BMMYK'nın İlgi Alanındaki Kişilere ait Kişisel Verilerin Korunmasına ilişkin POLİTİKA

1

GENEL HÜKÜMLER

1.1 AMAÇ

Bu Politika BMMYK'nin ilgi alanındaki kişilerin kişisel verilerinin işlenmesiyle ilgili kuralları ve ilkeleri ortaya koymaktadır. Amacı BMMYK'nin, 1990 yılı Birleşmiş Milletler Genel Kurulunun *Bilgisayara İşlenmiş Kişisel Veri Dosyalarının Düzenlenmesine ilişkin Kılavuz İlkelerine*[1] ve kişisel verilerin ve bireylerin mahremiyetinin korunmasına yönelik diğer uluslararası belgelere uygun şekilde kişisel verileri işlemesini sağlamaktır. Politikayı, uygulama, denetim ve hesap verebilirliğe ilişkin rehber olacak Operasyon İlkeleri tamamlayacaktır.

1.2 GEREKÇE

1.2.1 Uluslararası koruma ve çözüm yetkisi uyarınca ve Devletlere ayrıca iyi niyetini sunmak suretiyle, BMMYK'nin genellikle Kurumun ilgi alanına giren kişilerin kişisel verilerini işlemesi gerekmektedir. Bu durum kişisel verilerin Uygulayıcı Ortaklarla ve/veya üçüncü taraflarla paylaşılması gerekliliğini de içerebilir. Kişisel verilerin işlenmesinde kaza eseri ya da izinsiz kayıp ya da ifşa gibi doğal riskler mevcuttur. Özellikle, BMMYK'nin ilgi alanındaki kişilerin hassas durumu göz önüne alındığında, kişisel verilerinin yapısı genellikle hassastır ve bu sebeple bu Politika doğrultusunda dikkatle ele alınmalıdır. Bu yüzden, BMMYK için ilgi alanındaki kişilerin kişisel verilerinin uygun şekilde korunması oldukça önemlidir ve Kurumun veri koruma ilkelerine uyacak şekilde bu verileri işleme sorumluluğu vardır.[2]

1.2.2 Bu Politika BM Personel Yönetmeliği 1.2 (i) hükümlerini ve BMMYK Tüzüğündeki taahhütleri, özellikle de personelden erişimi olduğu bilgileri korumasını ve sorumlu bir şekilde kullanmasını talep eden 6.İlkeyi de tamamlamaktadır.

1.3 KAPSAM

1.3.1 Bu Politika BMMYK'nin ilgi alanındaki kişilerle ilgili olarak BMMYK'nin elinde bulundurduğu tüm kişisel veriler için geçerlidir.[3] Örneğin birleştirilmiş ve isim belirtilmemiş diğer verilerin işlenmesi bu Politikanın kapsamında dahildir, ancak diğer

[1] 14 Aralık 1990 tarihli A/Res/45/95 sayılı Karar tarafından Kabul edilen BM Genel Kurulu Bilgisayara İşlenmiş Kişisel Veri Dosyaları için Kılavuz İlkeleri, şu adreste mevcuttur: http://www.refworld.org/docid/3ddcafaac.html.

[2] Yüksek Komiserlik Programının Yürütme Komitesi şu sonuçlarda yer alan veri koruma ilkelerine atıfta bulunmaktadır: No. 91 (LII) – 2001 (f), mevcut olduğu Internet sitesi: http://www.unhcr.org/3bd3e1d44.html; No. 93 (LIII) – 2002 (b) (viii), mevcut olduğu adres: http://www.unhcr.org/3dafdd344.html; and No. 102 (LVI) – 2005 (v), mevcut olduğu adres: http://www.unhcr.org/43575ce3e.html.

[3] BMMYK, Ekim 2013 tarihli Mülteciler Yüksek Komiseri ve Komiserliğin yetki Alanına ilişkin Not, şu adreste mevcuttur: http://www.refworld.org/docid/5268c9474.html.

hususlarla birlikte, BMMYK'nin Bilgi Sınıflandırma, Kullanma ve İfşa Politikasına dahildir.

1.3.2 Bu Politika; veriler bir BMMYK ofisinde, aynı ya da birden fazla ülkedeki farklı BMMYK ofisleri arasında işlendiği ya da kişisel verilerin Uygulayıcı Ortaklara ya da üçüncü taraflara aktarıldığı durumlarda geçerlidir. Bu Politika kişiler artık BMMYK'nin ilgi alanında olmasalar da uygulanmaya devam edecektir.

1.3.3 Tüm BMMYK personeli bu Politikaya uymak zorundadır.

1.4 TERİMLER VE TANIMLAR

Bu Politikanın amaçları çerçevesinde aşağıda verilen tanımlar uygulanacaktır:

Rıza

Veri sahibi tarafından yazılı ya da sözlü beyan şeklinde ya da net bir onaylayıcı eylemle kişisel verilerinin işlenmesine yönelik özgür ve bilinçli bir uzlaşma göstergesi.

Veri Denetleyicisi

Kişisel verilerin işlenmesine ilişkin yönetimi denetleme ve veri işleme amaçlarını belirleme yetkisine sahip genellikle bir BMMYK ülke ofisinde Temsilci olan BMMYK personeli.

Veri İşleyicisi

Veri denetleyicisi adına kişisel verileri işleyen Uygulayıcı Ortaklar ya da üçüncü taraflar da dahil olmak üzere herhangi bir BMMYK personeli ya da başka bir gerçek kişi ya da kurum.

Veri Koruma Odak Kişisi

İlkesel olarak, bir BMMYK ülke ofisinde ya da operasyonunda, bu Politikaya ilişkin sorumluluklarını yerine getirirken veri denetleyicisine destek olan en kıdemli BMMYK koruma personeli

Veri koruma etki değerlendirmesi

Kişisel veriler işlenirken veri sahipleri üzerindeki koruma etkilerini değerlendirmeye ve bu tür etkilerin asgari düzeye indirilmesi için gerekli iyileştirici faaliyetlerin belirlenmesine yönelik araç ve süreç.

Veri Koruma Görevlisi

Genel Merkezdeki Uluslararası Koruma Bölümünde bu Politikaya uygunluğu denetleyen, izleyen ve bu uygunluğa ilişkin rapor veren bir BMMYK personeli. Veri Koruma Görevlisinin sorumlulukları Bölüm 7.3'te belirtilmektedir.

Veri sahibi

Kişisel verileri işleme tabi olan birey.

Veri aktarım anlaşması

BMMYK ve Uygulayıcı Ortak ya da üçüncü taraf arasında hangi veri bileşenlerinin paylaşılacağı, aktarım biçimi, verilerin nasıl kullanılacağı, veri güvenlik önlemleri ve ilgili diğer hususlar da dahil olmak üzere kişisel verilerin kullanım koşullarına ilişkin şartları belirleyen bir anlaşma.

Uygulayıcı Ortak

BMMYK'nin yetki alanı içerisinde programa dayalı faaliyetlerin uygulanmasını üstlenmeye yönelik proje ortaklık anlaşması ile dahil ettiği BMMYK'den bağımsız ve özerk olarak kurulan bir kurum.

Söz konusu veriden ya da başka bir bilgiden ya da söz konusu veriyle ilgili olarak kullanılması oldukça muhtemel yollarla tanımlanabilen bireyle ilgili her türlü veri. Kişisel veriler bireyin statü ve/veya özel ihtiyaçlarının değerlendirilmesi gibi görüşlere ilişkin ifadelerin yanı sıra isim, cinsiyet, medeni hal, doğum yeri ve tarihi, menşe ülke, iltica ülkesi, birey kayıt numarası, meslek, din ve etnik köken gibi biyografik verileri, fotoğraf, parmak izi, yüz ya da iris görüntüsü gibi biyometrik verileri[4] içermektedir.

Kişisel veri ihlali

Aktarılan, depolanan ya da işlenmiş olan kişisel verilerin kaza eseri ya da yasa dışı/ hukuka aykırı şekilde yok olmasına, kaybolmasına, değiştirilmesine, izinsiz şekilde ifşa edilmesine ya da erişilmesine yol açan veri güvenliğinin ihlali.

[4] Biyometrik veriler depolanmış referans verileriyle karşılaştırma yoluyla bir kişinin kimliğini belirlemek için kullanılabilen kişisel biyolojik (anatomik ya da fizyolojik) ya da davranışsal bir özelliktir.

İlgi alanındaki kişi

Koruma ve destek ihtiyaçları BMMYK'nin ilgi alanı dahilinde olan birey. Mülteciler, sığınmacılar, vatansız kişiler, ülkesinde yerinden edilmiş kişiler ve ülkesine dönenler bu grupta yer almaktadır.

Kişisel verilerin işlenmesi

Toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama ya da değiştirme, geri alma, danışma, kullanım, aktarım (bilgisayarla, sözlü ya da yazılı biçimde), yayma ya da başka şekilde erişilir kılma, düzeltme ya da yok etme dahil olmakla beraber ve bunlarla da sınırlı olmaksızın kişisel veriler üzerinde gerçekleştirilen otomatik olan ya da olmayan her türlü işlem ya da işlemler dizisi.

Üçüncü taraflar

Veri sahibi, BMMYK ya da Uygulayıcı Ortak dışındaki gerçek ve tüzel kişiler. Ulusal hükümetler ya da sivil toplum örgütleri, özel sektörde işletmeler ya da bireyler üçüncü taraflara örnek olarak verilebilir.

2

TEMEL İLKELER

2.1 KİŞİSEL VERİ İŞLEMENİN TEMEL İLKELERİ

BMMYK personeli kişisel verileri işlerken aşağıda yer alan temel ilkelere uymak ve bu ilkeleri uygulamak zorundadır:

(i) Meşru ve adil şekilde veri işleme

(ii) Amacın belirlenmesi

(iii) Gereklilik ve orantılılık

(iv) Doğruluk

(v) Veri sahibinin haklarına saygı

(vi) Gizlilik

(vii) Güvenlik

(viii) Hesap verebilirlik ve denetim

2.2 MEŞRU VE ADİL VERİ İŞLEME

Kişisel verilerin işlenmesi sadece yasal bir temelde, adil ve şeffaf bir şekilde gerçekleştirilebilir. BMMYK, sadece aşağıda belirtilen meşru dayanakların biri ya da daha fazlasını esas alarak kişisel verileri işleyebilir:

(i) Veri sahibinin rızası ile

(ii) Veri sahibinin çıkarına en uygun ve en elzem şekilde

(iii) BMMYK'nin yetkisini uygulamasını sağlamak için

(iv) BMMYK yetkisinin ötesinde, ilgili kişilerin ya da diğer bireylerin emniyetini sağlamak için

2.3 AMACIN BELİRLENMESİ

Kişisel veriler bir ya da birden fazla belirli ve meşru bir amaç için toplanmalıdır ve bu amaçlara aykırı şekilde işlenmemelidir.

2.4 GEREKLİLİK VE ORANTILILIK

Kişisel verilerin işlenmesi gerekli ve işlenme amaçlarıyla orantılı olmalıdır. Bu sebeple, işlenen veriler yeterli ve belirlenen amaçla ilgili olmalı ve bu amacın dışına çıkmamalıdır.

2.5 DOĞRULUK

Kişisel veriler mümkün olduğunca doğru kaydedilmelidir, gerektiği takdirde işlenme amacını yerine getirmek için güncellenmelidir.

2.6 VERİ SAHİBİNİN HAKLARINA SAYGI

Veri sahibinin bilgi, erişim, düzeltme, silme ve itiraz hakları bu Politikanın 3.Bölümünde ele alınmaktadır.

2.7 GİZLİLİK

BMMYK personeli ilgili kişilerin kişisel verilerinin gizliliğini her zaman, veri sahibi artık BMMYK'nin ilgi alanında olmasa bile korumalıdır.

2.8 GÜVENLİK

Kişisel verilerin gizliliğini ve bütünlüğünü sağlamak amacıyla uygun teknik ve organizasyonel veri güvenlik önlemleri uygulanmalıdır. Veri güvenliği ve ilgili diğer hususlar Bölüm 4'te ele alınmaktadır. Kişisel verilerin üçüncü taraflara aktarılması Bölüm 6'da yer alan koşullarla sınırlıdır.

2.9 HESAP VEREBİLİRLİK VE DENETİM

Bu Politika doğrultusunda kişisel verilerin işlenmesi için hesap verebilirliği sağlamak amacıyla BMMYK, Bölüm 7'de belirtildiği üzere bir hesap verebilirlik ve denetim yapısı oluşturacaktır.

3

VERİ SAHİBİNİN HAKLARI

3.1 BİLGİ

BMMYK, veri sahibinden kişisel verileri toplarken, aşağıda yer alan hususlar konusunda, yazılı ya da sözlü veri sahibi tarafından anlaşılacak bir biçimde ve dilde veri sahibini bilgilendirmelidir:

(i) Kişisel verilerin ya da kişisel veri kategorilerinin işlenmesine yönelik belirli amaç(lar);

(ii) Bu tür verilerin Uygulayıcı Ortak(lar)a ya da üçüncü taraflara aktarılıp aktarılmayacağı; verilerin BMMYK adına Uygulayıcı Ortak tarafından toplanması halinde veri sahibinin durumdan haberdar edilmesi;

(iii) Veri sahibinin doğru ve eksiksiz bilgi sağlamasının önemi;

(iv) Veri sahibinin BMMYK'yi ve/veya uygun görüldüğü takdirde Uygulayıcı Ortakları kişisel durumundaki değişiklikler konusunda bilgilendirme görevi;[5]

(v) İstenen kişisel verileri sağlamayı reddetmenin ya da sağlayamamanın tüm sonuçları;

(vi) Veri sahibinin kendi kişisel verilerine erişmeyi, bu bilgileri düzeltme ya da silmeyi talep etme hakkı;

(vii) Veri sahibinin kişisel verilerinin toplanmasına itiraz etme hakkı;

(viii) Veri denetleyicisi ya da Başmüfettişlik hakkında nasıl şikayette bulunacağı.

3.2 ERİŞİM

Talep üzerine veri sahibi aşağıda belirtilenleri BMMYK'den alabilir:

(i) Verilerin kendisiyle ilgili olup olmadığına ya da işlenmiş ya da işlenecek olup olmadığına dair teyit ve

(ii) İşlenen kişisel veriler, bu verilerin işlenme amaçları, verilerin aktarılmış, aktarılıyor ya da aktarılacak olduğu uygulayıcı Ortak(lar) ve/veya üçüncü taraf(lar) hakkında bilgi.

[5] Özellikle doğum, ölüm ya da evlilik gibi şahsi durumlardaki değişiklikler.

3.3 DÜZELTME VE SİLME

3.3.1 Veri sahibi yanlış, eksik, gereksiz ya da haddinden fazla olan kişisel bilgilerinin düzeltilmesini ya da silinmesini talep edebilir.

3.3.2 Veri sahibinin kişisel verilerinin düzeltilmesini ya da silinmesini talep ettiği durumlarda BMMYK söz konusu verilerin yanlışlığına ya da eksikliğine ilişkin kanıt talep edecektir.

3.4 İTİRAZ

Aşağıda yer alan Bölüm 3.7'ye tabi veri sahibi, kişisel durumuyla ilgili meşru dayanaklar olduğu durumda kişisel verilerinin işlenmesine itiraz edebilir. İtiraz haklı bulunduğu takdirde BMMYK ilgili kişisel veriyi işleyemez.

3.5 TALEP YÖNTEMLERİ

3.5.1 Kişisel verilere erişim, bu verilerin düzeltilmesi, silinmesi ya da bu verilere itiraz edilmesi hususlarında veri sahibi ya da yetkili yasal temsilcisi tarafından ya da veri sahibinin çocuk olması durumunda ebeveyni ya da yasal vasisi tarafından bilgi talep edilebilir. Talepler verilerin işlendiği ülkede bulunan BMMYK ofisine sözlü ya da yazılı iletilmelidir.

3.5.2 Herhangi bir talebi ya da itirazı yerine getirmeden önce BMMYK talebi ya da itirazı yapan kişinin kimliğinden emin olmalıdır. Birey kimliğini uygun şekilde belirtmelidir. Yasal temsilci ya da yasal vasi durumunda bu tür bir yasal yetki için kanıt sunulması gereklidir. Ebeveynlerden ya da vasilerden gelen talepler ya da itirazlar çocuğun çıkarına en uygun şekilde değerlendirilmelidir.

3.6 BMMYK TARAFINDAN KAYIT VE YANIT

3.6.1 BMMYK, alınan erişim, düzeltme, silme ya da itiraz taleplerini ve bu taleplerle ilgili olarak Bölüm 3.2, 3.3 ve 3.4'ü müteakiben verdiği yanıtları kaydetmenin yanı sıra Bölüm 3.1.'i müteakiben veri sahibine bilgi verdiğini de kayıt altına alacaktır.

3.6.2 BMMYK talebe ya da itiraza Bölüm 3 çerçevesinde makul bir süre içerisinde yazılı ya da sözlü olarak veri sahibinin ve/veya mevcut olduğu durumda yasal temsilcisinin ya da yasal vasisinin anlayabileceği bir şekilde ve dilde yanıt verecektir.

3.7 SINIRLAMALAR

BMMYK, Veri Koruma Görevlisi ve Merkez Ofisteki diğer ilgili görevlilerle yapılan istişarelere dayanarak, Bölüm 3 kapsamında aşağıdaki hususlarda yanıt vermeyi reddedebilir ya da bir talebe ya da itiraza verilecek yanıtı sınırlandırabilir:

(i) Aşağıda verilen hususlardan biri ya da daha fazlasını koruyacak ya da sağlayacak gerekli ve orantılı bir önlem ortaya konulur:

(a) BMMYK'nin, personelinin ya da Uygulayıcı Ortakların personelinin güvenliği ya da

(b) BMMYK'nin yetkisi kapsamında oldukça önemli operasyonel ihtiyaçları ve öncelikleri.

(ii) Talebin açık bir şekilde kötü, hilekar ya da veri işleme amacını engelleyici olduğunun düşünülmesi için sebepler mevcuttur.

4

BMMYK TARAFINDAN VERİLERİN İŞLENMESİ

4.1 KİŞİSEL VERİLERİN GİZLİLİĞİ

4.1.1 Kişisel veri, tanımı gereği gizli olarak sınıflandırılmaktadır. Kişisel veriler işlenirken BMMYK kişisel verilerin gizliliğine daima saygı göstermelidir.

4.1.2 Gizliliğin sağlanması ve buna saygı duyulması için kişisel veriler sadece yetkili personelin erişebileceği şekilde dosyalanmalı ve depolanmalıdır ve sadece korumalı iletişim araçlarıyla aktarılmalıdır.

4.2 KİŞİSEL VERİLERİN GÜVENLİĞİ

4.2.1 BMMYK kişisel verilerin yapısı ve işlenmesi ile ortaya çıkan risklere, gerekli ekipmanın uygunluğuna ve kalitesine, maliyete ve operasyonel fizibiliteye uygun üst düzey bir veri güvenliği sağlamalı ve uygulamalıdır.

4.2.2 BMMYK'nin veri güvenlik önlemleri kişisel verileri kaza eseri ya da hukuksuz/ gayrı meşru yok edilme, kaybolma, değiştirilme, izinsiz şekilde ifşa edilme ya da erişilme risklerine karşı koruyacaktır.

4.2.3 BMMYK, mevcut teknoloji ve uygulama maliyetini göz önünde bulundurarak veri işlemenin bu Politikanın gerekliliklerini karşılamasını sağlayacak uygun organizasyonel ve teknik önlemleri uygulamalıdır. Bu husus veri işlemcilerinin kişisel verileri daha iyi korumalarını sağlayacak teknoloji ve araçları geliştiren bir veri koruma uygulamasını içermektedir ("tasarlayarak ya da standart olarak gizlilik").

4.2.4 Organizasyonel önlemler aşağıda verilenleri içermektedir:

(i) Standart Çalışma Usulleri oluşturma;

(ii) Veri koruma ve veri güvenliği konularında personel eğitimleri organize etme; ve

(iii) Veri koruma etki değerlendirmelerini yürütme (Bölüm 4.5).

4.2.5 Teknik önlemler aşağıdakileri içermektedir:

(i) Tesislerin, taşınabilir ekipmanların, bireysel dosyaların ve kayıtların fiziki güvenliğinin sağlanması;

(ii) Erişim kontrolü (örneğin, kullanıcı şifresi, kademeli erişim), kullanıcı kontrolü, depolama kontrolü, giriş kontrolü, iletişim ve taşıma kontrolü (örneğin, şifreleme) gibi bilgisayar ve bilgi teknolojileri (IT) güvenliğinin sağlanması.

4.2.6 Kötüleşen ve ciddi kişisel veri ihlali riski ortaya çıkaran güvenlik durumlarında, BMMYK veri sahiplerine zarar gelmesini engellemek amacıyla bu tür kişisel veri ihlallerini önlemek için bireysel dosyaları yerini değiştirerek ya da veri ister kağıt formunda ister bilgisayar ortamında olsun son çare olarak kişisel verileri içeren bu dosyaları yok ederek gerekli tüm önlemleri almalı ve mümkün olan tüm adımları atmalıdır.

4.3 KİŞİSEL VERİLERİN DOĞRULUĞUNUN SAĞLANMASI

4.3.1 BMMYK, sistemlerinde yer alan, yanlış, eksik, gereksiz ya da haddinden fazla olan kişisel verileri düzeltebilir ya da silebilir.

4.3.2 BMMYK, gerektiğinde kişisel verileri güncellemeli ve periyodik olarak teyit etmelidir.

4.3.3 Kişisel veriler BMMYK'nin sistemlerinde düzeltildiğinde ya da bu sistemlerden silindiğinde, BMMYK mümkün olan en elverişli durumda ilgili kişisel verilerin aktarılmış olduğu tüm Uygulayıcı Ortakları ve/veya üçüncü tarafları konuyla ilgili bilgilendirmelidir.

4.4 KİŞİSEL VERİ İHLALİNİN BİLDİRİLMESİ

4.4.1 BMMYK personeli, kişisel veri ihlalinin farkına varır varmaz veri denetçisini bilgilendirmeli ve ihlali uygun şekilde kaydetmelidir.

4.4.2 Kişisel veri ihlali veri sahibinin kişisel olarak zarar görmesi ya da yaralanmasına sebep olabilirse, veri denetçisi veri sahibine söz konusu kişisel veri ihlalini bildirme konusunda elinden geleni yapmalı ve fazla gecikmeden uygun şekilde hafifletici önlemleri almalıdır. Bu tür durumlarda, veri denetçisi ayrıca Veri Koruma Görevlisini de kişisel veri ihlali konusunda haberdar etmelidir.

4.4.3 Bildirim aşağıda verilen hususları tanımlamalıdır:

(i) Veri sahiplerinin kategorileri, sayıları ve ilgili veri kayıtları da dahil olmak üzere kişisel veri ihlallerinin yapısı;

(ii) Kişisel veri ihlallerinin bilinen ve öngörülebilen olumsuz sonuçları;

(iii) Kişisel veri ihlallerinin olası olumsuz etkilerini azaltmak üzere alınan ve önerilen önlemler.

4.5 VERİ KORUMA ETKİ DEĞERLENDİRMELERİ

4.5.1 Yeni sistemler, projeler ya da politikalar hazırlarken ya da uygulayıcı Ortaklarla ya da üçüncü taraflarla, ilgili kişinin kişisel verilerinin korunması üzerinde olumsuz etkisi olabilecek veri anlaşmaları yapmadan önce BMMYK bir Veri Koruma Etki Değerlendirmesi (VKED) yürütmelidir. VKED, kişisel veri işlemenin ya da aktarımının geniş, mükerrer ya da yapısal olduğu durumda (diğer bir deyişle, verilerin belirli bir süre içerisinde Uygulayıcı Ortak ya da üçüncü bir tarafla paylaşıldığı durumda) gereklidir.

4.5.2 VKED tasarlanan sisteme, projeye, politikaya ya da kişisel verilerin işlenmesini içeren veri paylaşım anlaşmasına ilişkin genel bir tanımı, işlenen kişisel verilerin yapısı ve koşulları nedeniyle veri sahiplerinin haklarına yönelik risklerin analizini, bu Politika ile uygunluğu sağlama için uygulanan ya da önerilen tedbirleri, güvenlik önlemlerini ve diğer önlemleri içerir.

4.5.3 Veri denetçileri gerektiğinde VKED organize etmekten ve VKED'leri yürütmekten sorumludur. Sistem ya da düzenleme kapsamı sebebiyle VKED'in küresel ya da bölgesel düzeydeyürütülmesine karar verilmediği takdirde VKED'ler genellikle ülke düzeyinde gerçekleştirilmektedir. Veri denetçileri kendi sorumlulukları çerçevesinde yürütülen her VKED konusunda Veri Koruma Görevlisini tamamen bilgilendirmeli ve VKED'in bir nüshasını Veri Koruma Görevlisi ile paylaşmalıdır.

4.6 VERİLERİN MUHAFAZA EDİLMESİ

4.6.1 Bireysel dosyalara kaydedilmeyen kişisel veriler toplandığı amaçlar çerçevesinde gereğinden daha uzun bir süre muhafaza edilemez.

4.6.2 Açık ya da kapalı tüm bireysel dosyalar daimi kayıtlar olarak kabul edilir ve bu sebeple BMMYK Arşivlerinin[6] Erişim Politikası doğrultusunda daima muhafaza edilmelidir.

[6] BMMYK'nin Erişim Politikası şu adreste mevcuttur: http://www.unhcr.org/3b03896a4.html.

5

VERİLERİN UYGULAYICI ORTAKLAR TARAFINDAN İŞLENMESİ

5.1 GENEL KOŞUL

Kişisel verilerin toplanmasının ve işlenmesinin Uygulayıcı Ortakların sorumluluklarından biri olduğu durumda, kişisel veriler BMMYK adına toplanmakta ve işlenmektedir. Bu sebeplerden dolayı, Uygulayıcı Ortaklardan bu Politikada yer aldığı üzere (özellikle Bölüm 2, 3 ve 4) kişisel verilerin korunmasına yönelik aynı ya da benzer standartlara ve temel ilkelere saygı göstermesi ve söz konusu bu standartları ve ilkeleri uygulaması beklenmektedir. Bu durum, BMMYK kişisel verileri Uygulayıcı Ortaklara aktarma niyetinde olduğunda ya da Uygulayıcı Ortaklar mutabık kalınan faaliyetleri yürütmek amacıyla kişisel verileri topladığında da geçerlidir.

5.2 DOĞRULAMA

BMMYK, ortaklık anlaşmasına bakmaksızın, kişisel verileri bir Uygulayıcı Ortağa aktarmadan ya da Uygulayıcı Ortağı kişisel veri toplama ve işleme işine dahil etmeden önce kişisel verilerin Uygulayıcı Ortak tarafından işlenmesinin bu Politikanın standartlarını ve temel ilkelerini yerine getirdiğini doğrulamalıdır. Bu tür bir doğrulama Veri Koruma Etki Değerlendirmesinin bir parçasını oluşturabilir.

5.3 ORTAKLIK ANLAŞMALARI

BMMYK, Uygulayıcı Ortakların ortaklık anlaşmasını imzalamanın bir parçası olarak taahhüt vererek bu Politikaya uymalarını talep etmelidir. Bu tür anlaşmalar kişisel verilerin işlenmesine yönelik belirli amaçları ve meşru dayanakları da belirtmelidir.

5.4 ORTAĞIN KAPASİTESİ

BMMYK'nin, bu Politikada yer alan veri koruma standartlarına ve ilkelerine uymak amacıyla kapasite oluşturma ve geliştirme konusunda Uygulayıcı Ortaklara destek olması gerekebilir. Böyle bir destek politikaların oluşturulması ya da düzenlenmesi, eğitim verilmesi ya da teknik ve organizasyonel önlemlerin uygulanması ile ilgili olabilir.

5.5 ORTAKLIĞIN SONA ERMESİ

Ortaklık sona erdikten sonra ortaklık sırasında toplanan tüm kişisel veriler BMMYK'ye geri verilecektir. Ortaklık anlaşmaları özellikle meşru sebepler söz konusu olduğunda, diğer bir deyişle veri sahiplerinin rızası olduğunda istisnalar öngörebilir.

6

KİŞİSEL VERİLERİN ÜÇÜNCÜ TARAFLARA AKTARILMASI

6.1 GENEL KOŞULLAR

6.1.1 BMMYK, üçüncü tarafın bu Politika ile aynı ya da benzer bir veri koruma düzeyi sağlaması koşuluyla kişisel verileri üçüncü taraflara aktarabilir.

6.1.2 Üçüncü taraflara yapılan aktarımlardaki potansiyel veri koruma riskleri göz önünde bulundurulduğunda BMMYK bu Politikanın aşağıda verilen temel ilkelerine özellikle dikkat etmelidir:

(i) Aktarım bir ya da daha fazla meşru temele dayanmaktadır;

(ii) Aktarım bir ya da daha fazla belirli ve meşru amaç içindir;

(iii) Aktarılacak kişisel veriler, aktarılma amaçlarına ilişkin olarak yeterli, ilgili, gerekli olmalı ve haddinden fazla olmamalıdır;

(iv) Bölüm 3.7'de yer alan sınırlamalardan bir ya da daha fazlası geçerli değilse, veri sahibi Bölüm 3.1 uyarınca veri toplama sırasında ya da bu işlemi müteakiben kişisel verilerin aktarımına ilişkin olarak bilgilendirilmiştir;

(v) Üçüncü taraf BMMYK tarafından kendilerine aktarılan kişisel verilerin gizliliğine saygı gösterir. BMMYK ve üçüncü taraf arasında bir veri aktarım anlaşması imzalanmış olsun ya da olmasın, BMMYK üçüncü taraftan kişisel verilerin her zaman gizli tutulacağına dair yazılı bir anlaşma istemelidir. Gizliliği sağlamak ve buna uymak için kişisel veriler sadece yetkili personelin erişebileceği şekilde dosyalanmalı ve depolanmalıdır ve sadece korumalı iletişim araçları kullanılarak aktarılmalıdır;

(vi) Üçüncü taraf kaza eseri ya da yasa dışı/gayrı meşru yok etme, kayıp, değiştirme, izinsiz ifşa ya da erişim risklerine karşı kişisel verileri muhafaza eden üst düzey bir veri koruma sağlar.

6.1.3 Ayrıca BMMYK, örneğin BMMYK ile ilgili kişiler arasında güven ortamının kaybolması ya da BMMYK'nin siyasi olmayan, bağımsız ve insani bir kurum olduğu algısının kaybedilmesi gibi sebeplerden ötürü, kişisel veri aktarımının aşağıda belirtilenleri olumsuz etkilememesini sağlamalıdır:

(i) BMMYK personelinin ve/veya Uygulayıcı Ortakların güvenliği; ve/veya

(ii) BMMYK operasyonun etkili bir şekilde işlemesi ya da BMMYK'nin yetkisi konusunda uzlaşılması.

6.1.4 Kişisel verilerin üçüncü bir tarafa aktarılmasını kabul etmeden önce BMMYK üçüncü tarafça sağlanan veri koruma düzeyini değerlendirmelidir. Veri denetçisi, değerlendirmenin bir parçası olarak, diğer hususlara ilaveten, uygulanan teknik ve organizasyonel veri güvenlik araçlarının yanı sıra, uygulanacak yasa ve yönetmelikleri, üçüncü tarafın iç tüzük ve politikalarını, belirli veri koruma çerçevelerine uymaya yönelik sözleşmeye bağlı belirli yükümlülükleri ya da taahhütleri ve bunlara yönelik etkin uygulamayı değerlendirmelidir. Bölüm 4.5 çerçevesinde veri denetçisinin bir VKED yürütmesi gerekebilir.

6.2 VERİ AKTARIM ANLAŞMALARI

6.2.1 Kişisel verilerin üçüncü bir tarafa aktarımından önce, anlaşma yapmamak için geçerli bir sebep yoksa, veri denetçisi, özellikle kişisel verilerin geniş, mükerrer ya da yapısal olduğu durumlarda, diğer bir deyişle aynı tür verilerin belirli bir süre içerisinde aynı üçüncü tarafla aynı amaç çerçevesinde paylaşılması durumunda, bir veri aktarım anlaşması imzalamayı ya da uygun olduğu takdirde daha geniş anlaşmalar içerisine verileri korumaya yönelik maddeler eklemeyi talep etmelidir.

6.2.2 Veri aktarımı diğer hususların yanı sıra;

(i) veri koruma ve uygulanacak veri güvenlik önlemlerinin yanı sıra, veri aktarımının amaçlarını ve aktarılacak belirli veri elemanlarını ele almalı;

(ii) üçüncü tarafların bu Politikaya uygun veri koruma ve veri güvenlik önlemleri almasını talep etmeli ve

(iii) anlaşma süresince veri aktarımının gözetilmesine yönelik danışma, denetim, hesap verebilirlik ve inceleme mekanizmalarını şart koşmalıdır.

6.2.3 Veri Koruma Görevlisi ve Hukuki İşler Servisi tüm veri aktarım anlaşmalarını inceleyecek ve açık hale getirecektir. Veri Koruma Görevlisine nihai anlaşmaların nüshaları ile başvurulmalıdır.

6.3 ULUSAL KOLLUK TEŞKİLATLARINA VE MAHKEMELERE VERİ AKTARIMI

6.3.1 Uygun koşullar altında, BMMYK kişisel verileri ulusal emniyet teşkilatlarına ya da ulusal bir mahkemeye aktarabilir. Bu tür aktarımlar emniyet teşkilatlarının ya da mahkemenin talebi üzerine ya da BMMYK'nin kendi inisiyatifi ile gerçekleşebilir. Veri aktarımları işlendiği iddia edilen bir suça yönelik soruşturmaya tabi ya da bir suçun mağduru/ mağdurları ya da tanığı/tanıkları ile ilgili kişilere ilişkin olabilir.

6.3.2 Kişisel verilerin üçüncü taraflara aktarımıyla ilgili genel koşullara ek olarak (Bölüm 6.1.2 (iv) istisna olmak üzere Bölüm 6.1), BMMYK sadece aşağıdaki koşullar gerçekleştiğinde bu tür bir talebi kabul edebilir ve kişisel verileri ulusal emniyet teşkilatlarına ya da ulusal mahkemelere aktarabilir:

(i) Veri aktarımı ceza gerektiren ciddi bir suçun tespiti, önlenmesi, soruşturulması ya da kovuşturulması amacıyla, özellikle kişinin ya da halkın güvenliğine karşı ciddi ve yakın riskleri engellemek için gereklidir;

(ii) veri aktarım talebinde bulunan emniyet teşkilatı ya da mahkeme söz konusu suçun tespiti, önlenmesi, soruşturulması ya da kovuşturulması konusunda yetkilidir;

(iii) veri aktarımı bu tür amaçların gerçekleştirilmesinde ve kişisel verilerin başka kaynaklardan elde edilemeyeceği durumlarda emniyet teşkilatını ya da mahkemeyi büyük oranda destekler;

(iv) veri aktarımı orantısız şekilde veri sahibinin ya da ilgili kişinin mahremiyet hakkı ya da diğer insan haklarıyla çatışmayacaktır ve

(v) Mağdur ve tanıkların verilerine ilişkin durumlarda aktarım için rızaları alınmış olacaktır.

6.3.3 Kişisel verilerin ulusal emniyet teşkilatlarına ya da ulusal mahkemelere aktarılmasından önce, Uluslararası Koruma Bölümü içerisindeki Koruma ve Ulusal Güvenlik Birimi, Hukuki İşler Servisi ve ilgili Büro(lar) ile istişare ederek Veri Koruma Görevlisinden tavsiye alınmalıdır.

6.4 ULUSLARARASI EMNİYET TEŞKİLATLARI, ULUSLARARASI MAHKEMELER YA DA DİĞER ULUSLARARASI ORGANLAR

Uluslararası Ceza Mahkemesi, özel amaçlı uluslararası ceza mahkemeleri, BM'nin yetkisindeki soruşturma komisyonları ve benzer uluslararası organlar tarafından kişisel verilerin aktarılmasına yönelik talepler Uluslararası Koruma Bölümüne (Veri Koruma Görevlisi, Koruma ve Ulusal Güvenlik Birimi ve uygun olduğu takdirde İnsan Hakları İrtibat Birimi) ve Hukuki İşler Servisine aktarılmalıdır.

6.5 İMTİYAZLAR VE MUAFİYETLER

Kişisel verilerin aktarımı 1946 tarihli *Birleşmiş Milletler İmtiyazlar ve Muafiyetler Sözleşmesi* çerçevesinde BMMYK'nin imtiyazlarına ve muafiyetlerine halel getirmeksizin gerçekleşir ve bunun aksi şekilde yorumlanmamalıdır. BMMYK'nin ve personelinin imtiyazları ve muafiyetleri ülkelerin hükümetleri ile herhangi bir işbirliği anlaşması gözetilmeksizin geçerlidir. İmtiyazlar ve muafiyetlere ilişkin tüm sorular BMMYK'nin Hukuki İşler Servisine iletilmelidir.

7

HESAP VEREBİLİRLİK VE DENETİM

7.1 HESAP VEREBİLİRLİK VE DENETİM YAPISI

Bölüm 2.9'da belirtilen BMMYK'nin hesap verebilirliği ve denetim yapısı aşağıda yer alan anahtar aktörlerden oluşacaktır:

(i) BMMYK Merkez Ofisindeki Uluslararası Koruma Bölümü bünyesinde Veri Koruma Görevlisi,

(ii) Her ülke ofisinde/operasyonda veri denetçileri ve

(iii) Ülke ofislerinde/ operasyonlarda veri koruma odak noktaları.

7.2 VERİ DENETLEYİCİSİ VE VERİ KORUMA ODAK NOKTASI

7.2.1 Veri denetçisi kendi sorumluluk alanı çerçevesinde kişisel verilerin işlenmesinden ve denetlenmesinden sorumludur. Bu sebeple temel sorumluluğu bu Politikaya uygunluğu sağlamaktır. Bu amaçla veri denetleyicisi bir veri koruma odak noktası tayin etmelidir. Veri koruma odak noktası ilke olarak bir ülke ofisindeki/operasyondaki en kıdemli BMMYK koruma personeli olmalıdır.

7.2.2 Veri koruma odak noktası tarafından desteklenen veri denetçisi bu Politikayı diğer hususların yanı sıra, aşağıda verilen şekillerde uygulamalıdır:

(i) Veri işleme için uygulanacak meşru dayanakları ve belirli ve meşru amaçları belirleyerek;

(ii) Üçüncü tarafların veri güvenliğini değerlendirmenin yanı sıra organizasyonel önlemlerin ve güvenlik önlemlerinin uygulanmasını sağlayarak;

(iii) Örneğin Veri Koruma Standart Çalışma Usulleri şeklinde, bu Politikanın özellikle veri sahibinin haklarına saygı gösterilmesiyle ve veri gizliliği ve güvenliğinin sağlanmasını amaçlayan önlemlerle ilgili tüm yönlerini içeren iç usuller oluşturarak;

(iv) Veri koruma ve veri güvenliği hususlarına Uygulayıcı Ortak anlaşmalarında yeterli düzeyde yer vererek;

(v) Üçüncü taraflarla gerektiğinde ya da uygun olduğunda veri aktarım anlaşmaları imzalayarak.

7.2.3 Gerektiğinde, veri denetçisi ve/veya veri koruma odak noktası bu Politikanın uygulanması ve yorumlanmasına ilişkin sorularla ilgili olarak Veri Koruma Görevlisinden tavsiye almalıdır.

7.3 VERİ KORUMA GÖREVLİSİ

7.3.1 BMMYK, görevleri aşağıda verilenleri içerecek olan, BMMYK Merkez Ofisinde Uluslararası Koruma Bölümünde bir Veri Koruma Görevlisi atayacaktır:

(i) Veri koruma ve bu Politika üzerine tavsiye, destek ve eğitim vermek;

(ii) Veri denetçileri ve veri koruma odak noktaları tarafından sağlanan, veri aktarım anlaşmaları, BMMYK tarafından üçüncü taraflara yapılan belirli veri paylaşımı örnekleri, veri koruma etki değerlendirmeleri, veri ihlal bildirimleri ve veri sahipleri tarafından yapılan şikayetleri içeren bilgi envanterleri yürütmek;

(iii) Veri denetçilerini ve ilgili diğer aktörleri bu Politikaya uygunluğu hedefleyen önlemleri alma konusunda aktif şekilde desteklemek;

(iv) Bu Politikaya uygun şekilde izleme ve raporlama yapmak;

(v) Gerektiğinde bu Politika çerçevesinde Hukuk İşleri Servisi ile irtibat kurmak.

7.3.2 Veri Koruma Görevlisi Uluslararası Koruma Bölümü Direktörü aracılığıyla Koruma Yüksek Komiser Yardımcısına yıllık veri koruma raporu iletecektir.

7.4 BAŞMÜFETTİŞLİK

Bu Politika, Başmüfettişliğin gizliliğin ihlali ya da dolandırıcılık gibi iddia edilen görevi kötüye kullanma şikayetlerini alma başta olmak üzere, bu tür görevi kötüye kullanma vakalarına ilişkin soruşturmaları yürütme gibi yetkilendirildiği görevleri etkilemez.[7] Bu şekilde Başmüfettişlik bu Politika tarafından oluşturulan izleme ve uygunluk yapısını tamamlamaktadır.

7.5 ETİK BÜROSU

Etik Bürosu, bu Politikayı desteklemek için etik uygulamalar ve standartlar konusunda rehberlik edecek ve BMMYK'in Davranış Kurallarının ve BMMYK'nin Bireylerin

[7] Başmüfettişliğin görevlerine ve nasıl şikayette bulunulacağına ilişkin bilgiler şu adreste mevcuttur: http://www.unhcr.org/pages/52e11b746.html.

Misillemeye Karşı Korunmasına ilişkin Politikasının ("usulsüzlükleri bildirme politikası") uygulanmasıyla, kişisel verilerin işlenmesine ilişkin risklerin azaltılmasına destek olacaktır.


DIEBOLD