Sektör İncelemeleri - 1

Kişisel Verilerin Korunması

Denizcilik

Prof. Dr. Turhan MENTEŞ
Prof. Dr. Mustafa ALKAN
Mehmet Ali İNCEEFE
Av. Gökçe KURANEL

www.accert.com.tr

Bu Sektör İnceleme Raporu ACCERT A.Ş. Tarafından Hazırlanmıştır.

Ankara Nisan.2020

ISBN-978-625-400-112-3

İçindekiler

Önsöz

İnsanlık tarihi esas itibariyle değişimlerin ve dönüşümlerin tarihi olarak değerlendirilmektedir. Günümüzde ise toplumların bilgi toplumlarına döşünüm sürecinde, toplumların en değerli varlıkları bilgi varlıkları olarak kabul edilmekte olup ülkelerin zenginlik kriterleri de sahip oldukları bilgi miktarı ve bilgili insan sayısı ile ölçülmektedir. Çünkü insanoğlu sahip olduğu bilgi sayesinde yeni teknolojiler geliştirmekte, yeni teknolojiler sayesinde de yeni bilgilerin sahibi olmaktadır. Bu pozitif geri besleme üstel olarak çok büyük bir hızla yeni bilgilerin ve yeni teknolojilerin ortaya çıkmasını sağlamaktadır. Bunu başarabilen toplumlar günümüzün bilgi toplumlarını ve zengin ülkelerini oluşturmakta başaramayanlarsa geri kalmış ve fakir toplumlar sınıfında yerlerini almak durumunda kalacaklardır.

Bu durumun tabii bir sonucu olarak bilginin korunması ve güvenliği konusunu gündeme getirmiştir. Başta kişisel verilerin korunması olmak üzere, kurumsal ve ulusal verilerin güvenliği son yılların en önemli ve en öncelikli konular arasında yer almıştır.

Bu kapsamda kişisel verilerin korunması konusu özellikle önemli bir konudur ki, bu konu klasik bilgi güvenliğinden farklı olarak bireyin mahremiyetini daha fazla korumaya yönelik bir güvenlik olgusudur. Kişilerin hak ve özgürlüklerini öne çıkaran ve sahibi olduğu kişisel bilgileri üzerinde bir takım haklara sahip olma imkânı ve yetkisi veren düzenlemeler tüm ülkelerde son yılların öncelikli düzenlemelerinden birisi haline gelmiştir. Bu konuda başta AB olmak üzere ABD ve gelişmiş bütün dünya ülkeleri kendi vatandaşlarının hem ulusal anlamda hem de uluslararası alanda verilerini koruma yönünde bir dizi yasal mevzuatlar ve uygulamaları hayata geçirmiştir.

Bu gelişmelere ve ihtiyaçlara paralel olarak Türkiye'de de benzer düzenlemeler ve kurumsal yapılar oluşturuldu. Bu konuyla ilgili yasalar ve yönetmelikler yürürlüğe konuldu.

Ülkemiz için yeni bir konu olan "*Kişisel Verilerin Korunması*" konusunda yeterli ve yetkin insan kaynağı eksikliği ve bu alandaki bilgi ve bilinç düzeyinin eksikliği göz önünde bulundurulduğunda bu alanla yapılacak başta bilgilendirme, bilinçlendirme ve farkındalık konusundaki çalışmalar ve eğitimlerin büyük önem arz ettiği bir gerçektir.

Bir diğer önemli gerçek ise, bu alanda uluslararası düzenlemelerle karşılaştırıldığında ulusal düzenlemelerdeki eksikliklerdir. Daha önemlisi ise bu düzenlemelerin öngördüğü yükümlülüklerin yerine getirilmesinde ki kurumların teknik olarak yaşadığı ve yaşaması muhtemel yetersizliklerdir. Bunların başında kurumların düzenlemelerin öngördüğü uyumluluk yükümlülüklerini hukuki ve idari açıdan yerine getirebilmeleri konusunda yeterli teknik altyapılara sahip olma zorluğu gelmektedir.

Bu teknik zorlukların en başında kişisel verilerin korunmasına yönelik yapılacak çalışmaları yürütebilmek için sahip olunması gereken yeterli yazılım kaynaklarının olmayışıdır.

Kişisel verilerin korunmasına yönelik kurum ve kuruluşların düzenlemelere uygun iş ve işlemlerini yürütebilmeleri ve tam bir uyumluluk sağlayabilmeleri yukarıda özetlenmeye çalışılan tüm konuları içine alan, hukuki, idari ve teknik yönlerin tümünü içinde barındıran uçtan uca bir çözüm yaklaşımı gerektirmektedir. Bu da kurumların hem yetkin ve uzman insan kaynaklarına sahip olmalarını hem de yeterli teknik kurumsal alt yapıları oluşturmalarını zorunlu hale getirmektedir.

Tüm bu gelişmelerin ışığında ACCERT A.Ş. olarak alanlarında uzman bir kadroyla ülkemizin bu alanda ihtiyaç duyduğu tüm çözümleri ortaya koyacak bir anlayışla bir yılı aşkın bir süredir çalışmalarımızı yürütmekteyiz.

Kişisel verilerin korunmasına yönelik uçtan uça hukuki, idari ve teknik çözümleri ortaya koyan birçok projeyi ve uygulamayı hayata geçirmiş bulunuyoruz. Bu birikimlerimizi ilgili tüm taraflarla paylaşabilmek ve bu alanda yapılacak çalışmalara katkı sunmak amacıyla farklı ve öncelikli sektörlere yönelik hazırlamış olduğumuz bir dizi sektör inceleme raporunu ilgili tüm taraflarla paylaşmayı kamu yararı açısından önemli buluyoruz.

Özellikle uluslararası yoğun ticari ilişki ve işbirliklerinden dolayı hem KVKK hem de GDPR yükümlüsü olan Denizcilik Sektörüne yönelik hazırlamış olduğumuz ilk raporumuzu paylaşmaktan büyük mutluluk duyuyoruz.

Bundan sonraki süreçte farklı sektörler için hazırlamayı planladığımız Kişisel Verilerin Korunması kapsamındaki sektör inceleme raporları serisini kamuoyuyla paylaşacağız.

Raporun hazırlanması sürecinde değerli destekler sağlayan ve emeği geçen tüm kişi ve kuruluşlarımıza teşekkür ediyoruz.

Prof. Dr. Mustafa Alkan / Prof. Dr. Turhan Menteş
Nisan.2020 Ankara

Tanım ve Kısaltmalar

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AIS	Otomatik Tanımlama Sistemi (*Automatic Identification System*)
AİHS	Avrupa insan Hakları Sözleşmesi
AİHM	Avrupa insan Hakları Mahkemesi
Alt Veri İşleyen	Veri işleyen tarafından kendisine verilen yetkiye dayanarak ve yine Veri İşleyen'in talimatları doğrultusunda veri işleme faaliyetleri gerçekleştiren
AT	Avrupa Topluluğu
BIMCO	Baltık ve Uluslararası Denizcilik Konseyi
BT	Bilişim Teknolojileri
Direktif	Veri Koruma Direktifi (*95/46/EC Data Protection Directive*)
DTO	İMEAK Deniz Ticaret Odası
CCTV	Kapalı Devre Kamera Sistemi (*Closed Circuit Camera System*)
Çalışan	DTO bünyesinde istihdam edilen gerçek kişi
EBA	Avrupa Gezinti Tekneleri Birliği
ECASBA	Avrupa Topluluğu Brokerler ve Acenteler Birliği
ECDIS	Elektronik Harita Görüntüleme ve Bilgi Sistemi (*Electronic Chart Display System*)
EHK	5809 sayılı Elektronik Haberleşme Kanunu
ESN	Avrupa Kısa Mesafe Denizyolu Taşımacılığı Ağı
ETDK	6563 sayılı Elektronik Ticaretin Düzenlenmesi Kanunu
FONASBA	Gemi Brokerleri ve Acenteleri Ulusal Birlikleri Federasyonu
GDPR	Avrupa Genel Veri Koruma Tüzüğü (*General Data Protection Regulation)*
GPS	Küresel Konum Sistemi (*Global Positioning System*)
IBIA	Uluslararası Bunker Endüstrisi Birliği
ICC- IMB	Uluslararası Ticaret Odası-Uluslararası Denizcilik Bürosu
ICC Turkey	Uluslararası Ticaret Odası - Türkiye Milli Komitesi
ILO	Uluslararası Çalışma Örgütü (*International Labor Organization*)
İK	4857 Sayılı iş Kanunu
İlgili Kişi	Kişisel verisi işlenen gerçek kişi
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
KVK Kurumu	Kişisel Verileri Koruma Kurumu
OECD	Ekonomik işbirliği ve Kalkınma Teşkilatı (*Organization for Economic Cooperation and Development)*
TBK	6098 sayılı Türk Borçlar Kanunu
TCK	5237 sayılı Türk Ceza Kanunu
TD-IHK	Türk-Alman Ticaret ve Sanayi Odası
TMK	4721 sayılı Türk Medeni Kanunu
TOBB	Türkiye Odalar ve Borsalar Birliği
TYHA	Uluslararası Yat Limanları Birliği
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi

1. Denizcilik ve Kişisel Veriler

Dünya ticaretinin %90'ı deniz ticareti üzerinden yürütülmektedir. Deniz ticaretindeki herhangi bir aksama, dünya ticaretini veya tersi dünya ticaretindeki olası bir aksama denizcilik sektörünü etkilemektedir. Örneğin; ülkemizde 2019 yılsonu itibariyle, turizm sektörü, %16,5'lik oranla kullanılan kredilerin tahsil edilemeyip takibe düşmesinde ilk sırayı alırken, denizcilik sektöründe %14,4, takip oranı ile ikinci sırada yer almıştır.

Sektörün karmaşık ve küresel doğası, denizcilik ticaretini sadece ekonomik ve finansal alanlarda etkilemekle kalmayıp ayrıca ulusal ve uluslararası alanda işlenen ve değiştirilen yüksek düzeyde kişisel veriler açısından da daha kırılgan hale getirmektedir. Özellikle 2016 yılında hem ülkemizde yürürlüğe giren KVKK, hem de AB'de yürürlüğe giren GDPR düzenlemeleri, bu kişisel verilerin toplanması, işlenmesi, paylaşılması ve silinip yok edilmesi konusunda daha katı kurallar, daha ağır cezaları gündeme getirmiştir.

Denizcilik şirketleri, yolcu bilgileri, mürettebat ve çalışan bilgileri, müşteri listeleri ve iş bağlantılarının ayrıntıları dâhil olmak üzere çok sayıda kişisel veri toplamaktadır.[1]

ISM Kodu altındaki toplanan mürettebat verileri, tipik olarak mürettebat listelerini ve mürettebat hakkında yardımcı bilgileri içermektedir;

- ✔ İsimler, doğum tarihi,
- ✔ Mesleki nitelikler, sertifikalar,
- ✔ Geçmiş ve planlanan vardiyalar,
- ✔ Tıbbi geçmiş bilgileri.

Bunların bazıları KVKK/GDPR düzenlemeleri kapsamında özel nitelikli olarak tanımlanan verilerdir. Diğer taraftan, gemi IMO'su, pozisyon, rota, hız gibi Otomatik Tanımlama Sistemi (AIS) verileri, maruz kalan kişinin yeri gibi verileri için mürettebat listeleri ile ilişkilendirilebilir. Genelde özel bir kişiyi tanımlamak için kullanılabilecek bilgiler içermeyen AIS, mürettebat listelerine erişim gerektirdiğinde bazı kişisel verileri içerir.

Denizcilik sektörü, 6698 sayılı Kişisel Verilerin Korunması Hakkındaki Kanunun 6. maddesinde "***özel nitelikli kişisel veriler***" olarak tanımlanan ve "*işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şart*" koşulan **kişilerin sağlığı ile ilgili çok kritik ve en mahrem bilgilerin işlenmesi** ile bu verilerin bir kısmının denizcilik faaliyetlerinin doğası gereği **yurtdışına aktarılmasını** gerektiren iş ve işlemlerden oluşmaktadır.

Günlük çalışma süreçlerine etkili veri koruma denetimleri uygulamak büyük bir zorluktur, ancak KVKK ve GDPR düzenlemeleri yürürlüğe girdiğinden bu yana, kişisel verilerin toplanması, işlenmesi ve paylaşılması, bu düzenlemeler açısından bazı uyumsuzluklara yol açabileceğinden denizcilik şirketleri büyük para cezaları ve itibar gibi ciddi riskler ile karşı karşıya kalmaktadır.

Diğer yandan etkili bir KVKK/GDPR uyumluluk sürecinde ise ticari faydalar da vardır: yolcularının, çalışanlarının ve iş ortaklarının mahremiyetini koruyan ve düzenlemelere uygun şekilde faaliyet yürüten denizcilik şirketlerinin, iş, personel ve müşteri için daha cazip olmaları ve bunları elinde tutması daha olasıdır.

Bu nedenlerle, KVKK'nın ilgili tanımlarına göre denizcilik şirketleri çoğu durumlarda doğrudan **veri sorumlusu**, bazı durumlarda da **veri işleyen** niteliğini haiz olmaktadır.

Bu şirketler için, gerek doğrudan **veri sorumlusu**, gerekse de **veri işleyen** niteliği ile hem kendisinin eylemlerinden **doğrudan** hem de kişisel verileri paylaştıkları 3. tarafların işleyeceği eylemlerden dolayı **müştereken sorumluluklar** doğmaktadır.

[1] https://odatv2.com/istanbul-ekonomisinde-korkutan-gelisme-12032007_m.html

Bu kapsamda, denizcilik şirketlerinin;

- Bazı işlemleri **Kanunun açık hükümleri** uyarınca işlenmekte,
- Bazı işlemleri için **İlgilinin Aydınlatılması**,
- Bazı işlemler için ise **Açık Rıza** gerektirmektedir.

Bu durum, KVKK uyarınca bu şirketler tarafından, yapılan işlemler ile ilgili çok kapsamlı ve detaylı bir "**envanter**" çıkarılmasını ve risk/etki analizlerini gerektirmektedir.

Zira bazı **sorumlulukların yerine getirilememesi veya yükümlülüklerin ihlal edilmesi** TCK 135-140 ile düzenlenmiş suçlar bakımından **hapis cezası gerektirmektedir**. Benzer biçimde KVKK Md. 18'deki kabahatleri işleyen şirketlere **idari para cezaları** uygulanması riski de bulunmaktadır.

Denizcilik şirketleri tarafından **yurtdışına veri aktarımları** KVKK'daki koşullara ve yerine göre KVK Kurulu'nun iznine tabiidir. Bu nedenle yurtdışına veri aktarımı gerektiren tüm işlem süreçleri de KVKK'na uyum bakımından gözden geçirilmelidir.

Bu örneklerden görüleceği üzere, KVKK uyumluluğu denizcilik şirketleri için hayati önemi haizdir. Aksi takdirde, telafisi mümkün olmayan maddi ve manevi sonuçlar doğuracaktır. Bu sonuçlar, İdari Para cezaları ve hapis cezaları başta olmak üzere güven ve itibar kayıplarına sebep olacaktır.

Diğer taraftan KVKK sorumluluk ve yükümlülüklerinin yanı sıra, yaptığı iş ve işlemler ile aktardığı veya aktarılan bir takım kişisel verilerden dolayı denizcilik sektöründe faaliyet gösteren şirketlerin Avrupa Veri Koruma Tüzüğü (GDPR) kapsamına girmesi söz konusudur. Bu nedenle GDPR gereğince ek bazı teknik, idari ve cezai sorumluluk ve yükümlülükleri de bulunabileceği, GDPR yaptırımların sonuçlarının ise daha ağır olduğu göz önünde bulundurulmalıdır.

2. Kişisel Verileri Koruma Kanunu (KVKK)

6698 sayılı Kişisel Verileri Koruma Kanunu 07.Nisan.2016 tarihinde yürürlüğe girmiş ve 07.Nisan.2018 tarihinde 2 yıllık geçiş sürecini de tamamlamıştır. Kanunun **amacı**;

> *"kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek"*

olarak tanımlanmaktadır. Kanunda "***verilerin işlenmesi***" ise şöyle tanımlanmıştır:

> *"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****"*

Verilerin işlenmesi ile ilgili olarak KVKK ve diğer düzenlemeler kapsamında bir dizi kurumsal ve kişisel sorumluluklar ve yeni ünvanlar getirilmiş ve yükümlülükler de ayrıntılı olarak tanımlamıştır.

Veri Sorumlusu

KVKK'da Veri Sorumlusu; *"Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak tanımlanmış, ***herhangi bir kişi ya da kurum bu yükümlülükten muaf tutulmamıştır***.

Veri İşleyen

Diğer yandan KVKK, Veri İşleyeni de; *"Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* olarak tanımlamaktadır.

KVKK'nın ilgili tanımlarına göre denizcilik sektöründe faaliyet yürüten kurum ve kuruluşları bazı durumlarda doğrudan **veri sorumlusu**, bazı durumlarda da **veri işleyen** niteliğini haiz olmaktadır.

2.1. Yükümlülükler

KVKK'nın 10. ve 12. maddeleri **Veri Sorumlu** ile ilgili yükümlülükleri sıralamıştır:

> ***MADDE 10-****1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;*
>
> *a) Veri sorumlusunun ve varsa temsilcisinin kimliği,*
> *b) Kişisel verilerin hangi amaçla işleneceği,*
> *c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,*
> *ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,*
> *d) 11 inci maddede sayılan diğer hakları,*
>
> *Konusunda bilgi vermekle yükümlüdür.*

Kişisel verilerin güvenliğine yönelik yükümlülükler:

> ***MADDE 12-*** *1) Veri sorumlusu;*
>
> *a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,*
> *b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,*
> *c) Kişisel verilerin muhafazasını sağlamak,*
>
> *Amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli* ***her türlü teknik ve idari tedbirleri almak zorundadır****.*

Diğer taraftan denetime yönelik sorumluluklar da *"Veri sorumlusu, kendi kurum veya kuruluşunda, bu* ***Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır****."* olarak açıklanmıştır.

2.2. Yaptırımlar

6698 sayılı kanun, ilgili hükümleri ihlal edilmesi durumunda, ihlalleri niteliğine göre "***suçlar***" ve "***kabahatler***" olarak ayırmış olup, kabahatler için sorumlu kişi veya kurumlara KVKK idari para cezası uygulamayı, söz konusu ihlalin bir kamu kurumu tarafından yapılması durumunda disiplin cezası uygulanması için ilgili kurumun bilgilendirilmesini öngörmektedir.

Kişisel veriler ile ilgili ihlallerin suç niteliğini haiz olması durumunda ise TCK'nın 135-140. maddeleri gereği işlem yapılmasını öngörmektedir.

İdari Para ve Disiplin Cezaları

6698 sayılı kanun kişisel verilere yönelik yükümlülüklerin yerine getirilmemesi durumunda Veri Sorumlusuna **5.000 TL**'ndan **1.000.000 TL**'na kadar **idari para cezası** verilir ve/veya **diğer idari işlemler** uygulanır.

Hapis Cezaları

6698 sayılı kanunun 17. maddesinde kişisel verilere yönelik yükümlülüklerin ihlal edilmesinden kaynaklanacak suçlar için uygulanacak ceza işlemleri aşağıdaki gibi tanımlanmaktadır;

Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140. madde hükümleri uygulanır.

- ✓ *Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası,*
- ✓ *Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası uygulanır.*

Tazminat Hakkı

İdari para ve disiplin cezaları ile hapis cezalarının yanı sıra 6698 sayılı kanunun 14. maddesinin (3). fıkrasına göre "*Kişilik hakları ihlal edilenlerin, genel hükümlere göre **tazminat hakkı** saklıdır.*"

2.3. KVKK Uygulama Örnekleri

6698 sayılı KVKK ile kurulan Kişisel Verileri Koruma Kurumu ve Kurulu bugüne kadar bir dizi ikincil mevzuatı düzenleyip uygulamaya koymuştur. Bu düzenlemeler gereğince bir dizi inceleme ve yaptırımları da uygulamaya başlamıştır.

KVK Kurumu, kuruluşundan bugüne kadar çeşitli uygulamaları ve yaptırımları hayata geçirmiştir. Başlıca ceza gerekçeleri;

- ✓ *Veri Güvenliğine Yönelik Gerekli Teknik ve İdari Tedbirlerin Alınmaması*
- ✓ *Kanuna Aykırı Şekilde Kişisel Verilerin Paylaşılması*
- ✓ *Kişisel Veri Güvenliğinin Sağlanması Amacıyla Uygun Güvenlik*
- ✓ *İlgili Kişinin Verilerinin Silinmesi Talebinin Yerine Getirilmemesi*
- ✓ *Açık Rızanın Hizmet Şartına Bağlanması*
- ✓ *Özel Nitelikli Kişisel Verilerin Kanuna Aykırı Şekilde İnternet ve Sosyal Medya Mecralarında Paylaşılmasıdır.*

KVKK tarafından kesilen başlıca idari para cezaları ve gerekçeleri aşağıdaki gibidir;

Tarih	Veri Sorumlusu / İşleyen	Ceza [TL]	İlgili Maddeler	Açıklamalar
18.09.2019	Facebook	1.150.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
16.05.2019	Marriott International In.	1.000.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
11.04.2019	Facebook	1.000.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
17.08.2019	Dubsmash Inc	680.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
11.04.2019	Facebook	550.000	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
18.09.2019	Facebook	450.000	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
16.05.2019	Cathay Pacific Havayolu	450.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
16.05.2019	Click Bus	450.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.08.2019	Turizm Şirketi	400.000	m. 12/1 a-b-c	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
16.05.2019	Marriott International In.	350.000	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
6.02.2020	Banka	210.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.08.2019	S Şans Oyunları	150.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
14.02.2019	Teknik Servis	150.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
9.12.2019	Gazete	125.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
1.10.2019	Havayolu Taşımacılığı	100.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
10.09.2019	Banka	100.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.08.2019	Turizm Şirketi	100.000	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
16.05.2019	Cathay Pacific Havayolu	100.000	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
16.05.2019	Click Bus	100.000	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
8.07.2019	Yatırım Şirket	75.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
26.11.2019	Banka	70.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
7.11.2019	Doktor	50.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
18.09.2019	Sevinç Eğitim Kurumları	50.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
17.08.2019	Dubsmash Inc	50.000	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
31.05.2019	Avukat	50.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
31.05.2019	Şirket	50.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
5.03.2019	Teknik Servis	50.000	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
26.11.2019	Banka	30.000	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
27.08.2019	S Şans Oyunları	30.000	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
31.05.2019	Varlık Şirketi	20.000	m. 12/1 a	Genel Veri İşleme İlkelerine Uyumsuzluk
1.10.2019	Operatör Şirket	Talimat		
1.07.2019	M.S.G.S. Üniversitesi	Disiplin		
25.03.2019	Spor Salonu	İdari Para Cezası		
14.02.2019	Teknik Servis	Linkleri Durdurma		
2.05.2019	Ziraat Bankası	Talimat		

3. Avrupa Veri Koruma Tüzüğü (GDPR)

Denizcilik sektöründe faaliyet yürüten kurum ve kuruluşların KVKK sorumluluk ve yükümlülüklerinin yanı sıra Avrupa Veri Koruma Tüzüğü (GDPR) gereğince ek bazı teknik, idari ve cezai sorumluluk ve yükümlülükleri de bulunmaktadır.

3.1. Kapsam

AB, Avrupa Veri Koruma Tüzüğü (GDPR) kapsamını AB ülkeleri ile sınırlı bırakmayıp, Avrupa vatandaşları ile ilgili kişisel verilerin işlendiği **Avrupa dışında yerleşik tüm kurum ve kuruluşları** da kapsayacak biçimde genişletmiştir.

3.2. Cezalar

AB, Avrupa Veri Koruma Tüzüğü (GDPR) kapsamında öngörülen idari para cezaları da oldukça ciddi miktarlara ulaşmaktadır;

Bir takım idari yükümlülüklerin yerine getirilmemesi durumunda;

- ✓ ***10.000.000 Euro****'ya kadar* ***veya*** *bir teşebbüs olması halinde, bir önceki mali yılın yıllık* ***dünya çapındaki cirosunun %2'sine kadar*** *idari para cezalarına (hangi meblağ yüksek ise, o geçerlidir)*

Bir veri saçılması durumunda ise;

- ***20.000.000 Euro'ya kadar veya bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezalarına (****hangi meblağ yüksek ise, o geçerlidir****)***

GDPR kapsamında Mayıs.2018 tarihinden itibaren kesilen başlıca idari para cezaları aşağıdaki gibidir;

Ülke	Tarih	Ceza (€)	Veri Sorumlusu / İşleyen	İlgili Maddeler (GDPR)	Açıklamalar
İNGİLTERE	8.07.2019	204.600.000	British Airways	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İNGİLTERE	9.07.2019	110.390.200	Marriott International, Inc	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
FRANSA	21.01.2019	50.000.000	Google Inc.	m.13, m.14, m.6, m.5	Veri İşleme için Yetersiz Yasal Dayanak
İTALYA	15.01.2020	27.800.000	TIM	m.5, m.6, m.17, m.21, m.32	Veri İşleme için Yetersiz Yasal Dayanak
AVUSTURYA	23.10.2019	18.000.000	Austrian Post	m.5(1) a, m.6	Veri İşleme için Yetersiz Yasal Dayanak
ALMANYA	30.10.2019	14.500.000	Deutsche Wohnen SE	m.5, m.25	Genel Veri İşleme İlkelerine Uyumsuzluk
ALMANYA	9.12.2019	9.550.000	1&1 Telecom GmbH	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSVEÇ	11.03.2020	7.000.000	Google LLC	m.5, m.6, m.17	Veri Sahibi Hakları Sağlanama Yükümlülüğünün Tam Sağlanamaması
BULGARİSTAN	28.08.2019	2.600.000	Ulusal Gelir İdaresi	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
HOLLANDA	31.10.2019	900.000	UWV (Çalışan Sigorta Hizmetleri)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
POLONYA	10.09.2019	644.780	Morele.net	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
HOLLANDA	3.03.2020	525.000	Royal Dutch Tennis Association ("KNLTB")	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
BULGARİSTAN	28.08.2019	511.000	DCK Bank	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
FRANSA	21.11.2019	500.000	Futura Internationale	m.5, m.6, m.13, m.14, m.21	Veri Sahibi Hakları Sağlanama Yükümlülüğünün Tam Sağlanamaması
HOLLANDA	18.06.2019	460.000	Haga Hastanesi	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
PORTEKİZ	17.07.2018	400.000	Kamu Hastanesi	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
FRANSA	28.05.2019	400.000	SERGIC (Emlak)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İNGİLTERE	20.12.2019	320.000	Doorstep Dispensaree Ltd. (Pharmacy)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	11.06.2019	250.000	Profesyonel Futbol Ligi (LaLiga)	m.5(1) a, m.7(3)	Veri Sahibi Hakları Sağlanama Yükümlülüğünün Tam Sağlanamaması
POLONYA	26.03.2019	219.538	Özel Veri Şirketi	m.14	Veri Sahibi Hakları Sağlanama Yükümlülüğünün Tam Sağlanamaması
NORVEÇ	29.04.2019	203.000	Oslo Belediyesi Eğitim Birimi	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
DANİMARKA	3.06.2019	200.850	IDdesign A / S	m.5(1) e, m.5(2)	Genel Veri İşleme İlkelerine Uyumsuzluk
YUNANİSTAN	7.10.2019	200.000	Telekom Hizmet Sağlayıcısı	m.5(1) c, m.25	Genel Veri İşleme İlkelerine Uyumsuzluk
YUNANİSTAN	7.10.2019	200.000	Telekom Hizmet Sağlayıcısı	m.21(3), m.25	Genel Veri İşleme İlkelerine Uyumsuzluk
ALMANYA	19.09.2019	195.407	Delivery Hero	m.15, m.17, m.21	Veri Sahibi Hakları Sağlanama Yükümlülüğünün Tam Sağlanamaması
FRANSA	25.07.2019	180.000	ACTIVE ASSURANCES (Otomobil Sigorta)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
NORVEÇ	2019-03	170.000	Bergen Belediyesi	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
DANİMARKA	11.07.1905	160.000	Taxa 4x35	m.5(1) e	Genel Veri İşleme İlkelerine Uyumsuzluk
ROMANYA	9.10.2019	150.000	Raiffeisen Bank SA	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
LATVIA	2019-11	150.000	Bilinmiyor	m.6	Veri İşleme için Yetersiz Yasal Dayanak
YUNANİSTAN	19.12.2019	150.000	Aegean Marine Petroleum Network Inc.	m.5, m.6, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
YUNANİSTAN	30.07.2019	150.000	PWC Business Solutions	m.5(1),5(2), m.6(1), m.13(1)c, m.14(1)c	Veri İşleme için Yetersiz Yasal Dayanak
ROMANYA	27.06.2019	130.000	UNICREDIT BANK SA	m.25(1), m.5(1)c	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	27.02.2020	120.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
ALMANYA	3.12.2019	105.000	Hastane	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
MACARİSTAN	23.05.2019	92.146	SZIGET ve VOLT festivalleri Organizatörü	m.6, m.5(1)b, m.13	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	14.02.2020	80.000	Iberdrola Clientes	m.6	Veri İşleme için Yetersiz Yasal Dayanak
ALMANYA	11.07.1905	80.000	Bilinmiyor	m.32	Yetersiz İdari ve Teknik Veri Güvenliği Tedbirleri
ALMANYA	11.07.1905	80.000	Bilinmiyor	m.32	Yetersiz İdari ve Teknik Veri Güvenliği Tedbirleri
İSPANYA	3.02.2020	75.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	75.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	7.01.2020	75.000	EDP España S.A.U.	m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	7.01.2020	75.000	EDP Comercializadora, S.A.U.	m.6	Veri İşleme için Yetersiz Yasal Dayanak
LİTVANYA	16.05.2019	61.500	Payment service provider UAB MisterTango	m.5, m.32, m.33	Veri İhlali Bildirim Yükümlülüğünün Tam Olarak Yerine Getirilmemesi
İSPANYA	4.03.2020	60.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	60.000	Xfera Moviles S.A.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	60.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	21.11.2019	60.000	Viaqua Xestión Integral Augas de Galicia	m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	19.11.2019	60.000	Corporación radiotelevisión espanola	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	19.11.2019	60.000	Xfera Moviles S.A.	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	16.10.2019	60.000	Xfera Moviles S.A.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	16.08.2019	60.000	AVON COSMETICS	m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	-	60.000	Debt collecting agency (GESTIÓN DE COBROS, Y O COBRO	m.5(1) f	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	11.07.1905	60.000	ENDESA (Enerji Dağıtımı)	m.5(1) f	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	50.000	Vodafone España, S.A.U.	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
SLOVAKYA	-	50.000	Sosyal Güvenlik Kurumu	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İTALYA	17.04.2019	50.000	Italian political party Movimento 5 Stelle	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
ALMANYA	03.2019	50.000	N26	m.6	Veri İşleme için Yetersiz Yasal Dayanak
AVUSTURYA	03.2020	50.000	Sağlık Sektöründe Bir Şirket	m.13, m.37	Aydınlatma Yükümlülüğünün Tam Olarak Yerine Getirilmemesi
İSPANYA	28.02.2020	48.000	Vodafone ONO, S.A.U.	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	25.02.2020	48.000	HM Hastaneleri	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
POLONYA	16.10.2019	47.000	ClickQuickNow	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
İSPANYA	7.01.2020	44.000	Vodafone España, S.A.U.	m.5(1) f	Genel Veri İşleme İlkelerine Uyumsuzluk
İSPANYA	3.03.2020	42.000	Vodafone España, S.A.U.	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	14.02.2020	42.000	Vodafone España, S.A.U.	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	3.03.2020	40.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
SLOVAKYA	-	40.000	Slovak Telekom	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	25.10.2019	36.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSVEÇ	18.12.2019	35.000	Nusvar AB	m.6	Veri İşleme için Yetersiz Yasal Dayanak
MACARİSTAN	5.04.2019	34.375	Hugarian political party	m.33(1), m.33(5), m.34(1)	Veri İhlali Bildirim Yükümlülüğünün Tam Olarak Yerine Getirilmemesi
İSPANYA	14.02.2020	30.000	Xfera Moviles S.A.	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	14.11.2019	30.000	Telefónica SA	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
İSPANYA	1.10.2019	30.000	Vueling Airlines	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İTALYA	23.01.2020	30.000	Azienda Ospedaliero Universitaria Integrata di Verona	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İTALYA	23.01.2020	30.000	Sapienza Università di Roma	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
BULGARİSTAN	26.02.2019	27.100	Telekom Hizmet Sağlayıcısı	m.6, m.5(1) a	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	-	27.000	Vodafone España, S.A.U.	m.5(1) d	Veri Sahibi Hakları Sağlanama Yükümlülüğünün Tam Sağlanamaması
İSPANYA	3.03.2020	24.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İZLANDA	10.03.2020	20.600	National Center of Addiction Medicine ("SAA")	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	3.02.2020	20.000	Iberia Lineas Aereas de Espana, S.A. Operadora	m.5, m.6, m.21	Veri İşleme için Yetersiz Yasal Dayanak

4. Denizcilik ve Kişisel Verileri Koruma

Dünya ticaretinin %90'ı deniz ticareti üzerinden yürütülmektedir. Deniz ticaretindeki herhangi bir aksama, dünya ticaretini veya tersi dünya ticaretindeki olası bir aksama denizcilik sektörünü etkilemektedir.

Deniz ticaretinde kullanılan gemilerde ise giderek artan bir oranda dijital sistemler kullanılmaya başlanmıştır. Bir gemiye ait sistemde; **kargo yönetim sistemi**, **köprü sistemleri**, **makine sevk ve idare sistemleri**, **güç kontrol sistemi**, **erişim kontrol sistemleri**, **yolcu hizmet ve yönetim sistemi**, **toplu ağlar**, **idare ve mürettebat yardım sistemleri** ve **iletişim sistemlerinin** tümü veya bir kısmı bulunmaktadır.

Bu durum, gemilerin sistemlerine ve ağlarına yönelik siber saldırı riskini de beraberinde getirmektedir. Bu doğrultuda, gemilerin güvenlik yönetim sistemleri, işletim teknoloji sistemleri (*OT*[2]) ile bilgi teknoloji sistemlerinde (*IT*[3]) yer alan güvenlik açıkları siber saldırılara olanak sağlamakta, hatta IT sistemine kıyasla OT sistemine yönelik saldırılar veri kaybından çok geminin varlığı ve mürettebatın can güvenliğini tehlikeye atabilecek boyutlara ulaşabilmektedir.[4]

Ayrıca gemi sistemlerinin kendi güvenlikleri sağlansa bile diğer sistemlerle olan bağlantılarının siber güvenlik konusunda bir güvenlik oluşturabileceği değerlendirilmektedir. Nitekim bağlantılı sistemlere yönelik gerçekleştirilen siber saldırılar söz konusu sistemler üzerinden gemi sistemlerine yayılma riskini de artırmaktadır.

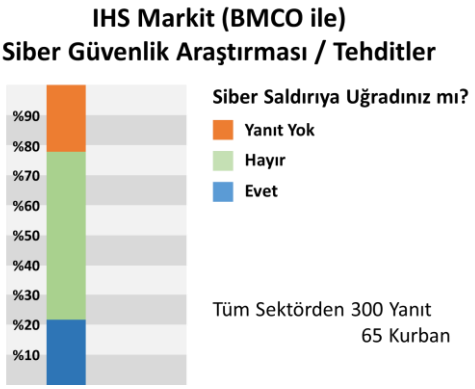
Bu kapsamda özellikle, GPS ile büyük çaplı yolcu gemileri ve ticari gemilerde zorunlu olarak bulunan AIS ve ECDIS gibi navigasyon sistemleri de siber saldırılara açıktır.[5] Söz konusu siber saldırılar sonucunda kargoya ilişkin gizli bilgilere erişilip, bazı durumlarda tüm makine sisteminin kontrolü ele geçirilmektedir. Doğal olarak bu saldırılar önemli ölçüde işgücü ve maddi kayıpların yanı sıra, kişilerin yaşamı da tehdit eden boyutlara ulaşmaktadır.[6]

Nitekim *"The Review of Maritime Transport 2017"* deniz taşıtlarında ve limanlarda kullanılan navigasyon ve diğer sistemlere yönelik siber saldırılar bulunduğunu ve saldırıların özellikle otomatik tanıma, elektronik harita gösterimi ve bilgi sistemlerini hedef aldığını ve kargo sistemlerini manipüle ettiğini duyurmuştur.

Söz konusu saldırılar doğrudan deniz ticaretini hedef almamış olsa dahi bu tür saldırıların deniz ticareti üzerinde ciddi etkisi olabilmektedir. Bu kapsamda, söz konusu sistemlere yönelik gerçekleştirilen siber saldırılar ile deniz korsanları saldırıları arasında bağlantı ihtimali olabildiği ve korsanların bu sistemler aracılığı ile değerli yük taşıyan veya minimum güvenlik önlemi bulunan gemileri belirlemesinin kolaylaştığı ifade edilmektedir.[7]

Siber saldırı riskinin her bir şirket özelinde ayrı ayrı değerlendirilmesi gerektiği ifade edilmektedir. Bu kapsamda, herhangi bir risk oluşması halinde bilinçli bir şekilde bu duruma müdahale edilmesi ve olası risklere

[2] Operational Technology.
[3] Information Technology.
[4] https://www.bimco.org/news/priority-news/20181207-industry-publishes-improved-cyber-guidelines
[5] https://www.marinelink.com/news/combatting-maritime393435.aspx
[6] https://www.portvision.com/news-events/press-releases-news/shipping-industrys-cyber-security-guidelines-to-protect-ais-navigation
[7] https://unctad.org/en/PublicationsLibrary/rmt2018_en.pdf



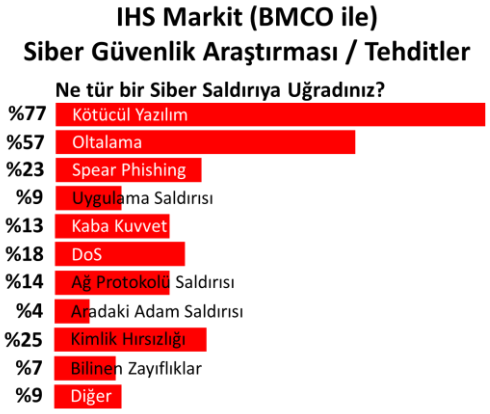
karşı önlemler alınması büyük önem teşkil etmektedir. Genel olarak, söz konusu durumlara yönelik siber güvenlik yaklaşımının aşağıdaki şekilde şekillenmesi tavsiye edilmektedir:[8]

BIMCO tarafından yapılan ankette, ankete katılan sektördeki 300 şirketten 65'i siber saldırı kurbanı olduğunu belirtmiştir[9]:

Söz konusu siber saldırı kurbanı şirketlerin büyük bir çoğunluğu kötücül yazılımlar (*malware*) aracılığıyla siber saldırıya uğradıklarını ifade etmişlerdir.

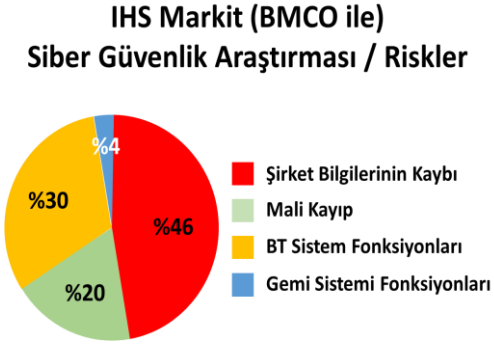
Anket sonuçlarına göre sektöre yönelik olarak gerçekleştirilen siber saldırı türleri aşağıdaki listelenmiştir:[10]

Genel olarak siber saldırganlar dört grupta toplanmaktadır. Bunlar; aktivistler (*örneğin hoşnutsuz çalışanlar*), suçlular (*finansal kar veya casusluk amacı ile)*, fırsatçı gruplar ile devletler, devlet destekli organizasyonlar ve terörist gruplar olarak sınıflandırılmaktadır.[11]



Söz konusu siber saldırılar sonucunda oluşabilecek riskler genel olarak; şirket verilerinin kaybı, finansal kayıplar, IT sistemleri ve gemi sistemi işlevselliğine yönelik kayıplar olarak sınıflandırılmıştır. Söz konusu risklere ilişkin risk oranları ise aşağıdaki grafikte verilmiştir:[12]

Siber saldırıların maliyetine ilişkin olarak, siber saldırıya uğramış şirketlerin yarısı siber saldırıların maliyetinin 5.000 $'dan daha az olduğunu ifade ederken, %15'i ise siber saldırılar nedeniyle 5.000-50.000 $ arasında bir maliyete katlandığını ifade etmiştir. Siber saldırıya uğramış şirketlerin yalnızca iki tanesi siber saldırıların maliyetinin 500.000 $'ın üzerinde olduğunu belirtmiştir.[13]



Diğer taraftan, Denizcilik şirketleri ticari faaliyetleri gereği yolcu bilgileri, mürettebat ve çalışan bilgileri, müşteri listeleri ve iş bağlantılarının ayrıntıları dâhil olmak üzere çok sayıda kişisel veri toplamaktadır.

Aşağıdakiler denizcilik sektöründe kullanılan kişisel verilerin yaygın örnekleridir:

- ✓ Adı-Soyadı / Doğum Tarihi ve Yeri
- ✓ Adresi
- ✓ IP Adresi
- ✓ Biyometrik Veriler

[8] https://www.liscr.com/sites/default/files/Guidelines_on_cyber_security_onboard_ships_version_2-0_Jul17.pdf
[9] http://www.ics-shipping.org/docs/default-source/Tripartite-2016-Presentations/7b-bimco-cyber-at-tripartite-2016-read-only-.pdf
[10] http://www.ics-shipping.org/docs/default-source/Tripartite-2016-Presentations/7b-bimco-cyber-at-tripartite-2016-read-only-.pdf
[11] IMO (Denizcilik) Siber Risk Yönetimi Rehberine paralel olarak Baltic and International Maritime Council (*BIMCO*), Cruise Lines International Association (*CLIA*), International Chamber of Shipping (*ICS*), International Association of Dry Cargo Shipowners (*INTERCARGO*), International Association of Independent Tankers (*INTERTANKO*), Oil Companies International Marine Forum (*OCIMF*) ve International Union of Marine Insurance (*IUMI*) kuruluşları tarafından hazırlanan ve desteklenen Gemilere Yönelik Siber Güvenlik Rehberi'ne bu linkten ulaşabilirsiniz:
https://www.liscr.com/sites/default/files/Guidelines_on_cyber_security_onboard_ships_version_2-0_Jul17.pdf
ICS tarafından hazırlanan ve gemilere yönelik siber güvenlik uyarılarını içeren kısa broşüre ise bu linkten ulaşabilirsiniz: http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/cyber-security-onboard-ships-awareness-poster.pdf
[12] http://www.ics-shipping.org/docs/default-source/Tripartite-2016-Presentations/7b-bimco-cyber-at-tripartite-2016-read-only-.pdf
[13] https://safetyatsea.net/news/2016/ihs-fairplay-maritime-cyber-security-survey-the-results/

- Sağlık verileri / İş Öncesi Tıbbi Muayene Bilgileri
- Banka Hesap Numarası / Kredi Kartı Numarası
- Sigorta Numarası
- Pasaport Numarası
- Denizcinin Taburcu Kitap (*Discharge book*) Numarası
- Akrabaların Kişisel Detayları
- Tahsis Detayları
- Sendika Üyeliği / Etnik Grup / milliyet, dini inançlar
- Sabıka kayıtları.

Bu kişisel veriler çeşitli kaynaklardan alınabilir. Bu kaynaklar şunları içerebilir:

- Çalışan Adayları / Çalışanlar
- Müşteriler / Yükleniciler / Taşeronlar
- Port Acenteleri / Sigortacılar / Diğer Şirketler
- Doktorlar ve diğer Sağlık Personeli
- Gemi Yöneticileri / Personel / Mürettebat Ajansları
- Kamu Kurum ve Kuruluşları
- Üçüncü Ülkelerdeki Kurum ve Kuruluşlar.

KVKK/GDPR düzenlemeleri kapsamında, bir işletme olarak doğrudan bir kişiden veri alıyorsa, **veri sorumlusu** olarak kabul edilmektedir. İstihdam için yetkili insan kaynakları acentesi ile çalışılıyorsa, bu insan kaynakları şirketleri **veri işleyen** olacaktır. Veri sorumluları, kişisel verilerin toplanma ve işlemenin amaçlarını ve araçlarını belirler. Veri işleyenler ile yaptıkları sözleşmelerin KVKK/GDPR düzenlemelerine uygun olması gerekmektedir.

Uygun bir güvenlik seviyesi sağlamak ve veri işlemenin KVKK/GDPR düzenlemelerine uygunluğunu sağlamak ve gerektiğinde göstermek için bir dizi hukuki, idari ve teknik önlemler uygulanmalıdır. Veri işleme, düzenlemelerde kişisel veriler üzerinde gerçekleştirilen ve aşağıdakileri içeren herhangi bir işlem olarak tanımlanır:

- Toplama / Kaydetme / Depolama
- Düzenleme / Uyarlama Veya Değiştirme
- İletme, Yayma veya Başka Bir Şekilde Kullanılabilir Hale Getirme
- Anonimleştirme veya Bulanıklaştırma (*Pseudonymization*)
- Silme Veya Yok Etme.

Sektörün karmaşık ve küresel doğası, denizcilik ticaretini sadece ekonomik ve finansal alanlarda etkilemekle kalmayıp ayrıca ulusal ve uluslararası alanda işlenen ve değiştirilen yüksek düzeyde kişisel veriler açısından da daha kırılgan hale getirmektedir.

Denizcilik ve deniz ticareti, 6698 sayılı Kişisel Verilerin Korunması Hakkındaki Kanun ile Avrupa Veri Koruma Tüzüğü (*GDPR*) kapsamında korunması ve özelikle de yurtdışına aktarılması için özel tedbirlerin alınması istenen kişisel veriler ve "***özel nitelikli kişisel veriler***" olarak tanımlanan ve "*işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şart*" koşulan ***kişilerin sağlığı ile ilgili çok kritik ve en mahrem bilgileri de*** içeren iş ve işlemleri de içermektedir.

Dolayısıyla ulusal ve uluslararası denizcilik mevzuatında yer alan sorumlulukların yanı sıra, 7.Nisan.2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verileri Koruma Kanunu ile yine 2016 yılının Mayıs ayında yürürlüğe konulan GDPR düzenlemeleri ile ek olarak bir dizi yeni yükümlülükler getirilmiştir.

GDPR, verilerin nerede tutulduğuna bakılmaksızın, Avrupa Birliği'nde yerleşik bir tüzel kişiliği bulunan bir işletme tarafından tutulan kişisel verilerin işlenmesi için geçerlidir. Aynı zamanda AB'deki veri sahiplerine mal ve hizmet sağlayan ya da davranışlarını izleyen AB üyesi olmayan işletmeler için de geçerlidir.

KVKK/GDPR düzenlemelerinin Denizcilik şirketlerinin bu düzenlemelerden etkilenecek olup yeni düzenlemelere en etkili ve verimli biçimde uyumluluk sağlaması gerekmektedir.

Günlük çalışma süreçlerine etkili veri koruma denetimleri uygulamak bazı sıkıntı ve zorluklar getirmektedir, ancak KVKK ve GDPR düzenlemeleri yürürlüğe girdiğinden bu yana, kişisel verilerin toplanması, işlenmesi ve paylaşılması, bu düzenlemeler açısından bazı uyumsuzluklara yol açabileceğinden denizcilik şirketlerini büyük para cezaları ve itibar gibi ciddi riskler beklemektedir.

Etkili bir uyumluluk sürecinde ise ticari faydalar da vardır: yolcularının, çalışanlarının ve iş ortaklarının mahremiyetini koruyan ve uygun şekilde hedeflenmiş pazarlama kampanyaları yürüten denizcilik şirketlerinin, iş, personel ve müşteri için daha cazip olmaları ve bunları elinde tutması daha olasıdır.

4.1. KVKK/GDPR ve Denizcilik Şirketlerinin Yükümlükleri

KVKK'na göre, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan her gerçek veya tüzel kişi "***veri sorumlusu***"dur. Denizcilik faaliyetleriyle ilgili yapılan işlemlerde işlenen kişisel veriler bakımından da **denizcilik şirketleri** veri sorumlusudur.

Denizcilik şirketleri genel olarak işlediği kişisel veriler (*örneğin, personel kayıtları*) ile ilgili olarak **veri sorumlusu** iken, 3. Taraflardan alarak kendi bilişim sisteminde kaydedip saklamakla yükümlü olduğu kişisel veriler için de bir **veri işleyen** konumundadır.

Veri sorumlusu sıfatıyla denizcilik şirketleri Kişisel Verilerin Korunması Kanunu'nda sayılan "*ilkeler*"e ve "*veri işleme şartları*"na eksiksiz uymakla mükelleftirler. Örneğin, kanunlarda "*açıkça*" öngörülen hallerde kişisel verinin ilişkili olduğu kişinin *(ilgili kişi")* "açık rızası" almadan veri işleyebilecektir. Bunun gibi Kanun'da sayılan istisnai işleme şartlarından herhangi birinin bulunmaması halinde ise veri işleyebilmek için ilgili kişinin açık rızasını alması bir zorunluluktur.

Veri sorumlusunun yükümlülükleri, koşulları oluştuğunda kişisel verilerin "*silinmesi*", "*yok edilmesi*" veya "*anonim hale getirilmesi*"ni de içermektedir. Keza, Kanun kişisel verilerin yurt içinde veya yurt dışına aktarılması bakımından ek yükümlülükler getirmekte, hatta belirli durumlarda Kişisel Verilerin Korunması Kurulu'nun iznini şart koşmaktadır.

Denizcilik şirketlerinin kişisel verileri işlenen gerçek kişilere *("ilgili kişi")* yönelik doğrudan yükümlülükleri de bulunmaktadır. İlgili kişilerin kendileriyle ilgili olarak işlenen veriler bakımından tam ve doğru şekilde denizcilik şirketleri tarafından işleme öncesinde (*en geç veri işlemesi esnasında*) aydınlatılması gerekir. Bu ödevin hiç veya gereği gibi yerine getirilmemesi bu şirketlerin ceza sorumluluklarını doğurmaktadır. Aynı şekilde ilgili kişilerin Kişisel Verilerin Korunması Kanunu ile özel olarak koruma altına alınmış olan haklarına bu şirketler tarafından riayet edilmemesi sorumluluklarına yol açacaktır.

Veri güvenliğinin Kanun'da öngörülen çerçevede tesis edilmesi gerek denizcilik şirketleri gerekse kişisel verileri paylaştıkları taraflar için başlı başına bir yükümlülüktür. Bu yükümlük sadece hukuki ve idari tedbirlerin alınmasını gerektirmemekte, aynı zamanda çeşitli teknik tedbirlerin de hayata geçirilmesini zorunlu kılmaktadır.

Denizcilik şirketlerince verilen hizmetlerin sadece ülkemiz ile sınırlı olmadığı göz önüne alındığında veri güvenliğine ilişkin alınması gereken tedbirlerin de sadece bu denizcilik şirketlerince ve yine sadece ülke sınırlarında alınması gereken tedbirlerden ibaret olmadığı açıktır.

4.2. KVKK/GDPR ve Denizcilik Şirketlerinin Riskleri

KVKK/GDPR düzenlemeleri kişisel verileri işleyen her kuruluşu etkileyecektir. Ancak, aşağıdaki kişisel verilerin toplanıp, işlenmesi ve diğer taraflara aktarılmasından dolayı denizcilik sektörü, özellikle etkilenecektir:

- ✔ Küçük denizcilik şirketleri bile mürettebatının kişisel verilerini günlük olarak işlerler. Çoğu deniz taşımacılığı şirketi, mürettebat üyelerinin kayıtlarını aydıktan sonra bile bir süre daha tutmaktadırlar.
- ✔ Denizcilik şirketleri tarafından işlenen kişisel veriler; kişisel kimlik belgelerini, banka bilgilerini, pasaport ve seyahat belgelerini, eğitim kayıtlarını ve ayrıca tıbbi kayıtlar gibi "**hassas**" kabul edilen verileri içerir.
- ✔ Denizcilik şirketleri, normal iş sürecinde bireylerin kendileri, personel acenteleri, liman acenteleri ve diğer üçüncü taraflar gibi birçok değişik kaynaktan kişisel veriler almaktadırlar.
- ✔ Liman acenteleri, seyahat acenteleri gibi birçok 3. Taraflara ile kamu kurum ve kurumlarına kişisel veriler gönderirler.
- ✔ Düzenli olarak diğer ülkelere ve uluslararası kuruluşlara, özellikle de veri aktarılmasının belirli izinlere tabii olan taraflara veri aktarımı yaparlar.

Sektörün karmaşık ve küresel doğası ve genellikle ulusal sınırlar boyunca işlenen ve değiştirilen yüksek düzeyde kişisel veriler, kasıtlı veya başka şekilde güvenlik ihlallerine karşı savunmasız kalabilir.

Fotoğraf ve parmak izi biyometrik verilerdir ve dolayısıyla "***özel nitelikli kişisel veri***"dir.

Bu kişisel verilerin işlenmesi, gerek KVKK gerekse TCK kapsamında bir takım hukuki, idari ve cezai müeyyideler ile güvence altına alınır. KVKK uyumun gereği yükümlülükleri yerine getirmeyenler de gerek ceza hukuku (TCK) gerek idare hukuku (KVKK) gerekse özel hukukun (*MK, BK ve diğer kanunlarda*) öngörülen yaptırımlara maruz kalacaklardır.

KVKK'nın 17. maddesinde işaret edildiği üzere, TCK 135 ile 140 arasında düzenlenmiş olan suç ve cezalar öncelikle kişisel verilen korunmasını ihlal eden fiilleri kapsar. Kişisel verilerin korunması ile ilgili suç teşkil eden fiilleri işleyenleri her bir fiil için 1 yıldan 6 yıla kadar hapis cezaları beklemektedir. Örneğin, kişisel verileri hukuka aykırı olarak bir başkasına veren bir denizcilik şirketi yönetici ve çalışanları, TCK 136'daki **suçun nitelikli halini işlemiş olacağından** 3 ile 6 yıl arasında bir hapis cezasına çarptırılacaktır.

KVKK'nın 18. maddesinde çeşitli kabahatler tanımlanmıştır. Bu kabahatleri işleyen veri sorumlularına 5 bin TL ile 1 milyon TL arasında idari para cezaları uygulanır. Her bir ihlal bakımından ayrı ayrı söz konusu olacak olan bu cezalar kişisel verilerin korunmasına ilişkin yükümlüklerini yerine tam olarak getirmeyen denizcilik şirketleri bakımından önemli bir risktir. Örneğin, veri güvenliğine ilişkin yükümlülüklerinin yerine getirilmemesi nedeniyle 1 milyon TL 'sına kadar idari para cezası verilmesi mümkündür.

Son olarak kişisel verilerin korunmasına ilişkin yükümlüklerin ihlali beraberinde özel hukuk hükümlerine göre denizcilik şirketlerinin sorumluluğunu doğuracaktır. KVKK 14. maddesinde bu hususa "*Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır*" demek suretiyle işaret etmektedir. Kişisel verilerin korunması bilinci yaygınlaştıkça, her geçen gün sayısı artarak devam edecek olan tazminat taleplerine muhatap olacaklardır.

Ayrıca, KVKK'nın kapsamına sadece otomatik olarak işlenen kişisel veriler değil, bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen veriler de girmektedir. Bu nedenle basılı veya dijital ortamda işlenip işlenmediğine bakılmaksızın denizcilik şirketlerinde işlenen ve kişisel veri niteliği taşıyan her türlü veriler bakımından KVKK tarafından belirlenmiş yükümlükler ve bu uygulamalara bağlı riskler mevcuttur.

Avrupa yerleşik kişilere yönelik işlemlerden dolayı da ayrıca GDPR kapsamında bazı idari ve hukuki yükümlülükler ile idari para cezası risklerini taşımaktadır.

4.3. Uyumluluğa Yönelik Adımlar

Günlük çalışma süreçlerine etkili veri koruma denetimleri uygulamak büyük bir zorluktur, ancak KVKK ve GDPR düzenlemeleri yürürlüğe girdiğinden bu yana, kişisel verilerin toplanması, işlenmesi ve paylaşılması, bu düzenlemeler açısından bazı uyumsuzluklara yol açabileceğinden denizcilik şirketlerini büyük para cezaları ve itibar gibi ciddi riskler beklemektedir. Etkili bir uyumluluk sürecinde ise ticari faydalar da vardır: yolcularının, çalışanlarının ve iş ortaklarının mahremiyetini koruyan ve uygun şekilde hedeflenmiş pazarlama kampanyaları yürüten denizcilik şirketlerinin, iş, personel ve müşteri için daha cazip olmaları ve bunları elinde tutması daha olasıdır.[14] [15]

Denizcilik şirketleri KVKK/GDPR düzenlemelerine uyumluluk için yapması gereken iş ve işlemler temel aşağıdaki gibidir:

Farkındalık

Denizcilik şirketlerinin KVKK/GDPR uyumluluk projelerini ve bu düzenlemeler göre nelere ihtiyacı olduğu ve kendi kuruluşları için önemli risklerin ne olduğu konusunda özellikle üst yönetim arasında farkındalığı artırarak başlatmaları çok önemlidir.

Kurumun gerekli zamanı ve kaynakları taahhüt etmesini ve mahremiyete saygı duyan bir kültür geliştirmesini sağlamak için doğru insanları en üst yönetim seviyesine dâhil etmek gerekir.

Eğitim

KVKK/GDPR uyumluk projesinin başlangıcında farkındalığa yönelik ve daha uyumluluk politika ve planlarının uygulanmasına yönelik tüm personele ve mürettebata gerekli eğitimler verilmelidir.

Gemilerde seyahat belgeleri ve diğer kişisel veriler tutulmaktadır. Bu nedenle gemideki görevlilere belirli aralıklarla ve uygun ölçüde eğitimlerin verilmesi de önemlidir.

Veri Koruma Takımının Oluşturulması

KVKK/GDPR uyumluluk projesini yürütmek için yönetimin tam desteğiyle, risk, yasal ve bilişim teknolojileri çalışanlarından oluşacak bir ekip kurmaları gerekir.

Güvenilir harici danışman desteği; teknik uzmanlık, maliyet ve zaman kazanmanıza yardımcı olacaktır.

Hesap Verebilirlik ve Yönetişim Çerçevesi

KVKK/GDPR uyumluluğu, üstyönetim düzeyinde destek gerektirir. Bu nedenle üstyönetimin KVKK/GDPR düzenlemelerinin gereklerini, yükümlülüklerini, risklerini ve sonuçlarını iyi anlaması gerekmektedir. KVKK/GDPR uyumluluğunun sağlanması ve daha da önemlisi sürdürülebilmesi için gerekli kaynakların uygunluğu sağlamak ve sürdürmek için gereken kaynakların tahsis edilmesi üstyönetimin bu konudaki bilgisi ile yakından ilgilidir.

Veri İşleme Envanterinin Hazırlanması

Veri işleme faaliyetlerini belirlemesi ve veri işleme envanterinin hazırlanması ciddi bir iş yükü getirir ancak yasal bir zorunluluk niteliğindedir.

Veri işleme envanterinin hazırlanması, her faaliyet için veri toplamadan yok etmeye kadar tüm veri yaşam döngüsünün anlaşılmasını ve hazırlanmasını sağlar.

[14] GDPR in shipping: Roadmap to compliance in 10 essential steps. Moore Stephens 03/2018
[15] https://www.itgovernance.asia/gdpr-compliance-checklist

Fark Analizi ve Uyumluluk Planı

Kişisel verilerin işlenmesi sürecinde kuruluşlar veri akışlarındaki bir dizi zayıflık ve kırılganlıkların oluşması olasıdır. KVKK/GDPR uyumluluk çalışmaları kapsamında bu zayıflıklar ve kırılganlıklar dikkatlice aranmalı ve bunların yol açacağı olası riskler değerlendirmelidir. Daha sonra bu riskleri kabul edilebilir bir seviyeye indirgeyecek veya ortadan kaldıracak pratik eylem planları oluşturulmalıdır.

Zayıflıkları uzun soluklu izlenmesi ve yeni kırılganlıkların oluşmasını engellemek için uygulama planları ve prosedürler belirlenmelidir.

Veri Koruma ve Gizlilik Politikalarının Hazırlanması

Belirli eylem planı tamamlandığında, uyumluluk için uygulama aşamasına geçebilir. Bu normalde gizlilik politikalarında değişiklik yapılmasını, personel acenteleriyle yapılan sözleşmeleri, liman acentelerine, personele ve mürettebata bilgi bildirimlerinin yanı sıra uygun rıza formlarının hazırlanmasını içerir.

Uygulama, manuel prosedürler, BT güvenliği (*güvenlik duvarları, şifreleme vb.*) ve iş sürekliliği ile olağanüstü durum kurtarma planındaki değişiklikleri de içermelidir.

Dış danışmanlar uygulamanın çeşitli yönlerini yerine getirmeye yardımcı olabilir, fakat aynı zamanda çabayı yönetmeye de yardımcı olabilirler.

Veri İhlal Süreçlerinin Hazırlanması

Denizcilik şirketleri, ihlal durumunda Kişisel Verileri Koruma Kurumuna ve veri sahiplerine (*veri ihlalinin tespitinden itibaren 72 saat içinde*) söz konusu ihlali ve olası etkileri ile ilgili bildirimde bulunmak zorundadırlar.

Bildirimin zamanında gönderilebilmesi için yapılması gereken ayrıntılı eylemleri içerecek bir Olay Raporu Planı tasarlaması çok önemlidir. Plan, önceden belirlenmiş net bir dizi ardışık eylem ve bu eylemler için açık bir sorumluluk tahsisi ve bildirim şablonları, araştırma gereksinimleri, raporlama, medya ve iletişim yönetimi vb. İçermelidir. Denizcilik şirketleri ayrıca ayrıntıları içeren bir olay günlüğü tutacak teknik altyapıyı da hazırlamalıdırlar.

Risk Değerlendirmesi

Gizlilik ve veri güvenliği alanında çok sayıda "risk" tanımı ve kavramı olmasına rağmen, KVKK/GDPR kapsamında sadece verileri işlenen kişiler için gündeme gelecek olan riske odaklanılmaktadır.

KVKK/GDPR düzenlemeleri, veri sorumlularının belirli proje ve faaliyetlerde bulunan riske uygun bir güvenlik düzeyi sağlamasını gerektirir. Denizcilik şirketleri, kişisel verilere yönelik riski azaltmak için uygun seviyede teknik ve idari önlemleri uygulamadan önce riski belirlemek için gerekli çalışmaları yapmalıdırlar.

Veri sorumluları karşılaşacakları tek riskin sistemlerine girmeye çalışan siber suçlular olduğunu düşünmemelidirler, kişisel verilerin kazara veya kasıtlı imha, kayıp veya ifşaya karşı savunmasız olduğunu da göz önünde bulundurmalıdır.

Kişisel Verilerin Güvenliğine Yönelik Teknik Önlemlerin Alınması

KVKK/GDPR düzenlemelerinin öngördüğü teknik ve idari önlemlerin alınması, idari ve hukuki önlemlerin tamamlayıcı ve zorunlu tamamlayıcısı durumundadır.

Bunun için var olan bir bilgi güvenliği politikalarına ek olarak kişisel verilerin korunmasına yönelik politika ve süreçlerin tanımlanması gerekmektedir.

Ayrıca, kişisel verilere erişim içim yetki matrisinin de hazırlanması, veri keşif ve kişisel verilerin sınıflandırılması ile veri korumaya yönelik şifreleme, anonimleştirme ve bulanıklaştırma (*pseudonymization*) tekniklerinin uygulaması, KVKK/GDPR uyumluluk sürecinin zorunlu parçalarıdır.

İzleme ve Raporlama

KVKK/GDPR düzenlemeleri gereğince denizcilik şirketleri gerektiğinde politikalarını ve prosedürlerini güncelleyerek, personelini ve mürettebatını eğitmeli ve gerekli resmi belgelerini ve anlaşmalarını güncelleyerek uyumluluklarını sürekli olarak izlemelidirler.

Ayrıca olası bir denetim için bu uyumluluk altyapılarını da gösterebilmelerinin en sağlıklı yolu da düzenli olarak ilgili raporların üretilmesi ve arşivlenmesidir.

Yönetişime Yönelik Bir Kültürün Geliştirilmesi

Bir denizcilik şirketinin iç denetim ortamında kişisel verilerin korunmasına yönelik güvenlik tedbiri, etkili risk azaltma yöntemleri her zaman sonunda insanların bu önlemleri ne kadar iyi anladıkları ve uyguladıklarına bağlı olacaktır.

Denizcilik şirketlerinin kendilerini aktif olarak korumaları için yönetişim odaklı bir kültürün oluşturulması ve sürdürülmesi gerekmektedir. Bu kişisel verilerin saçılma tehditlerine karşı çok daha etkili bir kalkan oluşturur.

Denizcilik şirketleri, gerçekten risk odaklı, etkili ve verimli bir şekilde uyumluluk çalışmaları ile hem uyumluluk maliyetlerini hem de olası riskleri ve etkilerini en aza indirgemelidirler.

5. Denizcilik Sektörü Yaptırım Örnekleri

AB kişisel verilerin korunması konusunda 1981 yılından bu yana ciddi mevzuat ve uygulamaları hayata geçirmiş, bu mevzuat ve uygulamaları gerek iş hayatının sürekliliği gerekse de kişilerin mahremiyetinin korunması açısından dengeleyecek daha çok tecrübe edinme fırsatı yakalamıştır.

Bu kapsamda, kişisel verilerin korunması konusunda yeterli hassasiyeti göstermeyen çok büyük ölçekli uluslararası firmalar ve birçok kamu kurumlarına çeşitli yaptırımlar uygulamıştır. Aşağıda bu idari para cezaları uygulamalarından bazı örnekler verilmiştir.

Entirely Shipping & Trading S.R.L.

13 Aralık 2019'da Romanya Ulusal Denetim Otoritesi, Entirely Shipping & Trading SRL'nin, çalışanların ofislerine, soyunma odalarına ve yemek odasına ses-video gözetim kameraları kurduğunu ve belirli yerlerde (*kısıtlı erişim alanları*) erişimin parmak izlerine dayandığını iddia eden bir şikâyet üzerine yaptığı incelemede;

- ✓ Veri sorumlusunun, faaliyetlerini yürüttükleri ofislerde ve yedek kıyafetlerini sakladıkları yerlerde (*soyunma odaları*) bulunan video kameralar aracılığıyla çalışanlarının kişisel verilerini aşırı derecede işleyerek GDPR'nin 5. maddesi (1) c, 6. ve 7. maddelerinin hükümlerinin ihlali için 5.000 €'ya eşdeğer,
- ✓ Veri sorumlusunun, daha az müdahaleci olan diğer araçlar kullanmak seçeneklerinin varlığına rağmen, çalışanların biyometrik verilerini (*parmak izlerini*) işleyerek GDPR'nin 5 maddesi (1) c, 9 ve 7. maddelerinin hükümlerinin ihlali için 5.000 €'ya eşdeğer

2 ayrı 5.000 € idari para cezası uyguladı.[16]

Veri sorumlusu, veri gözetiminin çıkarları veya temel hak ve özgürlükleri üzerinde hüküm sürecek olan video gözetim sisteminin tesisine kurulması için haklı bir meşru menfaat kanıtlayamamıştır. Ayrıca erişim kontrol sistemi yoluyla işlenen biyometrik veriler, yeterli, ilgili ve işlendikleri amaçlarla ilgili olarak gerekli olanlarla sınırlı amaçlar için toplanmamıştır.

Veri Sorumlusunun ayrıca, Veri Koruma Etki Değerlendirmesi (*DPIA*) yapmadığı da belirlenmiştir.

Veri sorumlusuna idari para cezalarının yanı sıra ayrıca aşağıdaki düzeltici önlemler de uygulanmıştır:

- ✓ "**veri minimizasyonu**" ilkesini gözeterek, kişisel veri işleme işlemlerinin video izleme faaliyeti içinde uygunluğunu sağlamak için düzeltici önlemler,
- ✓ "**veri minimizasyonu**" ilkesini gözeterek kişisel veri işleme operasyonlarının erişim kontrolü faaliyeti içinde uygunluğunu sağlamak için düzeltici önlemlerin alınması.

Clarkson Plc Veri İhlali

Londra merkezli deniz taşımacılığı hizmetleri veren Clarkson Plc., şirketin bilgisayar sistemine yetkisiz bir erişimin gerçekleştiğini ancak söz konusu yetkisiz erişim tespit edilir edilmez müdahale edildiğini ve söz konusu siber saldırının şirketin işleyişini herhangi bir şekilde etkilemediğini duyurmuştur. 7.Kasım.2017 tarihinde saldırıyı öğrenen Clarkson, söz konusu saldırıya karşı derhal önlem aldığını ve saldırı konusunda araştırma yaptığını belirtmiştir. Ancak ilerleyen zamanlarda, şirket bilgilerine yetkisiz erişen üçüncü kişilerin, elde ettikleri bilgiler karşılığında şirketten fidye istedikleri ve şirketin söz konusu isteği reddettiği belirtilmiştir. Çalınan bilgilerin kullanıcılara ait doğum tarihi, iletişim bilgisi, sosyal güvenlik numarası, banka hesap bilgisi ve pasaport ile kredi kartı bilgilerine ilişkin olabileceği ifade edilmiştir.[17]

[16] https://edpb.europa.eu/news/national-news/2019_en

[17] https://gcaptain.com/clarkson-plc-reveals-details-of-2017-cyber-security-incident/
https://www.theguardian.com/technology/2017/nov/29/shipping-charksons-data-hacker-cyber-attack
https://safetyatsea.net/news/2017/clarksons-braced-for-data-leak/

Maersk Veri İhlali

GoldenEye veya Petya olarak adlandırılan bir bilgisayar virüsü, dünya konteyner ticaretinde %18'lik bir hacme sahip olan Maersk'in dünya genelindeki tüm bilgisayar sistemlerini etkilemiştir. Söz konusu siber saldırı nedeniyle, dünya genelindeki birçok limanda gemilerin boşaltılması gibi işlemler yavaşlamış hatta sistemin arızalı olması nedeniyle bazı işlemler eski usulde yürütüldüğü gibi kâğıt üzerinden yürütülmüştür. IT devi olarak bilinen Maersk'in siber saldırıdan büyük çaplı olarak etkilenmesinin sektördeki güvenlik açığına işaret ettiği belirtilmiştir. Maersk, 2017 yılının Temmuz ve Ağustos aylarına ilişkin faaliyetlerini engelleyen siber saldırının şirkete yaklaşık 250-300 Milyon $ değerinde bir kayba mal olduğunu belirtmiştir.[18]

MTISC-GoG Veri İhlali

Gulf of Guinea (*MTISC-GoG*) adlı deniz ticareti bilgi paylaşım merkezi, deniz korsanlarının, bölgedeki gemilerin bulundukları konum da dâhil olmak üzere bölgedeki gemilere ilişkin detayları bir siber saldırı sonucunda ele geçirdiği bilgisini yalanlamıştır. Ancak Danimarka sahil güvenliği, söz konusu siber saldırının gerçekleşmiş olabileceğine dair birçok şikâyet aldıklarını belirterek bölgedeki gemileri dikkatli olmaları konusunda uyarmıştır.[19]

Austral Veri İhlali

Avustralyalı gemi yapım şirketi Austral, Avustralya'da gerçekleştirdiği faaliyetlerine yönelik bir siber saldırı gerçekleştirildiğini ifade etmiştir. Söz konusu duruma ilişkin olarak çeşitli ülkelere açıklama yapan şirket, Amerika ve Avusturya'ya ait bilgisayar ağlarının özellikle ayrı tutulması ve şirketin güvenlik sürecinin saldırıyı ortaya çıkarması nedeniyle saldırı sonucunda herhangi bir hassas verinin çalınmadığını ve Amerika'daki faaliyetlerinin söz konusu saldırı nedeniyle etkilenmediğini belirtmiştir. Austal yalnızca, bazı gemi tasarım çizimleri ile birlikte personele ait telefon numarası ve e-posta adresi bilgilerinin çalınmış olabileceğini duyurmuştur. Söz konusu bilgilerin karanlık webte satışa çıkmış olabileceği belirtilmiştir.[20]

COSCO Veri İhlali

24.Temmuz.2018 tarihinde Cosco Deniz Taşımacılığı tarafından fark edilen güvenlik açığının şirketin Amerika'daki faaliyetlerini olumsuz etkilediği ve gemi operatörü şirketin söz konusu siber saldırıya müdahale etmekte ve oluşabilecek büyük çaplı hasarları önlemede oldukça geç kaldığı belirtilmiştir. Konteyner hattına sahip olan Şangay merkezli şirketin 26 Temmuz'da müşterilerine dünya çapındaki ağlarından iç ağlarını izole ettiğini ve Amerika hariç diğer bölgelerde yer alan ağ uygulamalarını sürdürebileceğini bildirdiği ifade edilmiştir. Ancak siber güvenlik şirketlerinin, Cosco'nun uyarılarının aksine, Cosco'nun gemilerinin, gemi ve kıyı bazlı operasyonları arasındaki iç bağlantı nedeniyle saldırıya açık olduğunu belirledikleri de siber güvenlik şirketleri tarafından ifade edilmiştir. Bu kapsamda siber güvenlik şirketi Naval Dome, gemilerin doğrudan saldırıya maruz kalmalarının gerekli olmadığını, siber saldırının kıyı merkezli IT sistemlerinden gelerek kolaylıkla geminin kritik işletim sistemlerine sıçrayabileceğini belirtmiştir.[21]

Channel Veri İhlali

Deniz güvenliği hizmeti ile birlikte denizciliğe ilişkin çeşitli hizmetler sağlayan Chanel Gemi Hizmetleri (*CSS*), 2018 yılında TheDarkOverlord (*TDO*) adı verilen hacker grubu tarafından siber saldırıya uğramıştır. TDO, saldırı sonucunda ele geçirdiği CSS personeline ait denizci sözleşmelerini; sözleşmenin taraflarını, pasaport numaralarını, maaş bilgilerini ve sözleşmeye ilişkin diğer bilgilerini yayınlamıştır. Ayrıca TDO, e-dolandırıcılık gibi faaliyetlerde bulunmak isteyen kişilerin kullanabileceği nitelikteki müşteri bilgilerini de yayınlamıştır. Bunların yanında TDO ayrıca, navigasyon rotaları, gemilerde bulunan mürettebat ve silahlı güvenlik güçlerinin

[18] https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE
https://safetyatsea.net/news/2017/global-impact-of-cyber-breach-on-apm-terminals-muted-analyst-finds/
https://www.linkedin.com/pulse/4-cases-cyber-security-failures-shipping-history-chronis-kapalidis/

[19] https://www.helpnetsecurity.com/2016/03/03/sea-pirates-and-cyber-attacks-information-security-breaches-in-the-maritime-industry/

[20] https://safetyatsea.net/news/news-safety/2018/australian-defence-shipbuilder-austral-victim-of-iranian-cyber-attack/
https://www.marineinsight.com/shipping-news/shipbuilder-austal-suffers-data-breach-in-cyber-attack/

[21] https://safetyatsea.net/news/2018/cosco-fleet-could-still-be-at-risk-following-attack-warns-cyber-expert/

güzergâhlarına ilişkin bilgiler dâhil olmak üzere, CSS'e ait olan birçok hassas bilgiyi ele geçirdiklerini ve bu bilgilerin korsanlar tarafından gemi mürettebatlarını rehin almak üzere kullanılabileceğini belirtmiştir.[22]

IRISL Veri İhlali

İran'ın en iyi kargo deniz taşımacılığı şirketlerinden olan The Iranian Shipping Line (*IRISL*), 2011 yılında sisteminin çöktüğünü ve bütün kargo takip verilerini kaybettiğini duyurmuştur. Şirketin söz konusu siber saldırı sonucunda, kaybolan konteynerler ve iletilemeyen kargolar nedeniyle ciddi bir kayba uğradığı ifade edilmiştir.[23]

Antwerp Limanı Veri İhlali

Ekim 2013'te Belçika'da bulunan Antwerp limanı sistemine uyuşturucu tacirleri tarafından bir siber saldırı düzenlendiği ve saldırı sonucunda siber saldırganların konteynerlerin limandaki hareketini kontrol eden sisteme sızarak, uyuşturucu içeren sevkiyatların maskelenmesine ve tespit edilememesine imkân sağladığı ifade edilmiştir.[24]

Avustralya Gümrük Kargo Sistemi Veri İhlali

2012 yılında, hangi gemi konteynerlerinin polis tarafından işaretlendiğinin tespit edilmesi ve bu sayede kaçak ürün taşıyan yüksek riskli konteynerlerin terk edilmelerinin sağlanması amacıyla, Avustralya Gümrük ve Sınır Koruma Hizmeti Ajansı'nın kargo sistemine siber saldırı düzenlendiği belirtilmiştir.[25]

Güney Kore GPS Veri İhlali

2016 yılında, Kuzey Kore ajanları tarafından bozulan GPS sinyalleri nedeniyle 70 Güney Kore balıkçı gemisinin limana erken dönüş yaptığı ve Kuzey Kore'nin söz konusu sabotajı inkâr etmesine rağmen üç gün boyunca sinyal bozma işlemini sürdürdüğü ifade edilmiştir.[26]

[22] https://www.databreaches.net/channel-ship-services-hacked-by-thedarkoverlord-has-maritime-security-been-compromised/
[23] https://threatspan.com/2017/12/29/top-11-maritime-security-compromises-of-all-time/
[24] https://threatspan.com/2017/12/29/top-11-maritime-security-compromises-of-all-time/
[25] https://threatspan.com/2017/12/29/top-11-maritime-security-compromises-of-all-time/
[26] https://threatspan.com/2017/12/29/top-11-maritime-security-compromises-of-all-time/

6. KVKK/GDPR Uyumluluk Çözümü

Kişisel verilerin korunmasıyla tutarlı bir uygulama için tüm bu yapıları uçtan uca kapsayacak uygulama projesine gerek vardır. Bu, KVKK ve GDPR için uygulama projesinin tüm bileşenlerini kapsayan sürecin izlenmesi ve değerlendirilmesi için **tam bir çözüm** olmalıdır.

Bu nedenle; Kişisel Verilerin Korunmasına yönelik gerçekleştirilecek bir çalışmada hukuki, idari ve teknik olmak üzere üç farklı eksenli çalışmalarının bütünleşik olarak hep birlikte yapılması zorunludur.

6.1. Hukuki Çalışmalar

Hukuki değerlendirmeler;

- ✓ Aydınlatma ve açık rıza metinlerinin düzenlenmesi,
- ✓ Çalışanlar, tedarikçiler, müşteriler, işortakları ve benzeri 3. taraflarla düzenlenen sözleşmelerin gözden geçirilip KVKK /GDPR mevzuatına uyumlu hale getirilmeleri,
- ✓ Kişisel verilerle çalışan personel ile yine mevzuata uygun sözleşmelerin düzenlenmesi,
- ✓ Veri sahiplerinin KVKK/GDPR kapsamındaki taleplerinin incelenmesi ve değerlendirilmesi,
- ✓ KVKK/GDPR ilgili diğer konulardaki hukuki değerlendirmelerin yapılması konularını içerir.

6.2. İdari Çalışmalar

İdari değerlendirmeler;

- ✓ Veri koruma ve güvenlik politikalarının belirlenmesini,
- ✓ Risk yönetimini,
- ✓ Proje metodolojisini ve değişim/uyum sürecinin KVKK/GDPR düzenlemelerine göre yönetilmesini içerir.

Ayrıca,

- ✓ KVKK/GDPR mevzuatına göre kişisel verilerin korunmasına yönelik gerekli kurum içi organizasyonun oluşturulması,
- ✓ Görev ve sorumluluk matrisinin hazırlanması ve süreçlerin düzenlenmesi
- ✓ KVKK/GDPR kurumları ile iletişim ve başvurularda gerekli desteklerin sağlanması konularını da içerir.

Bu kapsamda yapılacak uyumluluk çalışmaları;

- ☑ KVKK Önleyici ve Düzeltici Danışmanlık
- ☑ Politikalar / Süreçler / Belgeler
- ☑ Gizlilik ve Mahremiyet Politikaları
- ☑ Veri Koruma Etki Analizi
- ☑ Eğitim

kapsamaktadır.

6.3. Teknik Çalışmalar

Müşteri verilerinin teknik kontrolü, uyumluluğunun anahtarıdır;

- ✔ Yapılandırılmış (*veritabanları*), yarı yapılandırılmış (*Excel vb.*) ve yapılandırılmamış (*dokümanlar, PDF vb*) veri analizi uygulamaları,
- ✔ Kullanılan uygulamalar ve veri tabanları,
- ✔ Veri merkezi, güvenlik duvarı sistemi, veri depolama,
- ✔ Bulut servisi, e-posta hizmetleri ve güvenlik sistemlerini içerir.

Ancak tümü bunlarla sınırlı olmayıp, KVKK/GDPR zorunlu kıldığı analizlerin ve değerlendirmelerin yapılması ve Müşteri tarafından kullanılan diğer özel uygulamalar da bu sürece dâhil edilmektedir. *(Kişisel Veri Yönetişimi, Müşteri Talep Yönetimi, Şifreleme vb.)*

KVKK/GDPR Uyumluluk çözümünün ikinci aşaması, idari ve hukuki süreçlerin belirlenen tespitlerin gözden geçirilmesi ve tamamlanması ile tüm teknik altyapının uyum otomasyonunu sağlayarak ***bütünleşik çözümü*** gerçekleştirecek bir aşamadır. Bu teknik uygulama süreçlerini tamamlamak, düzenli ve sürekli bir süreç otomasyonu ile uyum için hazır hale gelinmesinin ön koşuludur. Bu kapsamda;

- ☑ Yapılandırılmış / Yapılandırılmamış Ortamlarda Veri Keşfi
- ☑ Veri Sınıflandırılması / Süreç Yönetimi / Veri Yönetişimi
- ☑ Şifrelendirme / Anonimleştirme / Silme / Yok Etme
- ☑ Veri Sahibi Talep Yönetimi
- ☑ Risk Yönetimi / Veri Koruma Etki Analizi
- ☑ Uyumluluk
- ☑ Denetim

çalışmaları "İkinci Aşamada" gerçekleştirilmesi gereken ve temel bir teknik altyapıyı gerektiren iş ve işlemlerdir.

Kişisel verileri korumanın ve korumada sürekliliğin sağlanması ancak uçtan-uca izleme ve denetleme olanağı sağlayan teknik bir çözüm ile mümkündür ve **bu da KVKK/GDPR uyumluluğunun gerçek anahtarıdır.**

■

ACCERT A.Ş.

ACCERT A.Ş. 2018 Yılında sadece Kişisel Verilerin Korunması ile ilgili çalışmalar yapmak için kurulmuştur.

Kurucuları: Bilişim Teknolojileri, Bilgi Güvenliği ve Regülasyon alanında 30 yılın üzerinde deneyimli uzman ve akademisyenlerden oluşmaktadır.

Vizyonu: Kişi, kurum ve kuruluşları ulusal ve uluslararası kişisel verilerin korunması süreçlerine hazırlamaktır.

Misyonu: Kişilerin gizlilik hakları ile meşru iş fırsatları arasında adil denge kurmak için en uygun çözümleri sunmaktır.

Kişisel Verilerin Korunması Kanunu (*KVKK*) ve Avrupa Veri Koruma Tüzüğü (*GDPR*) gereklilikleri ve yükümlülükleri ile kurum ve kişiler arasında adil denge kurmak için farkındalığı artırmak ve güven ortamının devamlılığını sağlamak amacıyla bütünsel çözümler sunmaktır.

ACCERT A.Ş. Vizyon ve Misyonuna bağlı olarak konusunda uzman ulusal ve uluslararası kuruluşlar ile işbirliği yaparak kişisel verilerin korunması konusunda çözüm sunma çalışmalarını ilerletmiştir.

KVKK ve GDPR düzenlemelerine yönelik uyumluluk çalışmalarında danışmanlık, denetim ve eğitim hizmetleri sunmaktadır.

Bugün iş ortakları ile bu alanda uçtan uca çözüm sunabilen Türkiye'deki öncü kuruluşlardan biridir .

ACCERT Sertifikasyon, Belgelendirme, Danışmanlık, Eğitim ve Denetim A.Ş.

Uğur Mumcu'nun Sokağı No:39/7
Büyükesat Mahallesi, Çankaya / Ankara

Telefon : + 90 (312) 436 41 93
E-Posta : accert@accert.com.tr

ISBN-978-625-400-112-3

ACCERT