

KİŞİSEL VERİLERİN KORUNMASI

Kişisel Verileri Koruma Politikası

İÇİNDEKİLER

1. TANIMLAR VE İLGİLİ REGÜLASYONLAR
 1. İLGİLİ REGÜLASYONLAR
 2. TANIMLAR
2. AMAÇ
3. KAPSAM
4. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUSUSLAR
 1. İLGİLİ REGÜLASYONLAR
 2. TANIMLAR
5. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN HUSUSLAR
 1. KİŞİSEL VERİLERİN İŞLENMESİNDE TEMEL İLKELER
 2. KİŞİSEL VERİLERİN İŞLENMESİ ŞARTLARI
 3. ÖZEL NİTELİKLİ VERİLERİN İŞLENMESİ ŞARTLARI
 4. KİŞİSEL VERİ İŞLEME AMAÇLARI
6. KİŞİSEL VERİLERİN AKTARIMI
 1. KİŞİSEL VERİLERİN YURTİÇİ ÜÇÜNCÜ KİŞİLERE AKTARIMI
 2. KİŞİSEL VERİLERİN YURTDIŞI ÜÇÜNCÜ KİŞİLERE AKTARIMI
 3. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN AKTARIMI
 4. TİM, İLGİLİ BAKANLIK VE DİĞER İHRACATÇI BİRLİKLERİ
7. ÜÇÜNCÜ KİŞİLERDEN KİŞİSEL VERİLERİN ALINMASI
8. KİŞİSEL VERİ KATEGORİLERİ
9. BİNA GÜVENLİĞİ
 1. GÜVENLİK KAMERASI KAYITLARI
 2. XRAY
 3. ZİYARETÇİ KAYITLARI
 4. ARAÇ GİRİŞLERİ
 5. ZİYARETÇİ İÇİN İNTERNET ERİŞİMİ KAYITLARI
 6. PERSONEL TAKİP SİSTEMLERİ
 7. YEMEKHANE
10. TELEFON SANTRALİ
11. İNTERNET SİTELERİ
12. KİŞİSEL VERİLERİN ANONİMLEŞTİRİLMESİ-SİLİNMESİ
 1. KİŞİSEL VERİLERİN KAYDEDİLME SÜRESİ
 2. ANONİMLEŞTİRİLMESİ
 3. KİŞİSEL VERİLERİN SİLİNMESİ
 4. KİŞİSEL VERİLERİN İMHA EDİLMESİ

- 13. KİŞİSEL VERİ SAHİPLERİNİN HAKLARI**
14. VERİ KORUMA ETKİ DEĞERLENDİRMESİ
15. VERİ SORUMLUSU İRTİBAT KİŞİSİ, VERİ KORUMA GÖREVLİSİ
16. VERİ SIZINTISI DURUMUNDA ALINACAK TEDBİRLER

1. TANIMLAR VE İLGİLİ REGÜLASYONLAR

1. İLGİLİ REGÜLASYONLAR

HİB için bu politika oluşturulurken özellikle dikkat edilen regülasyonlar şu şekildedir.

6698 sayılı Kişisel Verilerin Korunması Kanunu

GDPR

5910 Sayılı Kanun

Türk Borçlar Kanunu

Türk Ticaret Kanunu

2. TANIMLAR-KISALTMALAR

KISALTMALAR	
KVKK	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu
GDPR	EU (Avrupa Birliği) General Data Protection Regulation
Anayasa	9 Kasım 1982 tarihli ve 17863 sayılı Resmi Gazete'de yayımlanan 7 Kasım 1982 tarihli ve 2709 sayılı Türkiye Cumhuriyeti Anayasası
HİB	Hizmet İhracatçıları Birliği Genel Sekreterliği
TİM	Türkiye İhracatçılar Meclisi
Veri İşleyen	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 kişi
Veri Sahibi/İlgili Kişi/İlgili Kişiler	HİB'in çalışanları, üye firma yetkilileri, çalışanları, çalışan adayları, stajyerleri, hizmet aldığı kişiler, tedarikçileri, iş birliği içerisinde olduğu kurumların çalışanları, ziyaretçiler, burada sayılanlarla sınırlı olmamak üzere diğer üçüncü kişiler gibi kişisel verileri HİB tarafından işlenen gerçek kişileri ifade eder.

Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Açık Rıza	Kişisel verilerin işlenmesi için, belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.

2. AMAÇ

HİB olarak kişisel verilerinizin güvenliğine ve gizliliğine önem vermekteyiz. Kişisel verilerinizin güvenli bir şekilde ve hukuka uygun olarak alınması, kaydedilmesi, işlenmesi, paylaşılması, korunması ve gerektiğinde silinmesi veya anonim hale getirilmesi için gerekli idari ve teknik önlemleri almaktayız.

Bu politikanın amacı, HİB'in kişisel verileri, evrensel hukuk kurallarına, Anayasaya, 6698 sayılı Kişisel Verileri Koruma Kanununa ve EEA Bölgesi dahilindeki kişisel verilerin kullanımına yönelik işlemlerde Avrupa Birliği Genel Veri Koruma Tüzüğüne (GDPR) uygun olarak elde etmesini, işlemesini, paylaşmasını, korumasını ve gerektiğinde silmesini veya anonim hale getirmesini sağlamak için uygulanacak temel ilkeleri ve izlenecek yöntemleri ortaya koymaktır.

Bu politika HİB'in internet sitesinde (<http://www.hib.org.tr>) yayınlanır. HİB tarafından kişisel verileri işlenen kişilerin talebi doğrultusunda ilgili kişilerin erişimine sunulur.

3. KAPSAM

Bu Politika HİB tarafından gerçekleştirilen, kişisel verilerin alınması, işlenmesi ve korunmasına yönelik her türlü faaliyet için ve HİB tarafından verisi işlenen bütün gerçek kişiler için uygulanır. Tüzel kişilerin gerçek kişi yetkilileri ve çalışanlarına ait olan kişisel veriler buna dahildir.

HİB'in altında yer alan ihracatçı birliklerinin her ne kadar tüzel kişilikleri bulunuyor olsa da, bütün veri işleme süreçleri HİB tarafından düzenlendiğinden, birliklerin kendilerine ait genel sekreterlik yapıları olmayıp, bütün idari işlemleri HİB Genel Sekreterliği tarafından yürütüldüğünden, insan kaynakları, bilgi işlem, idari işler, muhasebe, kurumsal iletişim gibi veri işleme ile ilgili bütün birimler HİB altında teşkilatlanmış olduğundan dolayı, VERBİS sistemine yapılacak kayıt, veri sahipleri ve Kişisel Verileri Koruma Kurumu ile olan bütün ilişkiler, verilerin düzenlenmesi, veri işleme envanterinin tutulması, gerekli idari ve teknik önlemlerin alınması ve kişisel verilerin işlenmesi ile ilgili bütün hukuki, idari ve teknik süreçler HİB tarafından düzenlenecek, koordine edilecek, gerçekleştirilecek ve denetlenecektir.

Bu Politika uluslararası ISO 27001 Bilgi Güvenliği Yönetim Standardına uyumludur ve bu standarda uygun bir şekilde uygulanır.

Bu Politika HİB'in bütün çalışanlarının ve yetkili personellerinin, üye firmaların yetkililerinin ve çalışanlarının, iş birliği içerisinde olduğu bütün kurumların yetkililerinin ve çalışanlarının, HİB'i ziyaret eden kişilerin ve üçüncü kişilerin HİB tarafından işlenen bütün kişisel verilerine ilişkindir.

4. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUSUSLAR

HİB kişisel verilerin korunması için gerekli olan bütün önlemleri bütçesi ile uyumlu olacak şekilde alır. HİB Bilgi Güvenliği Yönetim Sistemi kapsamında ilgili standarda uygun olarak alınması gereken bütün teknik ve idari tedbirleri almaktadır. Bu tedbirler sadece elektronik ortamda kaydedilen verileri değil aynı zamanda yazılı, basılı, sözlü ortamlarda bulunan tüm dokümanlara ilişkin olarak alınmaktadır.

1. KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK ALINAN TEKNİK TEDBİRLER

HİB kişisel verilerin korunmasına ilişkin aşağıda belirtilen teknik ve idari tedbirleri almaktadır

- HİB ISO 27001 standardı kapsamında hazırlanan ilgili politikalarda belirtilen teknik tedbirleri almakta ve sorumluluklarını belirtilen prosedürlere uygun olarak yerine getirmektedir.
- HİB kullandığı bütün elektronik sistemler, bilgisayarlar, mobil cihazlar ve bu cihazlar üzerinde çalışan yazılımlar için zamanında güncellemeleri yapmakta ve personel tarafından yapılmasını sağlamaktadır.
- HİB teknolojik gelişmelere uygun olarak gerekli tedbirleri almakta ve alınan önlemleri periyodik olarak güncellemektedir.
- HİB sistemleri için kullanıcı hesap yönetimi ISO 27001 ile uyumlu olarak yapılmaktadır.
- Kablosuz erişim noktaları ile ilgili ISO 27001 kapsamında hazırlanan politikalara uyar.
- Veri kaybının önlenmesine ilişkin uygun yazılımlar ihtiyaç olduğu takdirde kullanılır.
- Saldırı tespit ve önlemeye ilişkin uygun sistemler kullanılır ve gerekli danışmanlıklar ve destekler alınır.
- Veriler periyodik olarak yedeklenir, bu yedeklere istenildiği takdirde geri dönüş sağlanabilir.
- Güçlü parola kullanımı otomatik sistemler tarafından yönlendirmeler ile sağlanmaktadır.
- Anti-virüs programları, güvenlik duvarları içeren yazılım ve donanımlar kullanılmakta ve bu güvenlik sistemleri sürekli güncel tutulmaktadır.
- Verilere yalnızca ilgili birim ve personelin erişiminin sağlanması için gerekli erişim ve yetkilendirmeye ilişkin teknik çözümler kullanılmaktadır.
- Kişisel verilere ve kişisel veri içeren dosyalara yapılan erişimlerin, gerekli görüldüğü takdirde, log kayıtları tutulmaktadır.
- Teknik konularda bilgili personel istihdam edilmektedir

- HİB'in ihtiyaları dođrultusunda, teknik personelin ilgili alanlarda bilgi ve kabiliyetlerini artırmaları iin gerekli eđitimler sađlanmaktadır.
- alıřanların teknik kabiliyetlerini geliřtirmek iin yapmak istediđi alıřmalar teřvik edilmekte ve bunun iin uygun büte ayrılmaktadır.
- ISO 27001 standardı ile uyumlu olarak, güvenlik aıklarının tespiti, risklerin belirlenmesi ve bu risklerin elimine edilmesi iin gerekli güvenlik testleri periyodik olarak yapılmakta ve gereken önlemler alınmaktadır.
- Kiřisel Veri İřleme Envanteri ile ilgili olarak HİB personeline özel yazılmıř olan HİB Veri Envanteri Programı kullanılmaktadır ve Kiřisel Veri İřleme Envanteri sürekli olarak güncel tutulmaktadır.
- Veri sahiplerinin verilerine iliřkin olarak isteklerini en kısa sürede iřlemek ve cevaplandırmak iin HİB Veri Envanteri Programı kullanılmaktadır.
- Aık rıza yönetimi iin HİB Veri Envanteri Programı ile yapılmaktadır. Aık rızanın iptal edilmesi durumunda ilgili verinin silinmesi sađlanmaktadır.

2. KİŐİSEL VERİLERİN KORUNMASINA YÖNELİK İDARİ TEDBİRLER

HİB kiřisel verilerin korunmasına iliřkin ařađıda belirtilen idari tedbirleri almaktadır.

- Kiřisel Veri İřleme Envanteri hazırlanır ve bu envanter sürekli olarak güncel olarak tutulur.
- Hem ISO 27001 hem KVKK kapsamında kurumsal politikalar hazırlanır ve bu politikalar gerektiđinde güncellenir.
- Kiřisel verilerin üçüncü kiřilerle paylařılmak durumunda olduđu sözleşmeler Kiřisel Verileri Koruma Kanununa uygun řekilde ve Kiřisel Verileri Koruma Kurumu'nun önerileri ve direktifleri dođrultusunda hazırlanır.
- İř sözleşmesi, HİB alıřanları Aydınlatma Bildirimi, Disiplin Yönetmeliđi ve Kiřisel Verileri Koruma Kanununa uygun hükümler ierir.
- alıřanlara kiřisel verilerin korunması ile ilgili periyodik olarak eđitimler verilmektedir. Yeni istihdam edilen personel konu ile ilgili olarak bilgilendirilmekte ve en kısa sürede eđitim alması sađlanmaktadır.
- HİB'in teknolojik olarak satın aldıđı hizmet ve sistemlere iliřkin anlaşmaların teknik şartnameleri ve sözleşmeleri HİB'in Kiřisel Verileri Koruma Politikası ile uyumlu olacak řekilde ve gerekli teknik güvenlik önlemlerini ierecek řekilde hazırlanmaktadır.
- Kiřisel Veri İřleme Envanteri güncel olarak tutulmaktadır.
- Kiřisel Verileri Koruma Kurulu'nun aldıđı kararlar incelenmekte, bu kararlara bađlı olarak HİB'in alması gereken önlemler alınmaktadır.
- HİB yapılan iřlere uygun olarak gerekli gizlilik taahhütnamelerini hazırlar.
- HİB gerekli risk analizlerini periyodik olarak yapar.
- HİB kurum ii düzenli ve rastgele denetimler yapar.
- Veri sızıntısı söz konusu olduđu takdirde kriz yönetimi, kurul ve ilgili kiřiyi bilgilendirme süreçleri ve itibar yönetimi iin yapılmıř olan planlar devreye alınır, bu konu ile ilgili düzenli danıřmanlık hizmetlerinden faydalanılır.

5. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN HUSUSLAR

1. KİŞİSEL VERİLERİN İŞLENMESİNDE TEMEL İLKELER

Kişisel verilerin işlenmesinde HİB aşağıda belirtilen temel ilkelere uymaktadır.

Hukuka ve Dürüstlük Kurallarına Uygunluk

HİB kişisel verilerin işlenmesinde hukuksal düzenlemeler ile getirilen ilkelere, genel dürüstlük ve güven kurallarına uygun olarak hareket etmektedir. Bu kapsamda HİB kişisel verileri alınırken hangi amaçla ve ne şekilde işleneceği veri sahibine belirterek almaktadır ve yalnızca bu belirtilen amaçlar için ve belirtilen şekilde verileri işlemektedir.

Doğru ve Gerektiğinde Güncel Olma

HİB kendisine kanunla verilen görevleri en iyi şekilde yerine getirmek için ve kişisel veri sahiplerinin haklarını gözeterek kişisel verileri doğru ve gerektiğinde güncel olmasını sağlamak için gerekli çalışmaları yapar.

Belirli Açık ve Meşru Amaçlar İçin İşlenme

HİB yalnızca meşru ve hukuka uygun veri işleme faaliyetleri içerisindedir. HİB her veri işleme faaliyeti için amacını açık ve kesin olarak belirlemekte ve yalnızca bu amaç dahilinde kişisel verileri işlemektedir.

İşlendikleri Amaçlarla Bağlantılı, Sınırlı ve Ölçülü Olma

HİB kişisel verileri yalnızca belirtilen amaçlarla sınırlı olarak işler. Amacın gerçekleşmesi ile ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınır.

İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç ile Sınırlı Süre Muhafaza Edilme

HİB kişisel verileri yalnızca mevzuatta öngörülen veya işlendikleri amaca uygun süre muhafaza eder. Bu kapsamda HİB ilgili mevzuatta öngörülen bir süre olup olmadığını değerlendirir. Bunun haricindeki durumlarda kendi görevleri ile ilgili işlerde ilgili kurumlardan, Bakanlıktan ve gerekli olduğu takdirde KVK Kurumundan görüş alır ve buna göre süre belirler. Bu durumun haricinde kalan hallerde kişisel verileri işlendikleri amaç için uygun bir süre belirleyerek o süre kadar muhafaza eder.

Şeffaflık

HİB kişisel veri işleme konusunda şeffaflığa önem verir. Kişisel verilerin hangi amaçla ve hangi hukuki dayanak ile işlendiğine ilişkin ilgili kurumlara ve talep etmeleri halinde kişisel verilerin sahiplerine bilgi verir.

Veri Küçültme

HİB kişisel verileri, amacına uygun ve sadece bu amaçla ilgili ve sınırlı bir şekilde alır, kaydeder ve kullanır.

2. KİŞİSEL VERİLERİN İŞLENMESİ ŞARTLARI

HİB kişisel verileri 6698 sayılı kanunun 5. maddesinde yer alan aşağıdaki şartlardan en az birinin var olması durumunda işlemektedir.

- **Açık Rıza:** Bilgilendirmeye dayalı ve özgür irade ile açıklanan açık rızanın varlığı durumunda kişisel veri işlenebilir.
- **Kanunlarda Açıkça Öngörülmesi:** Kanunlarda açıkça öngörüldüğü durumlarda.
- **Fiili İmkânsızlık:** Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması halinde ilgili kişinin kişisel verileri işlenebilecektir.
- **Sözleşmenin Kurulması veya İfası:** Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin zorunlu olması durumunda ilgili kişilerin bu amaçla sınırlı olmak üzere kişisel verilerinin işlenmesi mümkündür. Örneğin, bir sözleşme gereği paranın ödenmesi için alacaklı tarafın hesap numarasının alınması veya bir bankayla kredi sözleşmesi yapılması sırasında bankanın, o kişiye ait maaş bordrosunu, tapu kayıtlarını, icra borcu olmadığına dair belgeyi edinmesi gibi. Ayrıca, sözleşme gereği satıcının, malı teslim borcunu yerine getirmesi için alıcının adresini kaydetmesi ya da işverenin maaş ödemesini gerçekleştirmek amacıyla çalışanların banka bilgilerini elinde bulundurması, bu kapsamda değerlendirilebilecektir.
- **Veri Sorumlusunun Hukuki Sorumluluğu:** Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlenmesinin zorunlu olduğu hallerde ilgili kişinin kişisel verileri işlenebilecektir.
- **İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması:** İlgili kişinin kendisi tarafından alenileştirilen, bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verileri işlenebilecektir. Bu duruma örnek olarak ise bir kişinin belirli hallerde kendisiyle iletişime geçilmesi amacıyla iletişim bilgilerini kamuya açık şekilde ilan etmesi verilebilir. Kurumsal internet sitelerinde, çalışanların işyeri telefon numaraları ve kurumsal elektronik posta adreslerinin üçüncü kişilerin erişimine açık şekilde paylaşılması halinde de alenileştirmeden söz edilebilir.
- **Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Zorunlu Olması:** Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması halinde ilgili kişinin kişisel verilerinin işlenmesi mümkündür. Örneğin, bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması ya da kısıtlı bir kişinin haklarının korunması amacıyla vasisinin veya kayyumun, kısıtlının mali bilgilerini tutması gibi. Ayrıca, sözleşme sona erdikten sonra, olası yasal takiplere karşı zamanaşımı süresinin sonuna kadar fatura, sözleşme, kefaletname gibi belgelerin bu amaçlar için saklanması bu kapsamda değerlendirilecektir.

- **Veri Sorumlusunun Meşru Menfaati:** İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydı ile veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumunda, kişisel verilerinin işlenmesi mümkündür.

HİB yukarıda yazılı olan şartlar dışında herhangi bir şekilde kişisel veri işlememektedir.

3. ÖZEL NİTELİKLİ VERİLERİN İŞLENMESİ ŞARTLARI

HİB, Kişisel Verileri Koruma Kanununun özel nitelikli kişisel verilere ilişkin gösterdiği hassasiyete uygun davranmaktadır. Özel nitelikli kişisel veriler

- İlgili kişinin açık rızası olması halinde,
- Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki kişisel veriler kanunun öngördüğü hallerde,
- Kişisel veri sahibinin sağlığı ve cinsel hayatına ilişkin 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 işlenmektedir.

4. KİŞİSEL VERİ İŞLEME AMAÇLARI

5910 sayılı Türkiye İhracatçılar Meclisi İle İhracatçı Birliklerinin Kuruluş Ve Görevleri Hakkında Kanun'un 3. Maddesinin 3. fıkrası kapsamında HİB'in görevleri şunlardır:

“a) Dış ticarete ve yurt dışı hizmetlere ilişkin konularda çalışmalar yapmak, bu kapsamda; kamu kurum ve kuruluşları, sivil toplum kuruluşları ve ulusal ve uluslararası kuruluşlar nezdinde üyelerinin menfaatlerini ülke çıkarları çerçevesinde koruyucu ve geliştirici çalışmalar yapmak.

b) İhracatçılar arasında mesleki ahlâk ve dayanışmayı sağlamak.

c) TİM'in görüşünü ve Müsteşarlık onayını almak kaydıyla sektörü ile ilgili mevcut eğitim ve öğretim kurumlarına yardımda bulunmak, yenilerinin kurulmasına öncülük etmek ve katkıda bulunmak.

ç) TİM'in görüşünü ve Müsteşarlık onayını almak kaydıyla; amaç ve görevlerini gerçekleştirmeye yönelik vakıf kurmak veya kurulmuş olanlara iştirak etmek, bütçe imkânları çerçevesinde gerektiğinde mal ve hizmet almak, yaptırmak, satmak, kiralamak, rehin ve ipotek işlemleri tesis etmek ve kaldırmak, gerektiğinde iştigal sahası ile ilgili ortak hizmet verecek şirket, dernek, tesis ve işletmeler kurmak, kurulmuş olanlara iştirak etmek, laboratuvar, test, muayene ve belgelendirme konularında üyelerini desteklemek, fuar, sergi ve tanıtım faaliyetlerini düzenlemek, düzenlenecek fuar ve sergilere iştirak etmek ve tanıtım faaliyetlerinde bulunmak.

d) (Ek: 10/9/2014 - 6552/130 md.) TIR karneleri, ATA, A.TR ve EUR.1 dolaşım belgeleri, menşe şahadetnameleri ve EAN-UCC çizgi kod işlemleri, mal ve hizmetlerin uluslararası ticaretindeki beyanname, vesika ve benzeri belgelerin düzenlenmesi ve/veya onaylanması.

e) TİM tarafından verilecek dış ticarete ilişkin diğer görevleri yapmak.”

HİB, kanunla verilmiş olan bu vazifeleri yerine getirmek için gerekli olduğu takdirde kişisel verileri işlemektedir. Bu asli hedefler doğrultusunda yapılan işler esnasında, HİB diğer kanunlarda yer alan zorunluluklardan veya 6698 sayılı kanun kapsamında veri sorumlusu olarak kanuna ve hukuka uygun amaçlar için veri işlemektedir.

Bu kapsamda HİB aşağıdaki amaçlarla veri işlemektedir:

- Dış ticarete ve yurt dışı hizmetlere ilişkin konularda çalışmalar yapılması, bu kapsamda; kamu kurum ve kuruluşları, sivil toplum kuruluşları ve ulusal ve uluslararası kuruluşlar nezdinde üyelerinin menfaatlerini ülke çıkarları çerçevesinde koruyucu ve geliştirici çalışmalar yapılması,
- HİB'in faaliyetlerini, kurum prosedürlerine ve ilgili mevzuata uygun olarak sürdürebilmesi,
- Acil durum yönetimi süreçlerinin yürütülmesi,
- Bilgi Güvenliği süreçlerinin yönetilmesi,
- Çalışan Adayı/Stajyer seçme ve yerleştirme süreçlerinin yönetilmesi,
- Çalışan adaylarının başvuru süreçlerinin yürütülmesi
- Çalışan memnuniyeti ve bağlılığının sağlanması,
- Çalışanlar için iş akdi ve mevzuattan kaynaklanan yükümlülüklerin yerine getirilmesi,
- Çalışanlar için yan haklar ve menfaatlerin sağlanması,
- Denetim faaliyetlerinin yürütülmesi,
- Eğitim faaliyetlerinin yürütülmesi,
- Erişim yetkilerinin yönetilmesi,
- Finans ve muhasebe işlerinin yürütülmesi,
- Görevlendirme süreçlerinin yürütülmesi,
- Hukuk işlerinin takibi ve yürütülmesi,
- İç denetim faaliyetlerinin yürütülmesi,
- İletişim faaliyetlerinin yürütülmesi,
- İş sağlığı/güvenliği faaliyetlerinin yürütülmesi,
- İş sürekliliğinin sağlanması,
- Mal/hizmet alım süreçlerinin yürütülmesi,
- Organizasyon ve etkinliklerin yapılması,
- Sosyal sorumluluk ve sivil toplum aktivitelerinin
- Sözleşme süreçlerinin yürütülmesi,
- Sponsorluk faaliyetlerinin yürütülmesi,
- Stratejik planlama faaliyetlerinin yürütülmesi,
- Talep ve şikayetlerin takibi,
- Ücret Politikasının yürütülmesi,
- Yetenek/kariyer gelişimi faaliyetlerinin yürütülmesi,

- Yetkili kiři, kurum ve kuruluřlara bilgi verilmesi,
- Ziyaretçi kayıtlarının oluřturulması ve takibi,
- HİB'in kaliteli ve etkin bir insan kaynakları politikasını sürdürebilmesi,
- Personel temin süreçlerinin en iyi řekilde gerçekteřtirilmesi,
- Yetenek-kariyer geliřimi faaliyetlerinin planlaması ve icrası,
- Personel için iř akdi ve mevzuattan kaynaklı sorumlulukların yerine getirilmesi,
- Bilgi güvenlięi süreçlerinin planlanması, denetimi ve icrası, bilgi teknolojileri alt yapısının oluřturulması ve yönetilmesi
- Personelin bilgi, kabiliyet ve performansının ölçülmesi,
- Üye firmalar için gerçekteřtirilen hizmetlerin ve desteklerin etkin řekilde sürdürülmesi,
- Finans ve muhasebe iřlemlerinin sürdürülebilmesi,
- Üye firmaların yeni pazarlara açılmasını temin için dıř ticaret heyetlerinin düzenlenmesi,
- Yurtdıřından ölkemize gelen ticaret heyetlerinin organize edilmesi,
- Üye firma yetkililerinin yeřil pasaport bařvurularının yapılması,
- Yurtdıřı fuarlara etkin katılım saęlanması,
- İlgili Bakanlıęa ve TİM'e, üye firmaların gerçekteřtirdięi ihracat ile ilgili bilgilerin saęlanması,
- HİB çalıřanları için saęlık, eęitim vb desteklerin saęlanması,
- HİB çalıřanları ve/veya üye firma çalıřanlarının bilgi ve kabiliyetlerini geliřtirmek için eęitimlerin verilmesi,
- HİB'e ait demirbařların ve/veya dięer kaynakların güvenlięinin saęlanması,
- Ziyaretçi kayıtlarının oluřturulması ve takibinin yapılması,
- Bina içinde gerekli güvenlik önlemlerinin alınması,
- Yetkili kiři veya kuruluřlara mevzuattan kaynaklı bilgi verilmesi,

6. KİŐİSEL VERİLERİN AKTARILMASI

HİB'in üçüncü kiřilerle veri paylařımında kanunun koyduęu sınırlara, veri gizlilięine uygun prensiplere, ISO 27001 standardının gereklerine uygun olarak davranır. 5910 sayılı Türkiye İhracatçılar Meclisi İle İhracatçı Birliklerinin Kuruluř Ve Görevleri Hakkında Kanun'un 3.maddesi kapsamında HİB İhracatçı Birlikleri ve TİM ile koordine bir řekilde çalıřmak durumundadır. Bu yükümlölükleri doęrultusunda hızlı ve güvenli bir řekilde veri paylařımının yapılması için ařaęıda belirtilen esaslara dayalı olarak üçüncü kiřilerle veri paylařımı yapılmaktadır.

1. KİŐİSEL VERİLERİN YURTIÇİNDEKİ ÜÇÜNCÜ KİŐİLERE AKTARIMI

Kiřisel verilerin yurt içerisinde aktarılması için 6698 sayılı kanunun 8.Maddesi uyarınca ařaęıdaki řartlardan en az birinin saęlanması gerekmektedir:

- İlgili kiřinin açık rızasının alınması,

- Kanunlarda açıkça öngörülmesi,
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- 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 işlenmesinin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

Burada belirtilen durumlar haricinde HİB kişisel verilerinizi üçüncü kişilerle hiçbir şekilde paylaşmamaktadır.

2. KİŞİSEL VERİLERİN YURTDIŞINDAKİ ÜÇÜNCÜ KİŞİLERE AKTARIMI

HİB Cumhurbaşkanlığı tarafından 2019/12 tarih sayılı 6 Temmuz 2019 tarihinde Resmi Gazete'de yayınlanan Bilgi ve İletişim Güvenliği Tedbirleri konulu genelge doğrultusunda hareket etmektedir. Bu nedenle yurtdışı bulut hizmetleri, yurtdışı veri yedekleme, yurtdışı veri merkezi hizmeti, yurtdışı bulut santral hizmeti kullanmamaktadır. HİB'e hizmet veren Eposta sunucuları HİB'in kontrolünde ve yurtiçinde bulundurulacaktır.

Ancak,

- Kanundan veya uluslararası bir anlaşmadan kaynaklanan sebeplerden dolayı,
- Bir sözleşmenin ifası kapsamında zorunlu olması halinde,
- Fiili imkânsızlık durumunda,
- HİB'in hukuki bir sorumluluğu dolayısıyla ile,
- Bir hakkın tesisi, korunması, kullanılması nedeniyle,
- Veya HİB'in elzem olan bir meşru menfaati kapsamında,

Yeterli korumanın sağlanacağına ilişkin taahhütnamelerin alınması ve aşağıda belirtilen şartların sağlanması ile veri paylaşımı yapılmaktadır.

Kanunun 9. Maddesine göre yurtdışına veri aktarımı;

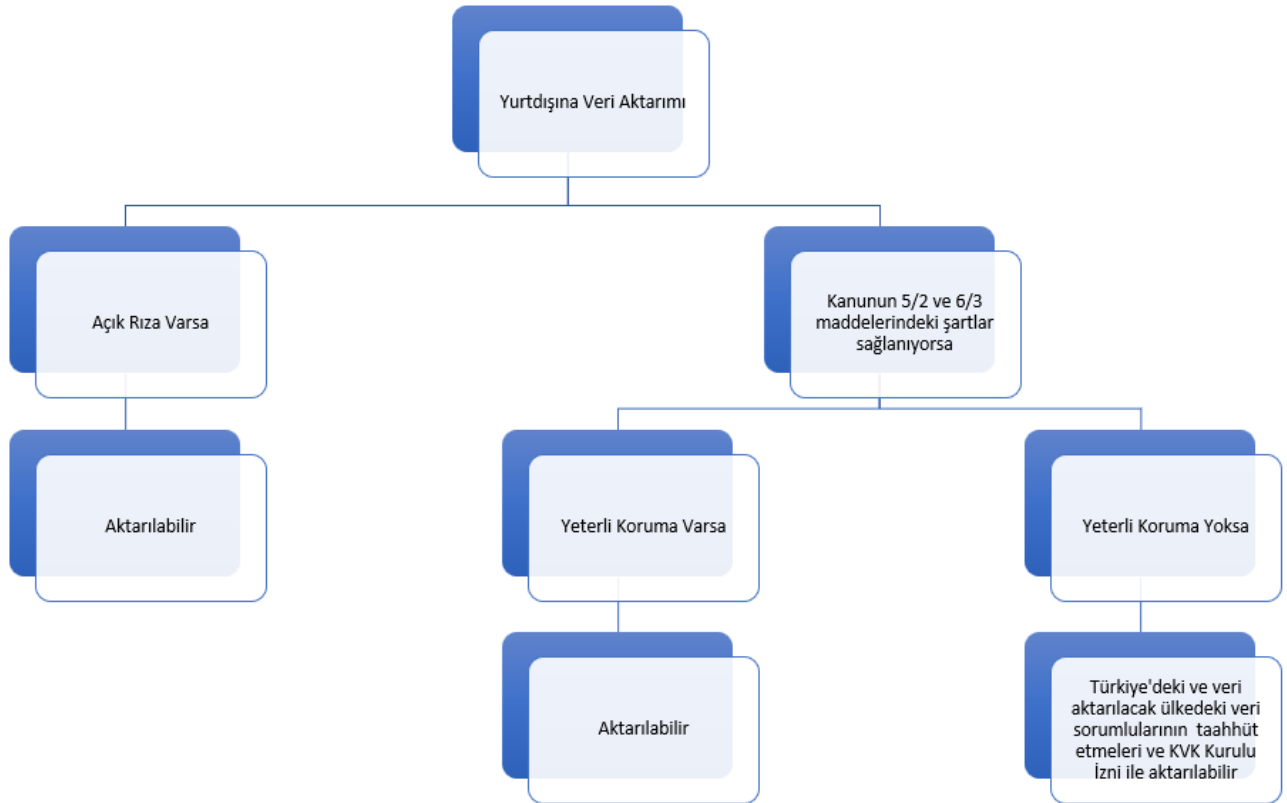
- İlgili kişinin açık rızasının bulunması,
- Yeterli korumanın bulunduğu ülkelere (Kurul tarafından güvenli kabul edilen ülkeler) veri aktarımında, Kanun'da belirtilen hallerin varlığı (Kanunun 5. maddesinin 2. fıkrası ile 6. maddesinin 3. fıkrasında belirtilen şartlar),
- Yeterli korumanın bulunmadığı ülkelere veri aktarımında Kanunda belirtilen hallerin varlığı (Kanunun 5. maddesinin 2. fıkrası ile 6. maddesinin 3. fıkrasında belirtilen şartlar) yeterli korumanın yazılı olarak taahhüt edilmesi ve Kurulun izninin bulunması,

durumlarında gerçekleştirilebilir. Kurulun izni bulunmadan yurtdışında bulunan üçüncü kişilere veri aktarılmaz.

HİB, yurtdışında bulunan ve **veri sorumlusu** durumunda bulunan üçüncü kişilere veri aktarımı yapar ise asgari şartlarını Kişisel Verileri Koruma Kurumu'nun belirlediği, her iki tarafın da veri sorumlusu olduğu duruma ilişkin, her iki tarafın imza ettiği bir taahhütnameyi Kişisel Verileri Koruma Kurumuna sunar. Kişisel Verileri Koruma Kurumunun onayı ile söz konusu veri aktarımı yapılır. Bu onay verilmeden HİB tarafından söz konusu üçüncü kişilere veri aktarımı yapılmaz.

HİB, yurtdışında bulunan ve **veri işleyen** durumunda bulunan üçüncü kişilere veri aktarımı yapar ise asgari şartlarını Kişisel Verileri Koruma Kurumu'nun belirlediği, veri sorumlusu-veri işleyen arasında yapılan ve her iki tarafın imza ettiği bir taahhütnameyi Kişisel Verileri Koruma Kurumuna sunar. Kişisel Verileri Koruma Kurumunun onayı ile söz konusu veri aktarımı yapılır. Bu onay verilmeden HİB tarafından söz konusu üçüncü kişilere veri aktarımı yapılmaz.

HİB ticaret heyeti düzenlenmesi, yurtdışı gezi, yurtdışı fuar vb. etkinlik ve faaliyetleri yaparken, karşı kurumlar ve tüzel kişilerle kişisel verileri paylaşabilmek için katılımcılardan kişisel verilerinin yurtdışı üçüncü kişilerle paylaşılabilmesi için açık rıza alır.



3. KİŞİSEL VERİLERİN İLGİLİ BAKANLIK, TÜRKİYE İHRACATÇI MECLİSİ VE DİĞER İHRACATÇI BİRLİKLERİ İLE PAYLAŞILMASI

5910 sayılı Türkiye İhracatçılar Meclisi İle İhracatçı Birliklerinin Kuruluş Ve Görevleri Hakkında Kanun'un 3. Maddesinin 3. fıkrası kapsamında ihracatçı birliklerinin görevleri arasında

- Dış ticarete ve yurt dışı hizmetlere ilişkin konularda çalışmalar yapmak, bu kapsamda; kamu kurum ve kuruluşları, sivil toplum kuruluşları ve ulusal ve uluslararası kuruluşlar nezdinde üyelerinin menfaatlerini ülke çıkarları çerçevesinde koruyucu ve geliştirici çalışmalar yapmak.
- İhracatçılar arasında mesleki ahlâk ve dayanışmayı sağlamak.
- TİM tarafından verilecek dış ticarete ilişkin diğer görevleri yapmak

sayılmıştır. Bu kapsamda yapılacak çalışmalarda, kanunla verilen bu görevlerin yapılabilmesi için HİB'in TİM, Bakanlık ve diğer ihracatçı birlikleri ile veri paylaşması gerekebilmektedir. Bu paylaşılan verilerin bir kısmı ise kişisel veri içermektedir. Kişisel verilerin TİM, ilgili Bakanlık ve diğer ihracatçı birlikleri ile paylaşılmasında HİB söz konusu kişisel verilerin sahiplerinin korunması için İlgili Bakanlık, TİM ve diğer ihracatçı birliklerinden kişisel veri içeren verilerin talep edilmesi durumunda aşağıda bulunan usule göre veri paylaşımını yapar.

- Talebin yazılı veya eposta üzerinden yapılması gerekmektedir.
- Talebi yapan kişi ve talebi ileten kişi belirtilmelidir.
- Talep 6698 sayılı kanuna uygun gerekçesini içermelidir.
- Alınan kişisel verinin ne amaçla işleneceği belirtilmelidir.
- Kişisel verilerin ne şekilde işleneceği belirtilmelidir.
- Şayet üçüncü kişilerle paylaşılacak ise paylaşılacak üçüncü kişilerin kimler olduğu ve bu üçüncü kişilerle paylaşma gerekçesi talepte belirtilmelidir.

Bu paylaşımlara ilişkin standart başvuru formu ilgili Bakanlık, TİM ve diğer İhracatçı Birliklerinin kolay başvuru yapabilmesi için kendilerine sunulur.

4. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN AKTARILMASI

Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

Özel Nitelikli kişisel veriler kişinin açık rızası ile işlenebilir. Bunun haricinde sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî 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.

Yukarıda belirtilen şartların olması durumunda ve veri sorumlusu veya veri işleyen tarafından KVK Kurumu tarafından önerilen önlemlerin alınması halinde özel nitelikli kişisel veriler veri üçüncü kişilere aktarılabilir.

Özel nitelikli verilerin yurtdışına aktarılması durumunda veri sorumlusu veya veri işleyen durumunda olan üçüncü taraftan KVK Kurumu tarafından önerilen yazılı taahhütname alınarak ve gerektiğinde ek önlemler de talep edilerek paylaşılabilir.

7. ÜÇÜNCÜ KİŞİLERDEN KİŞİSEL VERİLERİN ALINMASI

Üçüncü kişilerden kişisel verilerin alınması durumunda HİB verilerin hukuka uygun bir şekilde alındığını ve aktarıma ilişkin şartların sağlandığına ilişkin veri aldığı üçüncü kişiden gerekli taahhütleri alır. HİB almış olduğu veriler ile ilgili olarak gerekli her türlü teknik ve idari tedbirleri alır. Bu verilere ilişkin herhangi bir veri sızıntısı durumu söz konusu olduğu takdirde verilerin alındığı üçüncü kişiyi, KVK Kurumunu ve bilgisi olduğu takdirde ilgili kişileri derhal bilgilendirir.

8. KİŞİSEL VERİ KATEGORİLERİ

Kişisel Veri kategorisi	Açıklama
Kimlik Bilgisi	
İletişim Bilgisi	
Lokasyon Bilgisi	
Aile Bireyleri ve Yakınları Bilgisi	
Finansal Veri	
Banka Bilgileri	
Eğitim Verisi	
Bina Güvenliği Verisi	
Görüntü/Ses Verisi	
Adli Sicil Verisi	
Biyometrik Veri	

Kişilik ve Yetenek Verisi	
Özlük Verisi	
Performans Verisi	
Seyahat Verisi	
Şikâyet/Başvuru Verisi	
Yurtdışı Belge Verisi	
İmza Verisi	

Aşağıda bulunan veri sahibi gruplarının kişisel verileri HİB tarafından kaydedilmektedir.

Veri Sahibi	Açıklama
HİB Çalışanı	
Çalışan Adayı	
Stajyer	
Tedarikçi Çalışanı	
Tedarikçi Yetkilisi	
Eğitim, Ticaret Heyeti, Fuar ,Etkinlik Katılımcısı	
Mal/Hizmet Alınan Kişi	
Üye Firma Çalışanı/Yetkilisi	

9. BİNA GÜVENLİĞİ

HİB'in şu anda kullanmakta olduğu bina, Türkiye İhracatçılar Meclisi, Hizmet İhracatçıları Birliği, İstanbul Tekstil ve Konfeksiyon İhracatçı Birlikleri, İstanbul İhracatçı Birlikleri ve İstanbul Maden ve Metaller İhracatçı Birlikleri tarafından ortak olarak kullanılmaktadır. Bu nedenle bina yönetimi her birlikten ve TİM'den iki başkanın yer aldığı bir yönetim tarafından ortak olarak yapılmaktadır ve TİM'in koordinasyonunda yürütülmektedir. TİM bina güvenliğine ilişkin önlemleri ilgili mevzuata ve Kişisel Verileri Koruma Kanuna uygun olarak alır.

Bina güvenliğinin sağlanması için fiziksel güvenlik haricinde, binada güvenlik kameraları bulunmaktadır, bina girişlerinde X-Ray ile tarama yapılmaktadır. HİB'e gelen ziyaretçilerin ve araçların kayıtları alınmaktadır. Bütün bu faaliyetler bina yönetimi tarafından ortak alınan kararlar ile TİM koordinesinde yürütülür. TİM gerekli kararları

Bina güvenliğine ilişkin önlemler kapsamında HİB aşağıdaki prensiplere uymaktadır.

1. Güvenlik Kamerası Kayıtları

HİB'in hizmet verdiği binalarda güvenliğin sağlanması, HİB'in, HİB çalışanlarının ve diğer üçüncü kişilerin menfaatlerinin korunması için kamera ile görüntü kaydı yapılmaktadır.

HİB yalnızca kendi kullandığı katlar ve ortak alanlara ilişkin güvenlik kamerası kayıtlarına erişir ve yalnızca bu kameralarda yer alan görüntüleri işler ve değerlendirir. HİB'in kullanmakta olduğu katlarda yer alan kameralara ilişkin görüntü kayıtlarına diğer Birlikler ve TİM erişmez, bu verileri işlemez ve değerlendirmez.

1. Kamera ile Kaydın Yasal Dayanağı, Amacı,

HİB tarafından yürütülen kamera ile kayıt, Özel Güvenlik Hizmetlerine Dair Kanun ve ilgili mevzuat doğrultusunda yapılmaktadır. Bu güvenlik hizmeti KVKK açısından HİB'in meşru menfaatleri kapsamında değerlendirilmektedir. Bina girişinde konuya ilişkin bilgilendirme mesajı bulundurulmaktadır.

2. Kamera Görüntüsü Verilerinin Güvenliğinin Sağlanması

Kamera görüntülerinin korunmasına ilişkin HİB her türlü teknik ve idari tedbiri alır, güvenlik hizmeti aldığı firmaların her türlü teknik ve idari tedbiri alacağına ilişkin taahhütname alır. Bu teknik ve idari tedbirlere dikkat edilmesinin sağlanması için güvenlik hizmeti veren firma ve bu firma veya firmaların personellerini denetler.

3. Kamera Görüntülerine Erişim ve Görüntülerin Paylaşımı

Herhangi bir olayın vukuu durumunda güvenlik personeli aynı gün içerisindeki kayıtları inceleyebilir, ancak kopyalayamaz, başka bir yere aktaramaz. Bu erişime ilişkin log kayıtları ve inceleme gerekçesini içeren tutanak tutulur.

Geçmiş kamera kayıtlarına erişim sadece bu verileri incelemek üzere yetkilendirilmiş sınırlı sayıda personel tarafından yapılır.

Kamera kayıtları üçüncü kişilerle ancak verilerin incelenebilmesi için gerekli olduğu takdirde paylaşılır. Yargı mercileri tarafından talep edilmesi halinde hakim veya mahkeme kararı ile veya acil durumlarda savcılık yazısı ile kamera kayıtları adli birimlerle paylaşılır.

HİB'in kendi kullandığı katlardaki kayıtlar diğer Birlikler veya Türkiye İhracatçılar Meclisi tarafından alınamaz, güvenlik firmasından doğrudan talep edilemez. Böyle bir ihtiyaç durumunda ilgili Birlik veya TİM konuya ilişkin HİB'e hukuki gerekçesini belirterek yazılı olarak başvurur. HİB bu gerekçeye dayalı olarak yukarıda belirtilen usul ile kayıtları ister.

4. Kamera Görüntülerinin Saklanma Süresi

Kamera kayıtları 2 ayı geçmemek üzere, Başkanlar Kurulunun kararı ve Genel Sekreterin onayı ile belirlenen süre kadar tutulur. Bu süre sonunda söz konusu görüntü kayıtları bir daha geri döndürülemez bir surette silinir.

2. XRay

Ana girişte yer alan X-Ray cihazı ile bina güvenliğinin sağlanması amacıyla çalışanların, HİB'in hizmet verdiği firmaların çalışanlarının, ziyaretçilerin ve diğer üçüncü kişilerin çantaları X-Ray taramasından geçirilir.

X-Ray kayıtlarını aynı gün içerisinde güvenlik personeli değerlendirebilir. Daha önceki kayıtlara erişime bina yönetimi tarafından oy birliği ile karar verilir.

3. Ziyaretçi Kayıtları

Binanın güvenliğinin sağlanması, ISO 27001 kapsamında belirlenen siber güvenlik politikaları ve kişisel verilerin korunması politikası kapsamında HİB binasına girişte gelen ziyaretçilerin giriş ve çıkışlarının takip edilmesi için ziyaretçi kayıtları tutulur. Misafir giriş çıkışına ilişkin veriler yalnızca bu amaçla kaydedilir ve işlenir.

4. Araç Girişleri

HİB personeli ve ziyaretçilerine ait araçların giriş çıkışları plaka tanıma sistemi vasıtasıyla kaydedilmektedir.

HİB personeli kendi araçlarının Dış Ticaret Kompleksine giriş çıkışı için ruhsat fotokopisi ile bina yönetimine başvurur. Söz konusu aracın plakası araç giriş çıkışları için tutulan plaka tanıma sistemine kaydedilir.

Herhangi bir ihtiyaç durumunda, HİB yönetim kurulunda görevli en az iki üye ve Genel Sekreterin imzası ile geçmiş araç girişlerine ilişkin kayıtlar bina güvenliğinden sorumlu güvenlik firmasından yazılı olarak talep edilebilir. Bu kayıtlara yalnızca sınırlı sayıda yetkilendirilmiş personel ulaşabilir. Bütün erişimlerin log kayıtları tutulur.

5. Ziyaretçiler İçin İnternet Erişimi Kayıtları

5651 sayılı kanun kapsamında HİB ziyaretçiler için sağladığı internet hizmeti açısından toplu kullanım sağlayıcısı durumundadır. Kanun ve ilgili yönetmelikte belirtilen toplu

kullanım sağlayıcının yükümlülükleri doğrultusunda ziyaretçi olarak internet erişimini kullanan kişilerin verileri kaydedilmektedir.

HİB ziyaretçilere internet hizmeti sunarken kısa mesaj servisi (sms) ve benzeri yöntemlerle kullanıcıları tanımlayacak sistemleri kurar.

6. Personel Takip Sistemleri

Personelin giriş çıkışları HİB'in meşru menfaatleri kapsamında takip edilmektedir. Bu takip iki yöntemle yapılmaktadır.

1. Kartlı Geçiş Sistemi

HİB kurum çalışanlarına sürekli ve gelen ziyaretçilere geçici akıllı kart verilmektedir. Bu kartlar ile yapılan geçişler kayıt altına alınmaktadır.

2. Parmak İzi Geçiş Sistemi

Personel giriş çıkış saatlerinin belirlenmesi, bina güvenliğinin etkin şekilde sağlanabilmesi, personelin performansını ve bina içinde fiziksel mekanlara erişiminin etkin şekilde düzenlenebilmesi için personelin parmak izi verileri geçiş sistemlerinde kullanılır.

Personelin parmak izi verileri, parmak izi sistemini kuran firma dahil olmak üzere hiçbir şekilde üçüncü kişilerle paylaşılmaz. Ayrılan personelin geçiş izinleri iptal edilir. Ancak geçmiş kapı geçiş log kayıtları 2 yıl süre ile tutulur.

7. YEMEKHANE

Yemekhane hizmeti Bina Yönetimi tarafından TİM'in koordinasyonu ile hizmet alımı yolu ile verilmektedir. Bu kapsamda çalışan ve ziyaretçilerin verileri yalnızca bu sözleşme kapsamında hizmetin verilmesi için ve kanuni olarak gerekli süre kadar kaydedilmektedir.

10. TELEFON SANTRALİ

HİB çalışanlarına ve yöneticilerine, telefon santrali üzerinden yapılan aramaların içeriği gerekli aydınlatma bildirimini ile açıklama sonrasında kayıt altına alınmaktadır. Bu kayıtlar HİB'in hizmet kalitesinin artırılması; HİB çalışanlarının haklarının korunması; üye firmaların taleplerinin ve beyanlarının kaydedilmesi, işlenmesi ve en doğru şekilde değerlendirilmesi amacı ile yapılmaktadır.

Yargı makamları tarafından talep edilmesi halinde bu veriler yargı makamları ile kanun çerçevesinde paylaşılacaktır. Bu durumda ilgili kişiler yargı makamının talebi konusunda bilgilendirilir.

Telefon kayıtları üzerinde yapılan bütün işlemlere ilişkin log kayıtları tutulur. HİB haricinde telefon santralının ortak kullanıldığı diğer ihracatçı birlikleri ve Türkiye İhracatçı Meclisi çalışanları ve yetkilileri, santral hizmeti satın alınmakta ise bu hizmeti veren kurumun yetkilileri, HİB'e yapılan aramalara ilişkin telefon görüşmesi kayıtlarını, HİB'in talimatı haricinde görüntüleyemez, dinleyemez, kaydedemez, kopyalayamaz, silemez veya paylaşamaz.

Telefon santrali hizmetinin en kaliteli ve güvenli şekilde verilebilmesi için HİB gerekli teknik ve idari tedbirleri alır.

11. İNTERNET SİTELERİ

HİB ve alt ihracatçı birliklerine ait olan internet siteleri için 5651 sayılı kanun kapsamında tutulması gerekli olan IP bilgileri tutulmaktadır. Bu IP bilgileri haricinde, web sitesi tasarımlarının etkin olarak yapılabilmesi, internet sitesi tasarımlarının ve içeriklerinin daha iyi hizmet verecek şekilde yapılabilmesi ve internet sitesine giren kullanıcıların siteden en etkin şekilde faydalanabilmesi için çerezler kullanılabilir. Bu kişisel veriler alınırken gerekli bildirimler yapılmaktadır.

İnternet siteleri üzerinden kişisel verilerin alındığı durumlarda,

- Kişisel verinin alınması amacı,
- Kişisel verilerin alınmasının hukuki gerekçesi,
- Kişisel verilerin kayıt edilme süresi,

kişisel verisi alınan ilgili kişiye bildirilir.

Açık rıza alındığı durumlarda, açık rıza gerekli aydınlatma bildirimini yapılarak alınır ve açık rıza kayıtları tutulur.

12. KİŞİSEL VERİLERİN KAYIT SÜRESİ ANONİMLEŞTİRİLMESİ-SİLİNMESİ

Türk Ceza Kanununun 138. Maddesi ve 6698 sayılı Kişisel Verileri Koruma Kanununun 7. maddesi gereği kişisel veriler ilgili kanun hükümlerine uygun işlenmesine rağmen, veri işlemeye ilişkin sebeplerin ortadan kalkması halinde HİB'in karar ile veya kişisel veri sahibinin bu yönde bir talebi olması durumunda bir daha geri getirilemeyecek şekilde silinir, imha edilir veya anonim hale getirilir. Verilerin saklanma süreleri ilgili mevzuata ve HİB'in ihtiyaçlarına göre belirlenir.

Silinme, imha etme veya anonimleştirme işlemleri için Kişisel Verileri Koruma Kurumunun bu konularla ilgili aldığı kararlar ve öneriler dikkate alınır. ISO 27001 kapsamında konuya ilişkin prosedürlere uyulur. Teknolojinin izin verdiği en uygun çözüm, HİB'in ihtiyaçları ve imkanları dikkate alınarak uygulanır.

1. KİŞİSEL VERİLERİN KAYDEDİLME SÜRESİ

HİB işlemekte olduğu kişisel verileri, bu verilerin alınması amacı ile ilgili mevzuata bağlı olarak kaydetmesi gerektiği süre kadar kaydeder ve sonrasında imha eder veya anonimleştirir. HİB kendisine kanunla verilen görevler kapsamında aldığı ve kaydettiği kişisel veriler hususunda ilgili Bakanlığın görüşleri doğrultusunda kayıt süresini belirler.

Kamu kurum ve kuruluşlarında bulunan evrakların arşivlerde muhafazasına, bunlardan muhafazasına lüzum görülmeyenlerin ayklanmasına ve imhasına dair usul ve esaslar 16/05/1998 tarihli ve 19816 sayılı Resmi Gazete'de yayımlanan yürürlüğe giren "Devlet Arşiv Hizmetleri Hakkında Yönetmelik'te" belirlenmiş olup, anılan Yönetmelik'in "ayıklama ve imha" ile ilgili hükümleri Devlet Arşivleri Genel Müdürlüğü'nün internet adresinde yer alan "Ayıklama ve İmha Komisyonları Çalışma Rehberi'nde" açıklanmıştır. Strateji Geliştirme Dairesi Başkanlığı'ndan ilgili Bakanlığa (Ekonomi Bakanlığı) gönderilen 06/05/2015 tarihli ve 27467 sayılı yazı eki Standart Dosya Planı Kitapçığının 91 nci sayfasında da Dahilde İşleme Rejimi ile ilgili evrakların on beş yıl muhafaza edileceği tespit edilmiştir. Bu nedenle ilgili Bakanlıkla paylaşılan söz konusu evraklarda yer alan kişisel veriler on beş yıl muhafaza edilmektedir.

İşlem güvenliği başlığı altında 5651 log kayıtları, İnternet Toplu Kullanım Sağlayıcılar Hakkında Yönetmeliğin 4.Maddesinin b fıkrası kapsamında 2 sene kaydedilmektedir.

Fiziksel güvenlik için tutulan kamera kayıtları 1 ay süreyle kaydedilmektedir. Ziyaretçi kayıtları ise 2 sene süre ile kaydedilmektedir.

Çalışanların parmak izlerine dair olan veriler çalışanın ilişkisini kesmesi ile silinir. Ancak log kayıtları bilgisi 2 sene süreyle kaydedilecektir.

Görsel ve işitsel verilere ilişkin kayıtlar, arşiv değeri bulunan eğitim vb konular hariç olmak üzere 5 sene süreyle kaydedilecektir.

HİB'in verdiği hizmetler kapsamında veya yapmış olduğu sözleşmeler doğrultusunda kaydedilen diğer kişisel veriler Borçlar Kanunu azami zaman aşımı süresi olan 10 sene boyunca kayıt altına alınacaktır.

2. ANONİMLEŞTİRİLMESİ

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya alıcı grupları tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

HİB, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri alır. Kişisel verilerin anonim hale getirilmesi, Kişisel Verilerin Silinmesi Yok edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelikte belirtilen esaslara ve KVK Kurumunun konuya ilişkin yayınladığı rehberdeki yöntemlere uygun olarak yapılır.

3. KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

HİB, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri alır.

Verilerin silinmesi ile ilgili aşağıdaki yöntemler kullanılır.

1. Hizmet Olarak Uygulama Türü Bulut Çözümleri

Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

2. Kağıt Ortamında Bulunan Kişisel Veriler

Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılar görünemez hale getirilmesi şeklinde yapılır.

3. Merkezi Sunucuda Yer Alan Ofis Dosyaları

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmelidir.

4. Taşınabilir Medyada Bulunan Kişisel Veriler

Taşınabilir medyalarda gizli seviyede hiçbir veri taşınmamaktadır. Taşınabilir ortamda olan kişisel veriler, söz konusu donanıma uygun yazılımlar ile silinmelidir.

5. Veri Tabanları

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

4. KİŞİSEL VERİLERİN İMHA EDİLMESİ

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. HİB, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri alır.

1. Yerel Sistemler

Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir

- **De-manyetize Etme:** Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir
- **Fiziksel Yok Etme:** Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücünden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.
- **Üzerine Yazma:** Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır

2. Çevresel Sistemler

Ortam türüne bağlı olarak kullanılacak yok etme yöntemleri aşağıda yer almaktadır:

- **Ağ cihazları (switch, router vb.):** Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- **Flash tabanlı ortamlar:** Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- **Manyetik bant:** Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

- **Manyetik disk gibi üniteler:** Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatis parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.
- **Mobil telefonlar (Sim kart ve sabit hafıza alanları):** Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- **Optik diskler:** CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.
- **Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:** Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre 12.4.1.'de belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.
- **Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:** Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. 12.4.1.'de belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

3. Kağıt ve Mikrofiş Ortamlar

Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılabilir boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir. Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir

4. Bulut Sistemler

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılabilir hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

13. KİŞİSEL VERİ SAHİBİNİN HAKLARI VE BU HAKLARIN KULLANILMASI

Kanunun 11. maddesi çerçevesinde ilgili kişi HİB'e başvurarak kendisi ile ilgili;

- Kişisel verilerinin işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

- Kişisel verilerinin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- Kişisel verilerin silinmesini veya yok edilmesini isteme,
- Kişisel verilerin düzeltilmesi, silinmesi veya yok edilmesine ilişkin işlemlerin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir.

Kişisel veri sahipleri yukarıda sıralanan haklarını kullanmak için kimliklerini tespit edilebildiği bilgi ve belgelerle ve kurum internet adresinde yer alan formu doldurarak, form üzerinde belirtilen yöntemlerle (KEP, Islak İmzalı Bizzat Başvuru, Islak İmzalı Posta Yolu ile Başvuru, E-imzalı doküman içeren e-posta yolu ile başvuru) HİB'e taleplerini iletebilirler.

KVKK'nın 28.Maddesi gereğince aşağıdaki hallerde kişisel veri sahipleri yukarıda sayılan haklarını iddia edemezler.

- Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarî faaliyetler kapsamında işlenmesi.
- Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

KVKK'nın 28. Maddesi 2. fıkrası gereğince veri sahipleri zararın giderilmesi hariç yukarıda belirtilen haklarını iddia edemezler.

- Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- Kişisel veri işleminin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

- Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması

HİB veri sahipleri tarafından yapılan taleplere 30 gün içerisinde cevap verir. HİB yapılan talebi, hukuki gerekçesini açıklayarak reddedebilir.

14. VERİ SORUMLUSU İRTİBAT KİŞİSİ, VERİ KORUMA GÖREVLİSİ

HİB, KVK Kurumu ile irtibatın kurulması ve kurum içerisinde kişisel verilerin korunması konusunda koordinasyonu sağlamak üzere yeterli sayıda personel görevlendirir. Veri Sorumluları Sicili Hakkında Yönetmeliğin 11. Maddesi kapsamında “İrtibat Kişisi” olarak atanan kişi veya kişiler veri sorumlusu (HİB) ile ilgili kişi veya Kişisel Verileri Koruma Kurumu arasındaki iletişimin sağlanmasından sorumludur. 6698 sayılı Kanun kapsamındaki yükümlülük ve yaptırımlar açısından sorumluluk irtibat kişisinde değil bu tüzel kişiyi temsil ve ilzama yetkili organ üzerindedir. İrtibat kişisi olarak yapılan görevlendirme, Kanun hükümleri uyarınca veri sorumlusunun (HİB'in) sorumluluğunu ortadan kaldırmaz.

Veri Koruma Görevlisi (Data Protection Officer) olarak atanan personelin görevleri GDPR Madde 39 kapsamında şunlardır:

- Veri Sorumlusuna GDPR ve KVKK ile ilgili yükümlülükleri hakkında danışmanlık vermek
- HİB KVKK ve GDPR uyumluluğunu izlemek
- Kişisel Verileri Koruma Kurumu ve bu kurumun yurtdışı muadilleri ile gerektiği takdirde irtibatı sağlamak
- Kişisel verilerin sahibi durumunda olan ilgili kişiler için kurumun irtibat noktası olarak görev yapmak, Veri Sorumlusunun veri işleme faaliyetlerine ilişkin veri sahibi ilgili kişilerin taleplerini işleme almak, değerlendirmek ve cevaplandırmak

Veri Koruma Görevlisi bu görevlerini yerine getirebilmek için danışmanlık ve destek talep edebilir.

HİB'de yer alan şube ve birimlerin her birinde gerekli koordinasyonun sağlanması ve kişisel verilerin korunması kapsamında Veri Koruma Görevlisi kişilerle irtibat kurmak üzere görevlendirilen en az bir personel bulunur.

15. KİŞİSEL VERİ KORUMA ETKİ DEĞERLEMESİ

Kişisel verilere ilişkin, GDPR kapsamında zorunlu olan Kişisel Veri Koruma Etki Değerlemesi dokümanı, HİB Veri Envanteri programı ile İngilizce içerikle hazırlanır. Bu durum özellikle HİB'in AB üyesi, EEA bölgesi ülke vatandaşı olan kişilerin verilerine ilişkin olarak hazırlanır.

HİB, aşağıdakilerden herhangi birini gerçekleştirmeden önce veri işlemenin, EEA kişisel verilerinin korunması üzerindeki etkisini değerlendirir:

- veri sahibi için yasal sonuçlar doğuran veya benzer etkilere sahip olan otomatik veri kullanımı (profil belirleme dahil) temelinde veri sahibi ile ilgili sistematik ve kapsamlı değerlendirme
- büyük ölçekli veri kullanımı veya özel kişisel veri kategorileri veya cezai hüküm veya diğer suçlar ile ilgili kişisel verilerin kullanılması
- kamuya açık bir alanın büyük ölçekli ve sistematik bir şekilde izlenmesi
- doğası, kapsamı, bağlamı ve amacı göz önünde bulundurarak yeni teknolojilerin kullanıldığı durumlarda kişilerin hak ve özgürlükleri için yüksek risk oluşturabilecek kişisel veri kullanım alanları.

HİB, (asgari olarak) aşağıdakileri içermesi gereken veri koruma etki değerlendirmesi ile ilgili olarak Veri Koruma Görevlisi'nin (DPO) tavsiyelerine başvurur:

- veri işlemenin sistematik tanımı ve kontrol eden tarafça gözetilen tüm meşru menfaatler dahil olmak üzere kullanımın amacı
- veri işlemenin amacını baz alarak gerekli ve ölçülü olup olmadığının değerlendirilmesi
- veri sahiplerinin hak ve özgürlüklerine yönelik riskin değerlendirilmesi
- riske yönelik önlemler

Veri Koruma Etki Değerlemesi'ne göre veri işlemenin veri sahiplerine yönelik yüksek bir risk oluşturması halinde HİB kendisinden beklenen yükümlülükleri yerine getirecektir.

16. VERİ SIZINTISI DURUMUNDA ALINACAK TEDBİRLER

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, HİB bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

17. EĞİTİM

Bütün personel ve yöneticilerin, kişisel verilerin korunması konusunda bilinçlendirilmesi ve HİB'in kurumsal olarak ilgili kanun ve düzenlemelere uygun faaliyetlerde bulunmasının sağlanması için düzenli eğitimler düzenlenecektir.