirilmektedir.

Veri sorumlusunun ve varsa temsilcisinin kimliği
Kişisel verilerin hangi amaçla işleneceği
Kişisel verilerin kimlere ve hangi amaçlarla aktarılacağı
Kişisel veri toplamanın yöntemi ve hukuki sebebi
İlgili kişinin Kanununun 11. maddesinde sayılan diğer hakları

Ziyaretçilere ilişkin olarak; Şirketimiz tarafından Kanun ve ilgili mevzuat kapsamında güvenlik kamerası ile izleme faaliyeti sonucunda elde edilen kişisel verilerin güvenliğinin sağlanması için gerekli teknik ve idari tedbirler alınmaktadır.

Şirketimiz, müşterilerin ve kurum ile irtibatlı kişilerin güvenliğini sağlamak ve müşterilerin aldıkları mal/hizmete ilişkin menfaatlerini korumak, fiziksel mekan güvenliğini sağlamak amacıyla bina içerisi ve dışısında güvenlik kamera sistemi kullanmaktadır. Bununla birlikte misafir giriş ve çıkışları tarafımızca kayıt altına alınmaktadır.

Güvenlik kamerası ile kayıt altına alınan ve tarafımızca muhafaza edilen kayıtlara erişim sağlanması yalnızca Şirket tarafından bu konuda sınırlı olarak yetkilendirilen çalışan kişiler tarafından gerçekleştirilebilmektedir.

B.7 KİŞİSEL VERİLERİN AKTARILMASI

Politika gereğince Şirketimiz tarafından ayrı bir tüzel kişiliğe sahip olan her türlü tüzel kişi ve Şirketimizle organik bağı bulunmayan her türlü gerçek kişi arasında yapılan kişisel verilerin aktarımı Kanun ve ilgili mevzuata uygun yapılmaktadır.

I. Kişisel Verilerin Yurt İçinde Aktarılması

Şirketimiz içinde bir verinin farklı birimler ya da kişiler arasında paylaşılması aktarım olarak nitelendirilmemektedir. Bu şekilde Şirket içerisi paylaşımlar ikincil işleme faaliyetleri olmaktadır. Örneğin: Pazarlama departmanı tarafından sözleşme yapılan bir müşterinin verilerinin, sözleşme konusu hizmetin sunulması için operasyon birimine, fatura işlemleri için muhasebe birimine gönderilmesi aktarım değil; ikincil işleme faaliyetidir.

Ayrıca, tamamen Şirketimiz adına vekaleten ve tarafımızın gözetim, denetim ve kontrolü altında üçüncü kişiler tarafından gerçekleştirilen veri işleme faaliyetleri veri aktarım faaliyeti değildir. Örneğin: Şirketimizin çalışanlarının özlık bilgilerinin, erişim ve kontrol yetkisi tamamen tarafımıza ait olmakla birlikte, kriptografik olarak korunmuş halinin, kiralanan bir sunucuda tutulması veri aktarım faaliyeti kapsamında değildir.

Şirketimiz özel nitelikli kişisel verilerin aktarımı bakımından Politika gereğince hem aktarımı uygun hale getirecek bir işleme şartının bulunduğundan hem de gerekli güvenlik önlemlerinin alındığından emin olarak hareket etmektedir.

II. Kişisel Verilerin Yurt Dışına Aktarılması

Şirketimiz verilerin yurt dışına aktarılması söz konusu olduğunda farklı risklerin gündeme gelebileceği yaklaşımıyla gerekli teknik ve idari önlemleri almaktadır.

Yurt Dışına Aktarımın Koşulları:

İşleme şartlarının bulunması
Yeterli korumanın bulunması
Yeterli korumanın bulunduğu ülkeler
Yeterli korumanın Şirketimiz tarafından taahhüt edilmesi

Şirketimiz tarafından veri işleme şartlarından açık rızanın bulunması durumunda kişisel veriler doğrudan yurt dışına aktarabilir.

Kanunun 9. maddesinde Yabancı Ülkelerde yeterli koruma bulunup bulunmadığı Kurulca belirlenerek ilan edilecektir. Ancak henüz Kurul tarafından herhangi bir belirleme ve ilan yapılmamıştır.

Şirketimiz Kurulun ilanını güncel olarak takip ederken aynı zamanda yurt dışı veri aktarımı söz konusu olduğunda yazılı olarak yeterli korumayı sağlayacağını taahhüt etmekle birlikte Kurula başvurarak izin alacaktır.

Şirketimizin iş süreci faaliyetlerini uluslararası alanda gerçekleştirmektedir. Bundan dolayı yurt dışına veri aktarımı yapılmaktadır. Şirketimiz bu aktarımı gerçekleştirirken güvenli elektronik posta, kriptografik şifreli cloud sistemi kullanmaktadır. Söz konusu verilerin imhası sürecinde değer düzensizliğini sağlayan anonimleştirme yöntemlerini kullanmaktadır.

C. Kişisel Veri Saklama ve İmha Süreci

C.1 AMAÇ

Kişisel Veri Saklama ve İmha Politikası ("Süreç") faaliyetlerimiz sırasında elde edilen kişisel verilerin saklanması ve imhasına dair izlediğimiz yöntemler hakkında usul ve esasları belirlemek amacıyla hazırlanmıştır.

Es Uluslararası Taşımacılık ve Denizcilik Ticaret A.Ş. ("Şirket") olarak, müşterilerimizin, potansiyel müşterilerimizin, çalışan adaylarımızın, şirket hissedarlarının, şahıs firma yetkililerinin, şirket yetkililerinin, veri işleyen konumunda olan firma yetkililerinin, ziyaretçilerimizin, işbirliği içinde olduğumuz kurumların, kara nakliyecilerinin, gümrük müşavirlerinin ve sair üçüncü kişilerin kişisel verilerinin saklanma ve imha yöntemlerini göstermektedir.

Şirketimiz, veri sorumlusu sıfatı ile yürütmekte olduğu iş süreçleri esnasında elde ettiği gerçek kişilere ait tüm kişisel verileri Türkiye Cumhuriyeti Anayasası, 6698 sayılı Kişisel Verilerin Korunması Kanunu ('KVKK') ve 28.10.2017 tarihli Resmi Gazetede yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") başta olmak üzere ilgili mevzuata ve yönetmeliklere uygun olarak saklanmasını ve imha edilmesini taahhüt etmektedir.

Ayrıca, Şirketimiz kişisel verilerin saklanması ve imhası sürecinde, bu verilerin hukuka aykırı olarak saklanmasını önlemek ve/veya imhası amacıyla her türlü teknik ve idari tedbiri almaktadır.

Şirketimiz, kişisel verilerin saklanması ve imhası süreçlerinde özel hayatın gizliliğinin korunmasına önem vermekte ve veri güvenliğini en üst seviyede gözetmektedir.

C.2 TANIMLAR

Şirket: Es Uluslararası Taşımacılık ve Denizcilik Ticaret A.Ş.

Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişidir.

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 getirilmesini ifade eder.

Kanun: 24/3/2016 tarihli ve 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 ortamdır.

Kişisel veri işleme envanteri: Veri sorumlularının 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 oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri ifade eder.

Kişisel veri saklama ve imha süreci: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikadır.

Kurul: Kişisel Verileri Koruma Kurulu

Periyodik imha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla res'en gerçekleştirilecek silme, yok

etme veya anonim hale getirme işlemidir.

Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumlularının sicilidir.

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.

Kişisel Verilerin Silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.

Kişisel Verilerin Yok Edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Anonim Hale Getirme: Daha öncesinde bir kişiyle ilişkilendirilmiş olan verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

C.3 İlkeler

Süreç çerçevesinde kişisel verilerin saklanması ve imhası hususlarında Şirketimiz tarafından aşağıda yer alan ilkeler benimsenmiştir.

Şirketimiz tarafından kişisel verilerin hukuka aykırı olarak işlenmesi ve bu verilere yetkisiz kişiler tarafından erişimin önlenmesi amacıyla Politika'nın C.6. maddelerinde belirtilen tüm teknik ve idari tedbirler alınmaktadır.

Kişisel verilerin işleme şartlarının tamamıyla ortadan kalkması durumunda veriler 3 ay içerisinde Şirketimiz tarafından re'sen veya ilgili kişinin talebi üzerine İşbu Politika'nın C.8. maddesinde belirtilen yöntemler ile silinir, yok edilir veya anonim hale getirilir.

Kurul tarafından aksi karar alınmadıkça Şirketimiz, imha yöntemine; kişisel verinin niteliğine, büyüklüğüne, çeşitliliğine, verinin bulunduğu fiziksel ortamların yapısına, veri işleme amacına, verinin işleme sıklığına göre karar vermektedir.

Kişisel veriler Politika'nın C.9 maddesinde belirtilen süreler sonunda silinir, yok edilir veya anonim hale getirilir. Şirketimiz tarafından gerçekleştirilen her imha işlemi kayıt altına alınmakta ve söz konusu kayıtlar diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süre ile saklanmaktadır.

C.4 SAKLAMA ORTAMLARI

Şirketimiz tarafından kişisel veriler, ilgili verinin niteliğine uygun olarak saklanmaktadır.

Saklama işlemi, Kanun, ilgili yönetmelikler, taahhütnameler, politikalar, rehberler ve Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca belirlenmiş veri güvenliği prensipleri çerçevesinde gerçekleştirilmektedir.

Matbu (Fiziksel) Ortamlar	Birim Dolaplar, Arşiv
Yerel Digital Ortamlar	Sunucular, Sabit ya da Taşınabilir Diskler
Bulut Ortamlar	Microsoft Cloud, Kriptografik Yöntemlerle Şifrelenmiş İnternet Tabanlı Sistemler

Elektronik Ortamlar	Antivirüs(NOD 32) Sunucular(Microsoft Cloud, MS SQL DB, ORACLE) Güvenlik Yazılımı(FILE SERVER, CRYPTOLOG, AD DC, DHCP) Ofis Yazılımı(OFİS 365, LOGO TIGER-BORDRO, SHARE POINT PORTAL, ERP VE CRM SİSTEMLERİ, PDKS SİSTEMLERİ, SİSTEM MUHASABE) Çıkarılabilir Bellekler ve Mobil Cihazlar
---------------------	--

C.5 SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

Şirketimiz, iş süreci faaliyeti kapsamında elde ettiği tüm kişisel verileri aşağıda yer verilen amaçlar ile sınırlı olarak Kanun ve ilgili mevzuatta öngörülen güvenlik tedbirlerine uygun olarak saklamaktadır.

- Kişisel verilerin sözleşmenin kurulması ve ifası ile doğrudan doğruya ilgili olması
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla bağlantılı olması
- Kişisel verilerin, kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketin meşru menfaatleri için saklanması zorunlu olması
- Şirketin herhangi bir hukuki yükümlülüğünü yerine getirebilmesi
- Veri sahiplerinin açık rızalarının bulunması
- Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi

C.5.1 SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

Şirketimiz aşağıda belirtilen amaçlar ile sınırlı olarak kişisel veri işleme faaliyetlerini gerçekleştirmektedir.

- Şirket bünyesinde gerçekleştirilen denizyolu taşımacılığı, havayolu taşımacılığı, karayolu taşımacılığı, sigorta, gümrükleme ve depolama hizmetlerinin etkin şekilde yürütülmesi
- Şirketin ticari faaliyetleri ile sözleşme süreçlerinin yürütülmesi
- Yönetim faaliyetlerinin yürütülmesi
- Lojistik faaliyetlerinin yürütülmesi
- Şirketin genel ve ticari güvenliğinin temin edilmesi
- Ticari ortaklar ile stratejilerin doğru planlanması, yürütülmesi, yönetilmesi
- İş ortakları veya tedarikçilerle olan ilişkilerin yönetimi
- Yatırımcı ilişkilerinin yönetilmesi
- Finans ve muhasebe işlerinin yürütülmesi
- Kurumsal işleyişin sağlanması, yönetim ve iletişim faaliyetlerinin icrası
- İnsan kaynakları politikalarının en iyi şekilde planlanması ve uygulanması
- Müşteriler, ticari ortaklar, tedarikçiler, çalışanlar, çalışan adayları için veri tabanlarının oluşturulması
- Çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi
- Çalışanlar için yan hak ve menfaatleri süreçlerinin yürütülmesi
- Çalışan ve stajyer adaylarının başvuru süreçlerinin yürütülmesi
- Ürün ve hizmetlerden Kişisel Veri Sahipleri'nin en iyi şekilde faydalandırılması, onların talep, ihtiyaç ve isteklerine göre özel hale getirilerek önerilmesi
- Yetkili kişi, kurum ve kuruluşlara mevzuattan kaynaklı bilgi verilmesi
- Şirkete talep ve şikayetlerini ileten kişisel veri sahipleri ile iletişime geçilmesi, talep ve şikayet yönetiminin sağlanması
- Şirket hukuk işlerinin icrası/takibi
- Acil durum operasyonlarının koordinasyonu
- Bilgi güvenliği süreçlerinin yürütülmesi

Risk yönetimi süreçlerinin yürütülmesi
Saklama ve arşiv faaliyetlerinin yürütülmesi
İş sağlığı ve güvenliği eğitimlerinin koordinasyonu
İş kaza kayıtlarının tutulması
Güvenlik amacıyla veya yasal zorunluluklar sebebi ile görüntü kayıt süreçlerinin yürütülmesi
Ziyaretçi kayıtlarının oluşturulması

C.6 TEKNİK VE İDARİ TEDBİRLER

Şirketimiz kişisel verilerin hukuka aykırı olarak işlenmesini önlemek için teknolojik ve bilimsel gelişme seviyesi, iş süreci kapsamında işleme faaliyetinin önemi, kapsamı, bağlam ve amacı, gerçek kişilerin hak ve özgürlükleri açısından çeşitli olasılık ve ciddiyetlere sahip risklerin olup olmadığı uygulama maliyetine göre dikkate alınarak kanunlar ve ilgili yönetmeliklerle bağlantılı olarak gerekli teknik ve idari önlemler alınmaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanununda açıkça yer almamasına rağmen Kurul tarafından benimsenen ve GDPR ile de bağlantılı olarak Şirketimiz tarafından "tasarımdan itibaren mahremiyet" (privacy by design) benimsenmiştir.

Şirketimiz tarafından alınmış olan tüm idari ve teknik tedbirlere aşağıda yer verilmektedir.

C.6.1 İDARİ TEDBİRLER

Kişisel verilere erişimi olan tüm şirket personeline KVKK ve veri güvenliği kapsamında kişisel veriler, bilgi güvenliği, özel hayatın gizliliği konularında eğitimler verilmekte, çalışanların bilinçlendirilmesi için çalışmalar yapılmaktadır.

Kişisel verilere erişim Şirket İç Yönetmeliği gereği verilere erişmesi gerekli personel ile sınırlandırılır. Erişimin sınırlandırılmasında ayrıca verinin özel nitelikli kişisel veri olup olmadığı dikkate alınır. İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, Şirket bu durumu en kısa sürede ilgisine ve Kurul'a bildirir.

Şirket bilgi güvenliği, özel hayatın gizliliği, kişisel verilerin korunması alanlarındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti almaktadır.

Şirket kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar veya yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.

KVKK madde 12/2 uyarınca ; " Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınmasında bu kişilerle birlikte müştereken sorumludur." Şirket Kanundaki bu düzenleme kapsamında kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde, ilgili üçüncü kişilerle protokoller, taahhütnameler imzalamakta ve mevcut sözleşmelerine eklenen hükümler ile veri güvenliğini sağlamaktadır.

Kişisel verilerin muhafazasını sağlamak için verilerin bulunduğu fiziksel ortamların kilit altında tutulması, yetkisiz erişimlerin önlenmesi, fiziksel ortamlara giriş çıkışların kontrol altına alınması hususunda gerekli idari ve teknik önlemler alınmaktadır.

C.6.2 TEKNİK TEDBİRLER

Şirket yaptırdığı sızma testleri ile şirketin bilişim sistemlerine yönelik risk, tehdit, zafiyet ve açıklıklar varsa ortaya çıkarmakta ve gerekli önlemleri almaktadır.

Şirket bilişim sistemleri teçhizatı, yazılım ve verilerin güvenliği için gerekli önlemleri almaktadır.

Erişim yetki ve rol dağılımları için prosedürler oluşturulmakta ve uygulanmakta, yetki matrisi uygulanmakta, erişimler kayıt altına alınarak uygunsuz erişimler kontrol altında tutulmakta, saklama ve imha politikasına uygun imha süreçleri tanımlanmakta ve uygulanmaktadır.

Kişisel verilerin güvenli olarak saklanmasını sağlayan yedekleme programları kullanılmaktadır.

Bilgi sistemleri güncel halde tutulmakta, kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.

Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal ve yazılımsal (güvenlik duvarları, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.

Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.

Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.

Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.

Kişisel verilerin işlendiği elektronik ortamlarda parolalar kullanılmaktadır.

Kullanıcıların sistemlere giriş yaparken benzersiz kullanıcı adı ve şifre kullanmaları sağlanmaktadır.

Şirketimiz tarafından özel nitelikli kişisel verilerin korunmasına ilişkin ek güvenlik önlemleri alınmaktadır. Bu önlemler aşağıda sayılanlardan ibarettir.

Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlar ile gizlilik sözleşmeleri yapılmaktadır.

Özel nitelikteki kişisel verilere erişimi olan çalışanların isim, ünvan ve görevleri Politika'nın C.11. maddesinde belirtilmiştir.

Özel nitelikte kişisel verilere erişimi olan çalışanların yetkilerinin işbu Politikaya uygunluğu belli periyotlarla denetlenmektedir.

Görev değişikliği veya işten ayrılan çalışanların yetkisi dahilinde erişebildiği dijital ve fiziksel envanter geri alınmaktadır.

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testleri düzenli olarak yapılmakta, test sonuçları kayıt altına alınmaktadır.

Özel nitelikli kişisel verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak KEP hesabı kullanarak aktarılmaktadır. Taşınabilir bellek yoluyla aktarılması gerekiyorsa kriptografik şifrelemeler içeren USB'ler ile aktarım yapılmaktadır. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak 'gizli' formatta gönderilmektedir.

C. 7 İMHA NEDENLERİ

Şirketimiz tarafından işlenen kişisel veriler aşağıda belirtilen durumlarda İşbu Politika C.8.1 C.8.2 C.8.3. maddelerinde belirtilen yöntemler dahilinde re'sen silinir, yok edilir veya anonim hale getirilmektedir.

İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası
İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması
Kişisel veri işleme şartının yalnızca açık rıza şartına bağlandığı hallerde, ilgili kişinin açık rızasını geri alması
İşbu Politika'nın C.9. maddesinde belirtilen, saklamayı gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılabileceği herhangi bir şartın mevcut olmaması
Kanunun 5. ve 6. maddelerinde sayılan nedenlerin ortadan kalması halinde ilgili kişinin istemi

Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenler aşağıdakilerden ibarettir:

- Kanunlarda açıkça öngörülmesi.
- Fili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukukun geçerliliği tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

C.8 İMHA YÖNTEMLERİ

Şirketimiz tarafından iş süreci faaliyetleri kapsamında elde edilen kişisel veriler ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresi sonunda re'sen veya ilgili kişinin başvurusu üzerine İşbu Politika'da belirtilen teknikler ile imha edilmektedir.

Silme, Yok Etme, Anonim Hale Getirme şeklinde sayılan işlemlerin ortak amacı kişisel verinin ilgili kişiyi teşhis edemeyecek şekilde ortadan kaldırmasıdır.

C.8.1 KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirketimiz bünyesinde bannadınlan kişisel veriler, saklandıkları kayıt ortamlarına uygun şekilde silinmektedir. Ayrıca Şirketimiz gerekli görürse kendisi adına kişisel verileri silmesi konusunda bir uzman ile anlaşabilecektir. Bu durumda, kişisel veriler bu konuda uzman olan kişi veya kurum tarafından ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek şekilde güvenli olarak silinecektir.

<p>Matbu Ortamda Bulunan Kişisel Veriler</p>	<p>Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemez ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünmez hale getirilmesi şeklinde yapılır.</p>
<p>Yerel Dijital Ortamlar</p>	<p>Sunucularda yer alan kişisel veriler, sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silinir. Flash tabanlı saklama ortamlarında tutulan kişisel veriler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.</p>

Bulut Ortamlar	<p>Bulut ortamda tutulan kişisel veriler; yasal zorunluluklar sebebi ile ilgili veriye ulaşması gereken yetkili kişiler hariç, diğer kullanıcılar için bir daha erişilemeyecek şekilde dijital komutlarla silinir. 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.</p> <ol style="list-style-type: none">1. Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.2. Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması,
Elektronik Ortamlar	<p>Elektronik ortamda yer alan kişisel verilerden saklanması gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.</p>

C.8.2 KİŞİSEL VERİLERİN YOK EDİLMESİ

Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir. Şirketimiz tarafından, kişisel verilerin yok edilmesiyle ilgili her türlü teknik ve idari tedbiri alınmaktadır.

Matbu Ortamda Tutulan Kişisel Veriler İçin Fiziksel Yok Etme	Kağıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kağıt kırma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Yazılımdan ve Donanımdan Güvenli Olarak Silme	Hardware ortamında tutulan kişisel veriler bir daha kurtulamayacak şekilde dijital komutla silinir ve gerekli şifreleme anahtarının tüm kopyaları yok edilir.
Dijital Depolama Alanından Silme	Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılabilir hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

C.8.3 KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirtenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Şirket olarak saklama süresi sona eren kişisel verileri anonim hale getirmekte, veri ile ilgili kişi arasındaki bağı koparmakta ve bu sayede ilgili kişinin tespit edilmesini engellemekteyiz.

Anonimleştirme yöntemi olarak verilerin değer düzensizliğini sağlayan rastgeleleştirme, veri karması ve gürültü eklenmesi gibi veri ile ilgili kişi arasındaki bağı tamamen ortadan kaldırmayan fakat verinin doğruluğunu azaltmak suretiyle bu bağı zayıflatan yöntemler kullanılmaktadır.

C.9 SAKLANMA SÜRELERİ

Şirketimiz saklama sürelerini Şirketin ve veri sahibinin meşru menfaati ile birlikte ilgili mevzuat gereğince belirlemiştir. Kişisel verileriniz belirlenen bu sürelerin sonunda Şirket tarafından re'sen veya ilgili kişinin başvurusu üzerine Politika'nın C.8. maddesine uygun olarak silinir, yok edilir ve anonim hale getirilir.

Veri Kategorisi	Kişisel Veri	Veri Saklama Süresi	
Kimlik	Ad-Soyad, Anne-Baba Adı, Anne Kızlık Soyadı, Doğum Tarihi ve Yeri, Medeni Hali, Nüfus Cüzdanı Seri Sıra Numarası, T.C Kimlik Numarası, Ehliyet	10 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde
İletişim	Adres Numarası, E-posta Adresi, İletişim Adresi, Kayıtlı Elektronik Posta Adresi(KEP), Telefon Numarası	10 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde
Lokasyon	Bulunduğu Yerin Konum Bilgileri, Araç Takibi, Arvento	2 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde

Özlük	Kimlik, Özgeçmi Bordro Bilgileri, Sağlık Raporu, Diploma, Eğitim Bilgileri, Personel Aile Bilgisi, Fotoğraf, Adres, İkametgah, Özgeçmiş Yazılması Halinde İlgili Alanlar, Adli Sicil Kaydı, İş Yeri Sözleşme ve Ekleri	10 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde
Hukuki İşlem	Adli Makamlarla Yazışmalardaki Bilgiler, Dava Dosyasındaki Bilgiler	10 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşteri İşlem	Hizmet Siparişleri Geçmişi, Banka Bilgileri, İletişim, Kimlik, Çek Bilgileri, Fatura Bilgileri, Vergi Numarası, Ticaret Sicil Gazetesi, Faaliyet Belgesi, Yetkililik Belgesi, İlgili Firmaya Yönelik İşlemler	2 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde

Fiziksel Mekan Güvenliđi	Çalıřan ve Ziyaretçileri Giriř-Çıkıř Kayıt Bilgileri,Kamera Kayıtları,Ordino(ilgili řirket personeli)Teslim Almaya Gelenlerden Alınan Kimlik Bilgisi, Alarm Sistemi için ŞifreSahiplerinden Alınan Ad-Soyad ve İletişim Bilgileri, KameraKayıtları, AraçlardaTaşıt TanımaSistemi(OPET), Cep Telefonu Fatura Dökümü	2 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde
İřlem Güvenliđi	IP Adresi Bilgileri, E-Mail Yönetim Şifreleri, ESED Anti-Virüs, Microsoft Teams Cloud Sistemi*	2 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde
Mesleki Deneyim	Kurs Katılım Belgeleri,Sertifikalar, Diploma, İř Deneyim Bilgileri, Yetki Belgeleri,Finansal Performans Raporları	Çalıřan Adayları için 1 YIL Diğerleri için 10 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde

Saęlık Bilgileri	Saęlık Raporları, Engellilik Durumuna Ait Bilgiler, Kan Grubu Bilgisi, Kişisel Saęlık Bilgileri, Kullanılan Cihaz ve Protez Bilgileri vb.	15 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde
Ceza Mahkumiyeti ve Güvenlik Tedbirleri	Ceza Mahkumiyetine İlişkin Bilgiler, Güvenlik Tedbirlerine İlişkin Bilgiler,	10 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde

Finansal Bilgiler	Ödeme Bilgileri, Banka Bilgileri, Bilançolar, Finansal Performans(FİNDEKS) , Malvarlığı Bilgileri, Firmaların Cari Belgeleri, İmza Sirküleri, Finansal Veri İçerikleri, Firmaların Cari Belgeleri, Ticari Defterler, Personel Görevleri, Genel Kurul Pay Defteri, Kredibilite Amaçlı Mali Bilgiler, Fatura Bilgileri, Swift Bilgileri, Satın Alınan Mal Değeri Bilgileri, Beyannameler, Satış Bedelleri, Sigorta Bilgileri	10 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde
Risk Yönetimi	Ticaret Odasından Alınan Müşteri Bilgileri, Findex Notu, Yetki Belgeleri, Sigorta Belgeleri, Yeterlilik Belgeleri, Vergi Levhaları, İmza Sirküleri	10 YIL	Saklama süresinin bitimini takiben 180 gün içerisinde

C.10 PERİYODİK İMHA SÜRELERİ

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik madde 11 gereğince Şirketimiz, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, şirketimizde her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilmektedir.

Kişisel verileri resen silme, yok etme veya anonim hale getirme süreleri

MADDE 11 –(3) Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir.

C.11 KİŞİSEL VERİLERİ İMHA KURULU

İmha Kurulundaki kişilerde veya bu kişilerin görevlerinde değişiklik olması halinde değişikliğin meydana gelmesinden itibaren 1 ay; her halükarda periyodik imhadan en geç 1 hafta öncesine kadar gerekli güncelleme yapılarak ilan edilir.

İmha Kurulu 1 (bir) yıl süreyle oluşturulmuştur.

KİŞİ	UNVAN	GÖREV
MEHMET DENİZ	GENEL MÜDÜR	Görevi dahilinde olan süreçlerin İşbu Politika ve mevzuat çerçevesinde saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
ŞEBNEM DENİZ	SATIŞ MÜDÜRÜ	Görevi dahilinde olan süreçlerin İşbu Politika ve mevzuat çerçevesinde saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
ASLI METE	GENEL MÜDÜR YARDIMCISI	Görevi dahilinde olan süreçlerin İşbu Politika ve mevzuat çerçevesinde saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
İLKE GÜLÇİN GÜRER	İŞ PLANLAMA MÜDÜRÜ	Görevi dahilinde olan süreçlerin İşbu Politika ve mevzuat çerçevesinde saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

C.12 POLİTİKANIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kağıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır. Basılı kağıt nüshası şirketin arşivlerinde saklanır ve bir kopyası da tüm çalışanların görebileceği şekilde şirket merkezine asılır. Elektronik kopyası ise internet sitesinden kamuya açıklanır.

C.13 POLİTİKANIN GÜNCELLENME PERİYODU

Kanunda zorunlu bir değişiklik öngörülmediği sürece, politika her imha döneminden bir ay önce şirketin hukuki danışmanları tarafından gözden geçirilir ve gerekli olan bölümler güncellenir.

C.14 POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, tarihinde Şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Herhangi bir nedenle yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları İmha Kurulu tarafından iptal edilerek imzalanır ve en az 5 yıl süre ile Şirket tarafından saklanır.

D. VERİ İHLALİ

Kişisel verilere yetkisiz üçüncü kişi tarafından erişilmesi, veri sorumlusu ya da veri işleyen tarafından gerçekleştirilen hukuka aykırı eylem, verinin yanlış alıcıya gönderilmesi, kişisel veri içeren bilişim cihazlarının kaybolması veya çalınması, kişisel verilerin izinsiz olarak başkalaştırılması, kişisel verilere erişim sağlanamaması durumlarında veri ihlali gerçekleşmiş sayılır. Bu gibi durumların gerçekleşmesi halinde Şirketimiz ihlal niteliği taşıyan olayı öğrendiği andan itibaren elindeki mevcut bilgilerle makul olan en kısa süre içerisinde ilgili kişiye, bilgi teknolojileri ürün ve hizmet sağlayıcılarına ve 72 saat içerisinde Kurul'a bilgilendirmede bulunacaktır.

Daha sonrasında hangi verilerin ihlal edilip edilmediğinin ayrıntılı bir araştırması yapılarak gerçekleşen veri ihlali hakkında edinmiş olduğu ek bilgileri en kısa süre içerisinde bildirecektir.

İhlal bildiriminde;

Veri ihlalinin türü ve nasıl gerçekleştiğine

İhlalden etkilenen ilgili kişi kategorileri ve sayısına

İhlalden etkilenen kişisel veri kategorileri ve kayıt sayısına

İrtibat kişinin ve veri koruma görevlisinin isim ve iletişim bilgilerine

İhlalin muhtemel sonuçlarının tarifine

İhlal sonrası alınan ya da alınması teklif edilen teknik ve idari önlemlere yer verilecektir. (Örneğin: Şifrelerin değiştirilmesi, Log kayıtlarının koruma altına alınması gibi.)

İhlalden etkilenen ilgili kişilerin belirlenememesi ya da bu kişilere ulaşılmaması durumunda Şirketimiz ilgili kişiyi nasıl bilgilendireceğini Kurul'a soracaktır.

Kişisel verilerinin ihlalinin TCK'da düzenlenen Kişisel Verilerin Kaydedilmesi (m. 135), Kişisel Verileri Verme veya Ele Geçirme Suçu (m.136), Kişisel Verilerin Yok Edilmemesi (m.138) suç tiplerinden birini oluşturması halinde veri ihlaline sebep olan kişi hakkında ilgili makamlara başvurulacaktır.

E. VERİ GÜVENLİĞİNE İLİŞKİN BİLDİRİ

AMAÇ

ES Uluslararası Taşımacılık ve Denizcilik Ticaret A.Ş varlığı ve işleyişi sebebiyle edinmiş olduğu kurumsal her türlü bilgiyi değerli bir varlık olarak kabul eder. Şirket içerden veya dışardan, bilerek veya bilmeyerek meydana gelebilecek her türlü tehdide karşı bilgi varlıklarını korumayı amaçlar.

Şirketimiz bu bilinçle;

Bilgi varlıklarının kontrolünü ve sürekliliğini sağlamaktadır.

Bilgi varlıkları ile yasa ve yönetmeliğin arasında uygunluğu sağlamaktadır.

Bilgi varlıklarının, meydana gelebilecek her türlü tehdide karşı korunmasını amaçlamaktadır.

Bilgi varlıklarını korumak ve bilgi güvenliği yönetimini gerçekleştirebilmek adına gizlilik, bütünlük ve erişilebilirlik ilkelerini benimsenmiştir.

Gizlilik: Önem taşıyan bilgilere yetkisiz erişimlerin önlenmesi,

Bütünlük: Bilginin doğruluk ve bütünlüğünün sağlandığının gösterilmesi,

Erişilebilirlik: Yetkisi olanların gerektiği hallerde bilgiye ulaşılabilirliğinin gösterilmesi, anlamlarına gelmektedir.

KAPSAM

Veri Güvenliği Bildirisi, Şirket bilgilerini veya iş sistemlerini kullanan tüm yurtiçi-yurtdışı şirket personelini ,şirket personeli dışında kalan ve şirket ile arasındaki sözleşmesel ilişki gereğince Şirketin bilgi varlıklarına erişimi olan üçüncü şahıs hizmet sağlayıcılarını ve bunlara bağlı destek personelini kapsamaktadır.

Politikanın uygulama kapsamı, ilgili kişiler için tamamen veya kısmen uygulanabilir.

YÖNTEM

Şirketimiz,

Basılı veya elektronik ortamda tutulan tüm verilerin güvenliği ile ilgilenir.

Bilgi güvenliği yönetimi eğitimlerini tüm personele vererek bilinçlendirmeyi sağlar.

Bilgi güvenliği hususunda gerçekte var olan veya şüphe uyandıran tüm açıklıkları Bilgi Güvenliği Yönetim Sistemi Ekibine rapor eder ve soruşturulmasını sağlar.

Bilgi güvenliğine ilişkin riskleri tanımlar ve sistematik olarak yönetir.

Bilgi teknolojileri alanında meydana gelen değişime uyumluluk sağlar.

Veri güvenliği ile tüm yasal mevzuat ve sözleşmelere uyulması için gerekli teknik ve hukuki danışmanlık hizmetini alır.

Veri güvenliği ihlali durumunda gerekli görülen yaptırımları uygular.

Herhangi bir ihlal halinde

İş süreçlerinin veri güvenliği kapsamında hazırlanan ve onaylanan politika ve prosedürlere uygun bir şekilde yürütülmesini sağlar.

Bunlara ek olarak;

Şirket bilgi güvenliği yönetimini sağlamak ve bilgi varlıklarını korumak amacıyla Politikanın C.6. maddesinde yer alan teknik ve idari tedbirleri uygulamaktadır.

Ayrıca şirket bilgi varlıklarını meşru menfaatini aşan herhangi bir süre saklamamakla birlikte, veri sahiplerinin kişisel veriler üzerindeki haklarının iadesi hususunda tüm çabayı göstermektedir. Bu kapsamda Politikanın C.8. maddesinde bilgi varlıklarının imha edilme yöntemleri belirlenmiştir.

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ EKİBİ

Ekip 1 (bir) yıllık süreyle oluşturulmuştur. Güvenlik Ekibi gerekli gördüğü takdirde bilgi varlıklarının etkin şekilde korunması amacıyla hukuki ve teknik danışmanlık hizmeti alacaktır.

KİŞİ	UNVAN
MEHMET DENİZ	GENEL MÜDÜR
ASLI METE	GENEL MÜDÜR YARDIMCISI
ŞEBNEM DENİZ	SATIŞ MÜDÜRÜ
İLKE GÜLÇİN GÜRER	İŞ PLANLAMA MÜDÜRÜ