www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt:7 Sayı:2

Geliş:03.09.2025
Kabul:29.12.2025

INTERPOL'ün Veri İşlenmesine İlişkin Kuralları (2024 Yılı Değişiklikleri Dâhil)

Doç. Dr. Enver, KAŞLI
Emniyet Amiri, Ankara Emniyet Müdürlüğü
kaslienver@gmail.com
ORCID ID: 0000-0001-7738-1233

ÖZ

Günümüzde işlenen suçlar kolaylıkla birden fazla ülkeyi olumsuz etkileyebilmektedir. Uluslararası boyutu olan suçlarda başarı, büyük ölçüde uluslararası düzeyde etkin ve sürekli bir iş birliğine bağlıdır. INTERPOL, en büyük uluslararası adli polis işbirliği teşkilatıdır. Teşkilat, ulusal kolluk teşkilatlarının sahip olduğu yakalama, gözaltı, arama gibi operasyonel yetkilere sahip değildir. 7 gün 24 saat kesintisiz çalışan iletişim ağı sayesinde, polis teşkilatları arasında bültenler, difüzyonlar ve veri tabanları aracılığıyla veri değişimi sağlamaktadır. INTERPOL bünyesinde veriler, INTERPOL'ün Veri İşlenmesine İlişkin Kurallarına göre işlenmektedir. Bu Kurallar, Türk hukukunda yeni bir alan olan kişisel verilerin korunması hukukunda kolluk faaliyetleri açısından zorunlu olan veri tabanlarına ilişkin yapılacak düzenlemelere kaynak olabilecek hükümler ihtiva etmektedir. Bu çalışma giriş kısmından ve INTERPOL'ün Veri İşlenmesine İlişkin Kurallarının tercümesinden oluşmaktadır.

Anahtar Sözcükler: INTERPOL, bülten, kırmızı bülten, kişisel veri, veri tabanı.

INTERPOL's Rules on the Processing of Data (Including 2024 Changes)

ABSTRACT

Today crimes can easily negatively impact multiple countries. Success in crimes with an international dimension depends largely on effective and sustained international cooperation. INTERPOL is the largest international police cooperation organization. The organization lacks the operational powers of national law enforcement agencies, such as arrest, detention, and search. Thanks to its 24/7 communication network, it facilitates data exchange between police agencies through bulletins, diffusions and databases. Within INTERPOL, data is processed in accordance with INTERPOL's Rules on the Processing of Data. These Rules contain provisions that could serve as a basis for regulations regarding databases, which are essential for law enforcement activities in personal data protection law, a new area in Turkish law. This study consists of an introduction and a translation of INTERPOL's Rules on the Processing of Data.

Keywords: INTERPOL, notice, red notice, personal data, database.

Atıf Gösterme	Kaşlı, E., (2025). INTERPOL'ün Veri İşlenmesine İlişkin Kuralları (2024 Yılı Değişiklikleri Dâhil), *Kişisel Verileri Koruma Dergisi. 7*(2), 22-107.

GİRİŞ

INTERPOL, Uluslararası Adli Polis Teşkilatını (International Criminal Police Organization) ifade etmek için kullanılan dilimize yerleşmiş bir kısaltmadır. INTERPOL kelimesi, Türkçeye Uluslararası Kriminal Polis Teşkilatı olarak çevirisi yaygın olsa da kriminal ifadesinin Türk hukukundaki karşılığı "adli" kelimesi olduğundan Teşkilat adının Türkçemizde "Uluslararası Adli Polis Teşkilatı" (Teşkilat olarak kısaltılacaktır) olarak kullanılmasının daha uygun olacağı kanaatindeyim.

Günümüzde özellikle ulaşım ve iletişim alanlarında yaşanan gelişmeler, başta terörizm ve örgütlü suçlar olmak üzere hem suç olgusunu hem de suç faillerinin hareket tarzlarını değiştirmiştir. (Kaya, 2009). Artık suç, ulusal bir sorun olmayıp uluslararası kamu düzenini bozmaktadır. Artık suçlular, bulundukları ülkeden başka bir ülkede kolayca suç işleyebilmekte veya suç işlediği yerden kolayca farklı bir ülkeye kaçarak cezadan kurtulmaya çalışmaktadır. Suç dünyasındaki bu gelişmelere karşılık olarak kolluk teşkilatları arasında uluslararası iş birliği bir zorunluluk haline gelmiştir. Uluslararası boyutu olan suçlarda başarı, büyük ölçüde uluslararası düzeyde etkin ve sürekli bir iş birliğine bağlıdır.

Uluslararası kolluk iş birliği, devletler arasında ya da devletlerle uluslararası kuruluşlar arasında imzalanan anlaşmalar çerçevesinde yürütülmekte olup; sınır aşan suçların önlenmesi, suç delillerinin toplanması ve suç faillerinin yakalanması amaçlanmaktadır. INTERPOL, en büyük uluslararası adli polis iş birliği teşkilatıdır. INTERPOL'ün temelleri, 1914 yılında Monako'da 24 ülkenin katılımıyla düzenlenen I. Uluslararası Adli Polis Kongresi'nde atılmıştır. INTERPOL, mevcut kurumsal yapısıyla 1946 yılında fiilen faaliyetlerine başlamıştır. (INTERPOL, 1973). Teşkilatın merkezi Fransa'nın Lyon şehrindedir, 196 üyesi vardır. Resmi dilleri Arapça, İngilizce, Fransızca ve İspanyolcadır.

INTERPOL, uluslararası düzeyde suçların önlenmesi, suçluların yakalanması, tutuklanması ve talep eden ülkeye iade edilene kadar olan süreçteki işlemlerin yürütülmesi amacıyla faaliyet göstermektedir. Teşkilat, dünya genelinde polis teşkilatları arasında bilgi paylaşımı yaparak koordinasyonu sağlamaktadır. Teşkilat, ulusal kolluk teşkilatlarının sahip olduğu yakalama, gözaltı, arama gibi operasyonel yetkilere sahip değildir. 7 gün 24 saat kesintisiz çalışan iletişim ağı sayesinde, polis teşkilatları arasında hızlı, güvenli ve etkin bir iletişim mümkün olmaktadır.

INTERPOL'ün yapısı incelendiğinde Genel Sekreterlik, İcra Komitesi, Genel Sekreterlik, Ulusal Merkez Bürolar ve Dosya Kontrol Komisyonu birimleri bulunmaktadır. INTERPOL'e üye ülkeler tarafından görevlendirilen temsilcilerden oluşan Genel Kurul, teşkilatın en üst düzey organıdır. INTERPOL İcra Komitesi, INTERPOL bünyesinde Genel Kurulun kararlarının uygulanmasını denetleyen Genel Kurulun ardından en üst düzey yürütme organı olarak görev yapmaktadır. Genel Sekreterlik; Teşkilatın günlük faaliyetlerini yürüten daimi organdır. Ulusal Merkez Bürolar, INTERPOL faaliyetlerine katılım gösteren üye ülkelerin kolluk birimleridir. Dosya Kontrol Komisyonu ise kişisel verilerin Teşkilat tarafından işlenmesinin uygunluğunu kontrol eden bağımsız bir birimdir. (David ve Hearn, 2018).

Uluslararası kolluk iş birliğini sağlamak amacıyla INTERPOL, veri tabanları oluşturmakta ve farklı konularda renklere göre kodlanmış bültenler yayımlamaktadır. INTERPOL bünyesinde oluşturulan veri tabanları, üye ülkelere önemli bir kaynak sunmaktadır. Hali hazırda INTERPOL bünyesinde 19 veri tabanı bulunmaktadır. Nominal Veriler kısmında; uluslararası polis iş birliği talebi kapsamında olan kişilerin kimlik bilgileri ve suç geçmişlerine ilişkin kişisel veriler toplanmaktadır. Uluslararası Çocuklara Yönelik Cinsel İstismar Görüntü veri tabanı, mağdurlar, failler ve yerler arasında bağlantılar kurmak için gelişmiş görsel karşılaştırma yazılımı kullanmaktadır. Parmak izi veri tabanında, üye ülkelerdeki yetkili kullanıcılar, Otomatik Parmak İzi Tanımlama Sistemi (AFIS) aracılığıyla parmak izi kayıtlarını görüntüleyebilir, gönderebilir ve çapraz kontrol edebilir. DNA veri tabanı; suçlular, olay yerleri, kayıp kişiler ve kimliği belirsiz cesetlerden elde edilen DNA profillerini içermektedir. I-

Familia'nın amacı, aile DNA eşleştirmesi yoluyla dünya genelindeki kayıp kişilerin kimliklerini belirlemektir. Bu sistem, ailelerin yeniden bir araya gelmesine veya kapanmamış vakaların sonuçlandırılmasına yardımcı olarak hayatların yeniden inşa edilmesini sağlamaktadır. Yüz Tanıma Sistemi veri tabanı; firariler, kayıp kişiler ve şüpheli bireyleri tanımlamak amacıyla görüntülerin saklandığı ve çapraz kontrol edildiği özel bir platform sağlamaktadır. SLTD Veri tabanı (Seyahat ve Kimlik Belgeleri), çalıntı, kayıp, iptal edilmiş, geçersiz veya boş olarak çalınmış seyahat ve kimlik belgelerine dair bilgileri içermektedir. EDISON veri tabanı, sahte belgeleri tespit etmeye yardımcı olmak amacıyla ülkeler ve uluslararası kuruluşlar tarafından düzenlenmiş gerçek seyahat belgelerinin örneklerini, görüntülerini ve güvenlik özelliklerini sunmaktadır. Motorlu Taşıtlar veri tabanı; arabalar, kamyonlar, römorklar, ağır makineler, motosikletler ve tanımlanabilir yedek parçalar gibi çalıntı araçlara dair geniş kapsamlı tanımlayıcı bilgileri içermektedir. Deniz Araçları veri tabanı; çalıntı gemi ve motorların izini sürmek ve takip etmek için merkezi bir araçtır. Sanat Eserleri Veri tabanı, INTERPOL üye ülkeleri ve ICOM (Uluslararası Müzeler Konseyi), UNESCO gibi uluslararası ortaklar tarafından çalıntı olarak bildirilen kültürel objelere ait açıklama ve görselleri içermektedir. INTERPOL Ateşli Silah Referans Tablosu, sınır ötesi soruşturmalarda daha doğru bir tanımlama ve iz sürme amacıyla ateşli silahların standart şekilde tanımlanmasını sağlayan etkileşimli bir çevrimiçi araçtır. INTERPOL Kanuna Aykırı Silah Kayıtları ve Takip Yönetim Sistemi (iARMS), yasadışı, kayıp veya çalıntı silahların uluslararası düzeyde takibini destekleyen tek küresel kolluk platformudur. INTERPOL Balistik Bilgi Ağı (IBIN), dünya çapında tek büyük ölçekli uluslararası balistik veri paylaşım ağıdır. Farklı ülkelerdeki suçlar arasında bağlantı kurmak için merkezi balistik görüntüleme verilerini depolar ve karşılaştırır. Organize Suç Ağları veri tabanları istihbarat toplama ve paylaşımını geliştirmek, soruşturmalara destek sağlamak ve suç ağlarını daha iyi analiz etmektir. (INTERPOL, 2025a).

Yine renk kodlu bültenler; şüpheliler, sanıklar, hükümlüler, BM Güvenlik Konseyi Yaptırımlarına tabi kişiler, potansiyel tehditler, kayıp kişiler, kimliği belirsiz cesetler hakkındaki uluslararası uyarılardır. Bültenler renklerine göre kırmızı bülten, mavi bülten, yeşil bülten, sarı bülten, siyah bülten, turuncu bülten ve mor bültendir.

Bültenler ve difüzyonlar oluşturulurken veri tabanlarında birçok kişisel veri işlenmektedir. INTERPOL bünyesinde kişisel verilerin işlenmesine ilişkin ilk düzenlemeler 1982 yılında yapılmıştır. Bu düzenlemeler, zaman içinde geliştirilerek INTERPOL'ün Veri İşlenmesine İlişkin Kurallar (kısaca Kurallar şeklinde kısaltılacaktır) adlı düzenleme ortaya çıkmış, bu kurallar da en son 2024 yılında değiştirilmiştir. (INTERPOL, 2025b). Görüleceği üzere INTERPOL tarafından tutulan bu veri tabanlarında işlenmiş bir suçla ilişkili olan araç bilgileri, tarihi eser bilgileri, seyahat belgeleri bilgilerinin yanı sıra kişisel veriler de işlenmektedir. Bundan dolayı düzenlemenin başlığında kişisel veri yerine veri şeklinde üst kavram tercih edilmiştir.

Kişisel verilerin korunması, Türkiye'de yeni bir hukuk uygulama alanıdır. Ülkemizde kişisel verilerin korunmasına ilişkin genel bir kanun olan 6698 sayılı Kişisel Verilerin Korunması Kanunu yürürlüktedir. KVKK m.28'de kolluk faaliyetlerine ilişkin dar kapsamlı bir düzenleme bulunmakta, kişisel verilerle ilgili farklı mevzuatlarda dağınık hükümler (örneğin Polis Vazife ve Salahiyet Kanunu m.5'te parmak izleri ve fotoğrafla ilgili düzenlemeler vardır) mevcut olsa da kolluk faaliyetlerine ilişkin özel bir kişisel veri işleme kanunu mevcut değildir. (Kaşlı, 2023). Kolluk faaliyetlerinde kişisel verilerle ilgili yapılacak düzenlemede kolluk tarafından tutulan veri tabanları da düzenlenmelidir. Veri tabanlarının oluşturulması, veri tabanları arasındaki sorgulamalar, veri tabanlarına dahil edilebilecek veriler, verilerin gizlilik düzeyi, veri tabanlarına erişim yapabilecekler, veri tabanları üzerinde yapılan işlemlerin kayıt edilmesi (log kayıtları) bu düzenlemelere yer alması gereken hususlardan bazılarıdır. Kurallar başlıklı bu düzenleme, INTERPOL uygulamasında veri tabanları özelinde birçok konuyu düzenlemektedir. Bu tercüme ülkemizde kolluk faaliyetlerine ilişkin veri tabanlarına ilişkin yapılacak düzenlemelere kaynak olabilecek hükümler ihtiva ettiğinden dolayı, Kuralların İngilizceden Türkçeye tercüme edilmesinin faydalı olabileceği kanaatindeyim.

1. INTERPOL'ÜN VERİ İŞLENMESİNE İLİŞKİN KURALLARI

BAŞLANGIÇ

Uluslararası Adli Polis Teşkilatı – INTERPOL Genel Kurulu,

Teşkilatın Anayasası'nın 2. maddesinin 1. fıkrasını DÜŞÜNEREK,

Anlaşmanın 36. maddesinin 2. fıkrasına uygun olarak INTERPOL Dosyalarının Kontrol Komisyonu ile GÖRÜŞTÜKTEN SONRA,

Anayasa'nın 8(d) maddesine göre Genel Kurul'un INTERPOL Bilgi Sisteminin veri işleme ile ilgili işletme kurallarını belirleme sorumluluğuna sahip olduğunu DİKKATE ALARAK,

AŞAĞIDAKİ KURALLARI KABUL ETMİŞTİR:

Madde 1: Tanımlar

(1) "Adi suç", Anayasanın 3'üncü maddesinin kapsamına girenler ve Genel Kurul tarafından özel kuralları belirlenenler dışında kalan tüm suçları ifade eder.

(2) "Veri", kaynağı ne olursa olsun, adi suçların unsurlarına, bu tür suçların soruşturulmasına ve önlenmesine, suçluların kovuşturulmasına ve suçların cezalandırılmasına ilişkin her türlü bilgi ve kayıp şahıslar ile kimliği belirlenemeyen cesetlere ilişkin her türlü bilgi anlamına gelir.

(3) "Kişisel veri", kimliği belirli bir gerçek kişi veya makul bir şekilde kullanılabilecek araçlarla kimliği belirlenebilecek bir kişiyle ilgili her türlü veri anlamına gelir.

(4) "INTERPOL Bilgi Sistemi", Kuruluş tarafından uluslararası polis iş birliği bağlamında veri işlemek için kullanılan tüm yapılandırılmış maddi kaynaklar ve yazılımlar (veri tabanları, iletişim altyapısı, gelişmiş sensör teknolojisi ve diğer hizmetler) anlamına gelir.

(5) "İşleme", otomatik şekilde olsun veya olmasın, veriler üzerinde gerçekleştirilen toplama, kaydetme, sorgulama, iletme, kullanma, açıklama ve silme gibi herhangi bir işlem veya işlem kümesi anlamına gelir.

(6) "Kaynak", INTERPOL Bilgi Sistemindeki verileri işleyen ve bu verilerden nihai olarak sorumlu olan herhangi bir Ulusal Merkez Büro veya verileri INTERPOL Bilgi Sisteminde işlenen veya Sistemde verilerin adına kaydedildiği ve bu verilerden nihai olarak sorumlu olan herhangi bir uluslararası kuruluş veya özel kuruluş anlamına gelir.

(7) "Ulusal Merkez Büro", Teşkilat Anayasası'nın 32. maddesinde öngörülen irtibat görevlerini yerine getirmek üzere bir ülke tarafından belirlenen herhangi bir kuruluş anlamına gelir.

(8) "Ulusal kuruluş", ülkesinin Ulusal Merkez Bürosu tarafından, bir anlaşma yoluyla ve söz konusu Ulusal Merkez Bürosu tarafından belirlenen sınırlar dahilinde, INTERPOL Bilgi Sisteminde işlenen verileri doğrudan sorgulamak veya bu Kuralların 10. maddesinde listelenen işleme amaçlarından biri veya birkaçı için doğrudan veri sağlamak üzere özel olarak

yetkilendirilmiş, kamu kurumu rolünü yerine getirmek üzere yasal olarak yetkilendirilmiş kuruluş anlamına gelir.

(9) "Uluslararası kuruluş", uluslararası kamu yararı misyonunu yerine getiren, Teşkilat ile veri değişimi konusunda bir anlaşma imzalayan ve Teşkilat tarafından INTERPOL Bilgi Sisteminin bir bölümüne doğrudan veya dolaylı erişim izni verilen herhangi bir uluslararası, hükümetler arası veya hükümet dışı kuruluş anlamına gelir.

(10) "Özel kuruluş", uluslararası kuruluşlar kategorisine girmeyen, veri değişimi ve özellikle INTERPOL Bilgi Sistemindeki verilerin işlenmesi konusunda Teşkilat ile bir anlaşma imzalamış olan, özel hukuka tabi tüzel kişi, şirket, ticari dernek veya kar amacı gütmeyen kuruluş anlamına gelir.

(11) "Uluslararası işbirliği talebi", bir Ulusal Merkez Bürosu, uluslararası bir kuruluş veya Genel Sekreterlik tarafından, INTERPOL Bilgi Sistemi aracılığıyla, Teşkilatın amaç ve faaliyetlerine uygun olarak belirli bir eylemi gerçekleştirmek üzere Teşkilatın bir veya daha fazla Üyesine yardım talebi göndermek için atılan her türlü adım anlamına gelir.

(12) "Uluslararası uyarı", bir Ulusal Merkez Bürosu, uluslararası bir kuruluş veya Genel Sekreterlik tarafından INTERPOL Bilgi Sistemi aracılığıyla, kamu güvenliği, kişilere ve malvarlığına yönelik belirli tehditler hakkında Teşkilatın Üyelerinden birine veya daha fazlasına bildirim göndermek için atılan her türlü adım anlamına gelir.

(13) "Bülten", bir Ulusal Merkez Büro veya uluslararası bir kuruluşun talebi üzerine veya Genel Sekreterliğin girişimiyle Teşkilat tarafından yayımlanan ve Teşkilatın tüm Üyelerine gönderilen uluslararası işbirliği talebi veya uluslararası uyarı anlamına gelir.

(14) "Difüzyon", bir Ulusal Merkez Bürosu veya uluslararası bir kuruluştan gelen, doğrudan bir veya daha fazla Ulusal Merkez Bürosuna veya bir veya daha fazla uluslararası kuruluşa gönderilen ve aynı anda Kuruluşun polis veri tabanında kaydedilen herhangi bir uluslararası işbirliği talebi veya herhangi bir uluslararası uyarı anlamına gelir.

(15) "Mesaj", cezai konularda soruşturma ve kovuşturma yetkisine sahip bir Ulusal Merkez Bürosu veya uluslararası kuruluşun, INTERPOL Bilgi Sistemi aracılığıyla doğrudan bir veya daha fazla Ulusal Merkez Bürosuna veya bir veya daha fazla uluslararası kuruluşa göndermeyi seçtiği, ancak aksi belirtilmediği takdirde, aynı anda Teşkilatın polis veri tabanına kaydetmemeyi seçtiği uluslararası işbirliği talebi, uluslararası uyarı veya herhangi bir veri anlamına gelir.

(16) "Doğrudan erişim", Genel Sekreterliğin yardımı olmaksızın, açıkça yetkilendirilmiş kişiler tarafından otomatik araçlar kullanılarak INTERPOL Bilgi Sistemine veri girilmesi ve bu sistemden veri alınması anlamına gelir.

(17) "Dolaylı erişim", Genel Sekreterliğin yardımıyla INTERPOL Bilgi Sistemine veri girilmesi ve bu sistemden veri alınması anlamına gelir.

(18) "Özellikle hassas veriler", ırk veya etnik kökeni, siyasi görüşleri, dini veya felsefi inançları, sendika üyeliğini, sağlık veya cinsellikle ilgili verileri veya biyometrik verileri ortaya koyan her türlü kişisel veri anlamına gelir.

(19) "Bağlantı", INTERPOL Bilgi Sisteminin bir kısmını başka bir bilgi sisteminin bir kısmına bağlamayı içeren herhangi bir elektronik bağlantı anlamına gelir.

(20) "İndirme", INTERPOL Bilgi Sisteminden başka bir bilgi sistemine veri aktarımını içeren herhangi bir işlem anlamına gelir.

(21) "Yükleme", başka bir bilgi sisteminden INTERPOL Bilgi Sistemine veri aktarımını içeren herhangi bir işlem anlamına gelir.

(22) "Suç analizi", uluslararası polis işbirliği bağlamında gerçekleştirilen veriler arasındaki ilişkinin metodik olarak belirlenmesi anlamına gelir.

(23) "Kişinin statüsü", INTERPOL Bilgi Sisteminde verilerin işlenmesini gerektiren bir olayla bağlantılı olarak bir kişi hakkındaki bilgiler anlamına gelir.

(24) "Olumlu sorgu sonucu", INTERPOL Bilgi Sisteminde kayıtlı veriler ile bu sisteme girilen diğer veriler arasında varsayılan bir eşleşme anlamına gelir.

(25) "Gelişmiş sensör teknolojisi", otomatik veri işleme yoluyla kişilerin ve nesnelerin tanımlanmasını kolaylaştıran ve doğrulama amacıyla insan müdahalesi gerektiren yarı otomatik karar almaya olanak sağlayabilen teknoloji anlamına gelir.

(26) "Büyük veri seti", bir veri kaynağı tarafından Genel Sekreterlik ile paylaşılan, doğrulanmamış veya kategorize edilmemiş ve hacmi veya karmaşıklığı nedeniyle, Genel Sekreterlik tarafından ilk kez işlendiğinde bu Kuralların tüm gerekliliklerine uygun olarak değerlendirilemeyen yapılandırılmış veya yapılandırılmamış veri koleksiyonu anlamına gelir.

(27) "Daimi operasyonel polis veri tabanı", bu Kuralların 29 uncu maddesinde belirtilen şartlara uygun olarak, kullanılan özel veri işleme teknolojisinden bağımsız olarak, Genel Sekreterlik tarafından oluşturulan daimi polis veri tabanını ifade eder.

(28) "Kayıt", bu Kurallarda belirtilen kayıt koşullarına göre bir polis veri tabanına veya suç analiz dosyasına veri veya diğer bilgi öğelerinin eklenmesi anlamına gelir.

(29) "Kamuya açık bilgi", herhangi bir yasal kısıtlamaya tabi olmayan, özel bir yasal statü veya yetki olmaksızın elde edilen ve haber ve medya kaynakları, kitaplar ve dergiler, çevrimiçi materyaller, akademik materyaller, ticari veri tabanları ve kamuoyunun herhangi bir üyesinin kullanımına açık abonelik hizmetleri dahil olan ancak bunlarla sınırlı olmayan bilgi anlamına gelir.

(30) "Biyometrik veriler", parmak izleri, yüz görüntüleri veya DNA profilleri gibi fiziksel, biyolojik, davranışsal veya fizyolojik özelliklerle ilgili olup, bir bireyin kimliğinin belirlenmesini sağlamak veya doğrulamak için belirli teknik işleme tabi tutulmuş kişisel veriler anlamına gelir.

Madde 2: Amaç

Bu Kuralların amacı, INTERPOL kanalları aracılığıyla adli polis makamları arasında uluslararası işbirliğinin etkinliğini ve kalitesini, bu işbirliğinin konusu olan kişilerin temel haklarına gereken saygıyı göstererek, Teşkilat Anayasası'nın 2. maddesi ve bu maddenin atıfta bulunduğu İnsan Hakları Evrensel Beyannamesi'ne uygun olarak sağlamaktır.

Madde 3: Konu

Bu Kurallar, INTERPOL Bilgi Sisteminin işleyişine ilişkin genel ilkeleri, sorumlulukları ve düzenlemeleri belirlemektedir.

Madde 4: Kapsam

(1) Verilerin INTERPOL kanalları aracılığıyla işlenmesi yalnızca INTERPOL Bilgi Sisteminde gerçekleştirilir.

(2) Bu Kurallar, INTERPOL Bilgi Sisteminde gerçekleştirilen tüm veri işleme işlemlerine uygulanır.

(3) Bu Kuralların uygulanabilir hükümleri saklı kalmak üzere, Genel Kurul, Teşkilat Üyelerinin uluslararası adli iş birliği amaçları doğrultusunda verilerin işlenmesine ilişkin kurallara uymayı kabul ettikleri ayrı bir yasal çerçeve benimseyebilir.

BAŞLIK 1:

GENEL İLKELER

BÖLÜM I:

ULUSLARARASI POLİS İŞBİRLİĞİNE İLİŞKİN İLKELER

Madde 5: Verilerin işlenmesine ilişkin yönetişim ilkelerine ve sorumluluklara uyum

(1) INTERPOL kanalları aracılığıyla uluslararası polis işbirliği, Teşkilatın faaliyetlerini düzenleyen temel kurallara, özellikle de Anayasasına uygun olarak gerçekleştirilir.

(2) INTERPOL Bilgi Sistemindeki verilerin işlenmesi, özellikle Anayasanın 2, 3, 26, 31, 32, 36 ve 41'inci maddelerine uygun olarak gerçekleştirilir.

(3) Teşkilatın Üyeleri, Teşkilatın siyasi tarafsızlığı, bağımsızlığı ve yetkisi ile taraf oldukları ulusal mevzuat ve uluslararası sözleşmelere uygun şekilde gözetilerek, uluslararası

polis işbirliği amaçları doğrultusunda azami düzeyde ilgili bilgi alışverişinde bulunmaya çalışırlar.

(4) Ulusal düzeyde, Ulusal Merkez Büroları, INTERPOL Bilgi Sistemindeki verilerin işlenmesi konusunda merkezi bir rol oynayacaktır.

(5) Kaynak, INTERPOL Bilgi Sisteminde işlediği verilerden, bu işleme yöntemi ne olursa olsun ve bu işlemeden doğrudan kaynaklanan sonuçlardan tamamen sorumlu olacak ve verilerin yanlış işlenmesini düzeltmek için uygun önlemleri alacaktır.

(6) INTERPOL, INTERPOL tarafından verilerin yetkisiz veya yanlış kullanımı ve/veya depolanmasından ve bu yetkisiz veya yanlış veri kullanımı ve/veya depolanmasından doğrudan kaynaklanan sonuçlardan tamamen sorumlu olacak ve Teşkilat tarafından verilerin yanlış işlenmesini düzeltmek için uygun önlemleri alacaktır.

(7) INTERPOL Bilgi Sisteminde işlenen verilerin alıcıları, şunlardan tamamen sorumlu olacaktır:

(a) Aldıkları verilere dayanarak ulusal düzeyde yapılan herhangi bir işlemden,

(b) Herhangi bir değişiklik veya silinme hakkında bilgilendirildiklerinde, alınan verilerin ulusal düzeyde derhal güncellenmesini sağlamak için uygun önlemleri almaktan.

Madde 6: INTERPOL Bilgi Sistemine Erişim

(1) Ulusal Merkez Büroları, Anayasa uyarınca görevlerini yerine getirirken Sisteme doğrudan erişim hakkına sahiptir. Bu erişim şunları içerir:

(a) Kuruluşun polis veri tabanlarında doğrudan verilerin kaydedilmesi, güncellenmesi ve silinmesi ve veriler arasında bağlantıların oluşturulması;

(b) her bir veri tabanı için belirlenen özel koşullara ve kaynakları tarafından belirlenen kısıtlamalara ve gizlilik kurallarına tabi olarak Teşkilatın polis veri tabanlarına doğrudan sorgu yapılması;

(c) INTERPOL'ün işbirliği taleplerinin ve uluslararası uyarıların iletilmesine olanak sağlayan bülten ve difüzyonlarının kullanılması;

(d) olumlu sorgu sonuçlarının takip edilmesi;

(e) mesajların iletimi.

(2) INTERPOL Bilgi Sistemine ulusal ve uluslararası kuruluşların erişimi, izne ve bu Kuralların sırasıyla 21 ve 27'nci maddelerinde öngörülen koşullara tabidir.

Madde 7: Veri işlemenin denetimi

(1) Ulusal Merkez Büroları ve uluslararası kuruluşlar, bu Kurallara uygun olarak, verilerinin işlenmesi üzerinde her zaman kontrol sahibi olacaklardır. Herhangi bir Ulusal Merkez Büro veya uluslararası kuruluş, özellikle, bu Kuralların 58'inci maddesinde öngörülen koşullar altında, Teşkilatın polis veri tabanlarından birinde bulunan verilerine erişimi veya bunların kullanımını kısıtlamakta serbesttir.

(2) INTERPOL Bilgi Sisteminde işlenen veriler, Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar tarafından sağlanan verilerdir. Bununla birlikte, bu Kuralların 28'inci maddesi uyarınca özel kuruluşlar tarafından sağlanan veya bu Kuralların 24(2) maddesi uyarınca Genel Sekreterlik tarafından kaydedilen veriler de Sistemde işlenebilir.

Madde 8: INTERPOL bülten ve difüzyonlarının kullanımı

(1) INTERPOL kanalları aracılığıyla yapılan işbirliği talepleri ve uluslararası uyarılar, INTERPOL bültenleri veya difüzyonları yoluyla gönderilir.

(2) Ulusal Merkez Büroları, Anayasa uyarınca görevlerini yerine getirirken INTERPOL bültenlerini ve difüzyonlarını kullanma yetkisine sahiptir. Uluslararası kuruluşlar için bu yetki, yetkilendirmeye tabidir.

(3) INTERPOL bültenlerinin yayımlanması ve difüzyonların iletilmesi, bu Kuralların 73 ve sonraki maddelerine uygun olacaktır.

(4) Ulusal Merkez Büroları, aşağıdaki 9 uncu maddeye uygun olarak, işbirliği taleplerini ve uluslararası uyarıları mesajlar yoluyla gönderebilir. Cezai konularda soruşturma ve kovuşturma yetkisine sahip uluslararası kuruluşlar için bu seçenek izne tabidir.

Madde 9: Mesajlar aracılığıyla doğrudan iletişim

(1) INTERPOL Bilgi Sistemi, Ulusal Merkez Büroları arasında mesajlar aracılığıyla doğrudan iletişimi mümkün kılar.

(2) Ulusal Merkez Büroları, Anayasa uyarınca görevlerini yerine getirirken mesaj gönderme yetkisine sahiptir. Uluslararası kuruluşlar için bu yetki, yetkilendirmeye tabidir.

(3) Ulusal Merkez Büroları veya uluslararası kuruluşlar, bir mesaj göndermeden önce, mesajın bu Kurallara uygun olduğundan emin olmalıdır.

(4) Genel Sekreterlik, söz konusu mesajı gönderen Ulusal Merkez Bürosu veya uluslararası kuruluşun önceden onayı olmaksızın, söz konusu mesajı Teşkilatın polis veri tabanlarından birine kaydedemez. Genel Sekreterlik söz konusu mesajın alıcılarından biri ise, Ulusal Merkez Bürosu veya uluslararası kuruluşun önceden onay verdiği varsayılır.

(5) Belirli projeler veya girişimler bağlamında, farklı kuruluşlarla doğrudan mesaj yoluyla iletişim kurma yetkisi verilebilir. İstisnai durumlarda, Ulusal Merkez Bürosu, personeli olmayan ve açıkça yetkilendirilmiş kişilere bu tür mesajları gönderme yetkisi verebilir.

BÖLÜM II:

BİLGİ İŞLEMEYE İLİŞKİN İLKELER

Madde 10: Uluslararası polis işbirliğinin amaçları

(1) INTERPOL Bilgi Sistemindeki verilerin işlenmesi, yalnızca Teşkilatın amaç ve faaliyetlerine uygun, belirli ve açık bir amaç için gerçekleştirilebilir.

(2) Veriler, INTERPOL Bilgi Sisteminde en azından aşağıdaki amaçlardan biri için işlenecektir:

(a) aranan bir kişiyi gözaltına almak, yakalamak veya hürriyetini kısıtlamak amacıyla aramak,

(b) Polisin ilgilendiği bir kişi veya nesnenin yerinin tespit edilmesi,

(c) Bir suç soruşturması veya bir kişinin suç geçmişi ve faaliyetleriyle ilgili bilgi sağlamak veya elde etmek,

(d) Suç faaliyetleriyle ilgili bir kişi, olay, nesne veya yöntem hakkında uyarıda bulunmak,

(e) bir kişiyi veya cesedi teşhis etmek,

(f) adli analizler yapmak,

(g) uluslararası polis işbirliğine doğrudan ilişkin olan ve suçu önlemeyi veya tespit etmeyi amaçlayan güvenlik kontrolleri yapmak,

(h) sınır yönetimi ve sınır kontrol faaliyetlerini yürütmek,

(i) suç analizi de dahil olmak üzere tehditleri, suç eğilimlerini ve suç ağlarını tespit etmek.

(3) Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, verilerinin işlenme amacını belirlemekten ve özellikle bu amaç elde edildikten sonra düzenli incelemeler yapmaktan sorumludur.

(4) Genel Sekreterlik, söz konusu amaca her zaman uyumu garanti altına almak için mekanizmalar ve araçlar oluşturacak ve bu, bu Kuralların 125 ila 127'inci maddelerinde öngörülen koşullar çerçevesinde gerçekleştirilecektir.

(5) Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, verileri kullanırken bu amaca uygun hareket etmelidir.

(6) Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, uluslararası polis iş birliğinin diğer amaçları veya idari amaçlar için verileri yalnızca, işlemenin Kuruluşun amaç ve faaliyetlerine uygun olması ve verilerin INTERPOL Bilgi Sistemi'nde başlangıçta

işlendiği amaçla bağdaşmaması durumunda işleyebilirler. Kaynak, bu tür bir işlemeden haberdar edilecek ve bu Kuralların 64. Maddesinde belirtilen koşullar altında buna itiraz etme hakkını saklı tutacaktır. Bu tür bir işleme, verileri başlangıçta işlendiği amaçlar dışında işlemeyi seçen Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluşun sorumluluğundadır.

(7) Veriler, bu Kuralların 132 ve sonraki maddelerinde öngörülen koşullar altında, uluslararası polis işbirliğinden farklı herhangi bir meşru amaç için de işlenebilir.

Madde 11: Hukukilik

(1) INTERPOL Bilgi Sisteminde veri işleme, Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşa uygulanabilir hukuk dikkate alınarak yetkilendirilmeli ve işbirliğinin konusu olan kişilerin temel haklarına, Teşkilatın Anayasası'nın 2. maddesi ve söz konusu maddenin atıfta bulunduğu İnsan Hakları Evrensel Beyannamesi uyarınca saygı gösterilmelidir.

(2) Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, INTERPOL Bilgi Sistemine ilişkin verilerin toplanması ve kaydedilmesinin hukuka uygunluğunu sağlamaktan sorumludur.

(3) Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, INTERPOL Bilgi Sistemine girilen verilerin sorgulanmasının hukuka uygunluğunu sağlamakla da yükümlüdür.

Madde 12: Kalite

(1) INTERPOL Bilgi Sisteminde işlenen veriler, Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar tarafından kullanılabilmesini sağlayacak şekilde doğru, ilgili, amacına aykırı olmayan ve güncel olmalıdır.

(2) Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, INTERPOL Bilgi Sisteminde kaydettikleri ve ilettikleri verilerin kalitesinden sorumludur.

(3) Genel Sekreterlik, yukarıda belirtilen kaliteye her zaman uyulmasını sağlayacak mekanizma ve araçları oluşturur.

(4) Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, bu Kuralların 63 üncü maddesinde öngörülen koşullar uyarınca, verileri kullanmadan önce verilerin kalitesini kontrol etmek zorundadır.

Madde 13: Şeffaflık

(1) INTERPOL Bilgi Sistemindeki verilerin işlenmesi, her zaman Ulusal Merkez Bürolarının, ulusal kuruluşların ve uluslararası kuruluşların işleme haklarına, bu Kurallara uygun olarak saygı gösterilmesini garanti etmelidir.

(2) Genel Sekreterlik, veri işleme işlemlerinin ve Teşkilatın veri tabanlarının işleyişinin şeffaflığını sağlamakla sorumludur:

(a) Bu Kuralların 27 ila 31, 55, 56, 61, 68(4, d), 73(2) ve 97(3) maddelerinde belirtilen kişisel verilerin işlenmesini içeren herhangi bir işlem yapmayı planladığında INTERPOL Dosyalarının Kontrol Komisyonu'nun görüşünü talep edecektir,

(b) Bu Kuralların 51(7), 59, 118 ve 125(2, b) maddeleri uyarınca yapılan herhangi bir adımı INTERPOL Dosyalarının Kontrol Komisyonu'na bildirecektir.

(c) INTERPOL Bilgi Sistemi'nde veri işlenmesiyle ilgili ve önceden yetkilendirme gerektiren herhangi bir proje veya talebi, bu Kuralların 17(5), 22(3), 23, 29, 30, 31, 55(3), 68(8), 97(3) ve 131(3) maddelerine uygun olarak Yürütme Komitesi'ne sunacak ve gerektiğinde INTERPOL Dosyalarının Kontrol Komisyonu'nun görüşünü ekleyecektir. Yürütme Komitesi, verdiği yetkilendirmeler hakkında Genel Kurul'a, bu Kuralların 55(6) maddesinde öngörülen koşullar çerçevesinde rapor sunacaktır.

(d) Bu Kuralların 59, 68(4) ve 118. maddeleri uyarınca alınan önlemler hakkında Yürütme Komitesi'ni bilgilendirecektir.

(e) Bu Kuralların 126. maddesinde öngörülen koşullar çerçevesinde, aşağıdakilerin güncel kayıtlarını tutacaktır:

(i) INTERPOL Bilgi Sistemi'ne erişim sağlanan veya Sistemde işlenen verileri sağlayan Ulusal Merkezi Bürolar, ulusal kuruluşlar ve uluslararası kuruluşlar;

(ii) Teşkilatın analiz dosyaları dahil, polis veri tabanları,

(iii) bağlantı işlemleri,

(iv) gerçekleştirilen indirme ve yükleme işlemleri,

(v) veri tabanlarına kaydedilen veri işleme işlemleri,

(vi) Genel Sekreterlik tarafından uygulanan veri yönetim araçları,

(vii) doğrulama amacıyla gerçekleştirilen karşılaştırma işlemleri.

Bu kayıtlar, Ulusal Merkez Bürolarının her zaman erişimine açık olacaktır. Ayrıca, kendilerine verilen erişim haklarına göre uluslararası kuruluşların ve Ulusal Merkez Büroları aracılığıyla ulusal kuruluşların erişimine açık olacaktır.

(f) Genel Sekreterlik, Yürütme Kurulu tarafından bu Kurallar uyarınca belirlenen azami veri saklama sürelerinin güncel bir listesini tutar ve bu listeyi kamuoyunun erişimine açar.

Madde 14: Gizlilik

(1) INTERPOL Bilgi Sistemi'nde işlenen verilerin gizliliği, işbirliğinin konusu olan kişiler, kaynaklar ve Teşkilat açısından açıklanmasının oluşturabileceği risklere göre belirlenmelidir. Verilere yalnızca bu bilgileri bilmeye yetkili kişiler erişebilir.

(2) Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, INTERPOL Bilgi Sistemine girdikleri verilere gizlilik düzeyleri atamak ve sorguladıkları, ilettikleri veya dış işleme amaçları için kullandıkları verilerin gizliliğini gözetmek, bu Kuralların 112 ve sonraki maddelerinde öngörülen koşullar altında sorumludur.

(3) Genel Sekreterlik, tüm verilerin INTERPOL Bilgi Sisteminde, işlemeyi gerçekleştiren Ulusal Merkez Büro, ulusal kuruluşlar veya uluslararası kuruluşlar tarafından belirlenen gizlilik düzeyine uygun olarak işlenmesini sağlar.

(4) Genel Sekreterlik, bu Kurallara uygun olarak, verilerin açıklanmasının işbirliğinin konusu olan kişiler, veri kaynakları ve Teşkilat açısından oluşturabileceği risklere karşı verilerin gizlilik seviyesini artırmak için gerekli ve uygun tüm önlemleri alacaktır.

Madde 15: Güvenlik

(1) INTERPOL Bilgi Sisteminde işlenen veriler, bütünlüklerini ve gizliliklerini ihlal edebilecek risklere karşı korunmalı ve INTERPOL Bilgi Sistemine doğrudan erişimi olan Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar tarafından her zaman erişilebilir olmalıdır.

(2) Genel Sekreterlik, bilgi güvenliği yönetim sisteminin kurulmasından sorumludur. Bu amaçla, Ulusal Merkez Büroları veya bu amaçla kurulan danışma organlarındaki temsilcileriyle istişare ederek, uluslararası kabul görmüş standartlara ve risk değerlendirmesine dayalı bir güvenlik politikası oluşturur ve düzenli olarak günceller.

(3) Genel Sekreterlik, verilerin güvenliğinin sağlanması amacıyla, oluşturulan güvenlik politikasına uygun olarak iletişim altyapısı ve veri tabanlarının geliştirilmesinden sorumludur.

(4) Genel Sekreterlik, bu Yönetmeliğin 112'nci ve devamındaki maddelerinde öngörülen koşullar uyarınca, personelinin her veri gizliliği düzeyi için yetkilendirme veya güvenlik izni prosedürlerini tanımlamaktan sorumludur.

(5) Ulusal Merkez Büroları ve uluslararası kuruluşlar, INTERPOL Bilgi Sistemine erişim sağlamaktan, bu sisteme erişimlerini sağlayan tesislerin güvenliğinden, yerleşik güvenlik kurallarına uymaktan ve harici işlemelerde verilerin en az Genel Sekreterlikçe belirlenen güvenlik düzeyine eşdeğer bir düzeyde tutulmasından sorumludur.

(6) Genel Sekreterlik, INTERPOL Bilgi Sisteminde işlenen verilerin güvenliğini korumak için bu Kurallara uygun olarak tüm uygun önlemleri alır.

Madde 16: Polis amaçları doğrultusunda harici işleme

(1) INTERPOL Bilgi Sistemi'nde başlangıçta işlenen veriler, bu işlemin gerekli olması ve polis amaçları doğrultusunda gerçekleştirilmesi halinde sistem dışında da işlenebilir. Herhangi bir harici işleme, yukarıda belirtilen veri işleme ilkelerine uygun olmalıdır.

(2) Ulusal Merkez Büroları ve uluslararası kuruluşlar, bu Kuralların 114(4) ve 116. maddelerinde öngörülen koşullar altında, harici işleme ilişkin düzenlemeleri uygulamaktan sorumludur.

(3) Genel Sekreterlik, bu düzenlemelerin uygulanmasında Ulusal Merkez Bürolarına ve uluslararası kuruluşlara tavsiyelerde bulunur.

Madde 17: Etkili uygulama

(1) Mevcut Kurallar etkili bir şekilde uygulanmalıdır.

(2) Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, özellikle personel eğitimi yoluyla, faaliyetlerinin bu Kurallarda belirtilen ilke ve yükümlülüklere uygunluğunu garanti altına almak için etkili ve uygun önlemleri tanımlamak ve oluşturmaktan sorumludur.

(3) Ulusal Merkez Büroları, INTERPOL Bilgi Sisteminde işlenen verilere doğrudan erişim yetkisi vermeden veya Sistemde doğrudan işleme amacıyla veri sağlamadan önce, ulusal kuruluşlarının faaliyetlerinin bu Kurallarda belirtilen ilke ve yükümlülüklere uygunluğunu garanti altına almak için prosedürleri tanımlamak ve oluşturmakla yükümlüdür.

(4) Ulusal Merkez Büroları, mevcut Kurallar ışığında her bir ulusal kuruluşunun işleyişini düzenli olarak değerlendirmekten sorumlu olacak ve mevcut Kurallar tarafından belirlenen sınırlar dahilinde, söz konusu ulusal kuruluşlara karşı, verilerin uygunsuz şekilde işlenmesini sonlandırmak için gerekli ve uygun tüm düzeltici önlemleri alacaktır. Verilerin açıkça uygunsuz şekilde kullanılmasının oluşturacağı riski hesaba katmak için gerekli tüm önlemleri alabilirler.

(5) Genel Sekreterlik, Ulusal Merkez Bürolarının işleyişini bu Kurallar ışığında düzenli olarak değerlendirmekten sorumludur. Bu Kuralların 131'inci maddesinde belirtilen koşullar uyarınca, uygunsuz veri işlemelerini sonlandırmak için gerekli ve uygun tüm düzeltici önlemleri alır. Bir Ulusal Merkez Büronun işleme haklarının uzun süreli olarak askıya alınmasına yol açabilecek her türlü önlem, önceden onay alınmak üzere Yürütme Kuruluna sunulur.

(6) Genel Sekreterlik, uluslararası kuruluşların faaliyetlerini bu Kurallar ışığında düzenli olarak değerlendirmekten sorumludur ve bu Kuralların 131. maddesinde öngörülen koşullar altında, uyumsuz veri işlemelerini sonlandırmak için gerekli ve uygun düzeltici önlemleri alır.

Madde 18: Verilere erişim, düzeltme ve silme hakları

(1) Herhangi bir kişi veya kuruluş, INTERPOL Dosyalarının Kontrol Komisyonuna, söz konusu kişi veya kuruluşla ilgili INTERPOL Bilgi Sisteminde işlenen verilere erişim, düzeltme ve/veya silme talebinde bulunma hakkına sahiptir.

(2) Verilere erişim, düzeltme ve silme hakları, INTERPOL Dosyalarını Kontrol Komisyonu tarafından garanti altına alınacak ve ayrı kurallara tabi olacaktır. Bu kurallarda aksi belirtilmedikçe, verilere erişim, düzeltme ve/veya silme talepleri INTERPOL Bilgi Sistemi'nde işleme alınmayacaktır.

BAŞLIK 2:

KATILIMCILAR

BÖLÜM I:

ULUSAL MERKEZİ BÜROLARIN ROLÜ

Madde 19: Veri akışının koordinasyonu

(1) Ulusal Merkez Büroları, kendi ülkeleri tarafından sağlanan verilerin INTERPOL Bilgi Sisteminde işlenmesinin ulusal düzeyde eşgüdümünden sorumludur.

(2) Ulusal Merkez Büroları, mevcut Kurallara uygun olarak, INTERPOL Bilgi Sisteminde işlenen ve görevlerinin yerine getirilmesi için gerekli olan verileri ülkelerindeki kurumlara sağlamakla yükümlüdür.

Madde 20: Ceza soruşturmalarının koordinasyonu

(1) Ceza soruşturmalarına ilişkin hususlar Ulusal Merkez Büroları ile işbirliği halinde yürütülür.

(2) Ulusal Merkez Büroları, INTERPOL bültenleri, difüzyonları ve mesajları yoluyla kendilerine gönderilen işbirliği taleplerinin ve uluslararası uyarıların ulusal düzeyde işlenmesinin eşgüdümünü sağlamaktan sorumludur. Bu nedenle, ulusal düzeyde etkili uluslararası işbirliği için en uygun araçları belirleme konusunda özgür olacaklardır.

(3) Ulusal Merkez Büroları, kendi ülkelerinin kurumlarının talebi üzerine INTERPOL bültenleri, difüzyonları ve mesajları yoluyla gönderdikleri işbirliği taleplerini ve uluslararası uyarıları takip etmekle yükümlüdür.

Madde 21: INTERPOL Bilgi Sistemine ulusal düzeyde doğrudan erişim yetkisi verilmesi

(1) Ulusal Merkez Büroları, kendi ülkelerindeki kuruluşların INTERPOL Bilgi Sistemine erişim yetkisini verme ve erişim ve veri işleme haklarının kapsamını belirleme yetkisine sahiptir.

(2) Ulusal Merkez Büroları, doğrudan erişime izin vermeden önce aşağıdaki tüm koşulların karşılandığından emin olmalıdır:

(a) Doğrudan erişim yetkisi verilecek kuruluş, bu Kuralların 1(8) maddesinde tanımlanan ulusal kuruluş olmalıdır,

(b) Söz konusu kuruluşun faaliyet ve görevlerinin niteliği, Teşkilatın amaçlarına veya tarafsızlığına aykırı olmamalıdır,

(c) Ulusal yasalar, bu kuruluşun erişimini yasaklamamalıdır,

(d) Kuruluş, bu Kurallara uyabilecektir,

(e) Verilecek erişim ve işleme hakları, kuruluşun görev ve işlevlerini yerine getirmesi için sınırlı, kesinlikle gerekli ve orantılı olmalıdır.

(3) Bir Ulusal Merkez Bürosu, INTERPOL Bilgi Sistemine doğrudan erişim yetkisi verdiğinde, bu yetki Ulusal Merkez Bürosu ile yeni ulusal kuruluş arasında önceden yapılmış bir anlaşmaya tabi olacaktır. Bu anlaşma, mevcut Kurallara eklenen "Ulusal Kuruluşların INTERPOL Bilgi Sistemine Erişimine İlişkin Tüzük" ile uyumlu olmalıdır.

(4) Ulusal Merkez Bürosu, yeni bir ulusal kuruluşa yetki verdiğinde, Genel Sekreterliğe ve tüm Ulusal Merkez Bürolarına ve uluslararası kuruluşlara derhal bildirimde bulunur.

(5) Ulusal kuruluşlar, kendilerine tanınan işleme hakları çerçevesinde verilerini INTERPOL Bilgi Sisteminde işlerler.

(6) Ulusal Merkez Büroları, bu işleme haklarını kullanabilmeleri için gerekli bilgileri ulusal kuruluşlarına iletir.

(7) Ulusal Merkez Büroları, INTERPOL Bilgi Sistemine erişim yetkisi verdikleri ulusal kuruluşlar tarafından verilerin işlenmesinden sorumludur.

BÖLÜM II:

GENEL SEKRETERLİĞİN ROLÜ

Madde 22: Sistemin yönetimi

(1) Genel Sekreterlik, INTERPOL Bilgi Sisteminin genel yönetiminden sorumludur.

(2) INTERPOL Bilgi Sistemini tasarlar, düzenler ve yönetir ve hangi teknolojilere dayandırılacağına karar verir. Veri işleme teknolojilerini uygularken, Genel Sekreterlik, uygun teknik ve organizasyonel önlemler aracılığıyla bu Kuralların gerekliliklerinin mümkün olan en kısa sürede tasarım ve varsayılan olarak entegre edilmesini sağlar.

(3) Yürütme Kurulunun denetimi altında ve bu Kurallara uygun olarak, Ulusal Merkez Büroları tarafından sunulan indirme ve bağlantı taleplerini, bu Kuralların 55 ve 56'ncı maddelerinde belirtilen koşullar çerçevesinde inceler ve işleme koyar.

(4) Kuruluşun veri tabanlarını muhafaza eder.

(5) INTERPOL Bilgi Sistemi'ndeki verilerin işlenmesini yönetir ve Kuruluşun veri tabanlarındaki veri işleme koşullarının usulüne uygun olarak gözetilmesinin sağlanmasını temin eder. Verilerin ve Sistem'e erişimin yönetilmesine yönelik araçları devreye sokar. Yerinde denetimler gerçekleştirirken ve işleme olaylarını çözerken bir yönetim rolü üstlenir.

(6) INTERPOL Bilgi Sistemi aracılığıyla doğrudan veri alışverişini mümkün kılmak için INTERPOL'ün iletişim altyapısını yönetir. Mevcut Kuralların 1. Başlığı, II. Bölümü ve 22(5) Maddesi uyarınca kendisine uygulanan herhangi bir yükümlülüğe bakılmaksızın, Genel Sekreterlik veri paylaşımına katılmamış veya paylaşımdan yararlanamamışsa, rolü aşağıdaki şekilde sınırlandırılır:

(a) Bu Kuralların 15. maddesi uyarınca, söz konusu veri alışverişlerinin güvenliğini sağlar,

(b) Mevcut Kuralların veya belirli bir projeye uygulanabilir hüküm ve koşulların potansiyel bir ihlalinin farkına vardığında, Başlık 4, Bölüm III kapsamındaki tedbirleri uygulamak da dahil olmak üzere, mevcut Kurallara uyumu incelemek ve sağlamak için harekete geçer,

(c) Yukarıdaki (b) paragrafı uyarınca rolünü yerine getirmek için gereken eylemler hariç olmak üzere, ilgili kuruluşun açık izni olmadan doğrudan görüşmelerin içeriği için INTERPOL'ün iletişim altyapısına erişemez.

Madde 23: İşbirliğini artırmaya yönelik ek önlemler

(1) Genel Sekreterlik, Genel Kurula veri işlemeyle ilgili anlaşmaların yapılmasını teklif etme ve Yürütme Kuruluna, bu Yönetmeliğin 27, 28, 29, 73 ve 97'nci maddelerinde belirtilen şartlar altında veri tabanları oluşturulmasını, INTERPOL bültenleri ve difüzyonlarının yapılmasını veya dağıtılmasını teklif etme yetkisine sahiptir.

(2) Genel Sekreterlik, bu Kurallarda belirlenen sınırlar içinde, yukarıdaki teklifleri incelemek ve hazırlamak için denemeler yapabilir.

Madde 24: Verilerin kaydedilmesi

(1) Bu Kurallara uygun olarak, Genel Sekreterlik, Teşkilatın polis veri tabanlarındaki verileri kaydeder, günceller ve siler:

(a) INTERPOL Bilgi Sistemi'ne doğrudan erişimi olmayan kaynaklar adına,

(b) Veriler kamuya açık bilgi niteliğinde olduğunda veya Genel Sekreterlik, Ulusal Merkezi Bürolar, uluslararası kuruluşlar veya özel kuruluşlarla iletişime geçen kişi veya kuruluşlardan alındığında, bu Kuralların 47. maddesinde öngörülen koşullar çerçevesinde veya veriler, Genel Sekreterlik tarafından yapılan suç analizlerinin sonucu olduğunda kendi girişimiyle,

(c) Olağanüstü durumlarda, INTERPOL Bilgi Sistemi'ne doğrudan erişimi olan bir Ulusal Merkezi Büro, ulusal kuruluş veya uluslararası kuruluşun talebi üzerine veya onun adına,

(2) Genel Sekreterlik, INTERPOL Bilgi Sistemine erişimi olmayan kaynaklar adına veya bilgilerin güncellenmesi ve silinmesine ilişkin prosedürler önceden belirlenmişse kendi inisiyatifi ile veri kaydedebilir.

Madde 25: Koordinasyon

(1) Genel Sekreterlik, Ulusal Merkez Büroları arasındaki işbirliğini kolaylaştırır. Bu Kurallar ve kaynak tarafından belirlenen gizlilik kısıtlamaları ve kuralları uyarınca, uluslararası işbirliğinin koordinasyonunu iyileştirebileceğine inandığı tüm verileri onlardan talep eder veya onlara iletir.

(2) Uluslararası işbirliğinin amaçları gerektiriyorsa, Genel Sekreterlik, ilgili Ulusal Merkez Bürolarının açık iznine tabi olmak üzere, ulusal kuruluşlarla doğrudan koordinasyon rolünü üstlenebilir.

(3) Genel Sekreterlik, gerektiğinde Ulusal Merkez Büroları ile uluslararası ve özel kuruluşlar arasındaki işbirliğini kolaylaştırır.

(4) Genel Sekreterlik, uluslararası koordinasyonu geliştirmek amacıyla, bu Kuralların 103'üncü maddesinde belirtilen şartlar çerçevesinde kendiliğinden bültenler yayımlayabilir.

Madde 26: Acil önlemler

(1) Teşkilatın kurduğu iş birliği mekanizmaları, bağımsızlığı veya taahhütlerini yerine getirmesi ciddi ve yakın bir tehdit altındaysa ve INTERPOL Bilgi Sisteminin düzgün işleyişinin kesintiye uğraması muhtemelse, Genel Sekreter, Teşkilat Başkanı ile resmi istişare sonrasında veri işleme konusunda bu koşullar altında gerekli olan uygun önlemleri alır. Ulusal Merkez Büroları ve INTERPOL Dosyalarının Denetimi Komisyonu'nu bilgilendirir. Bu önlemler, Ulusal Merkez Bürolarının Anayasa uyarınca görevlerini yerine getirmelerini sağlayacak araçlara en kısa sürede sahip olmalarını sağlama isteğinden kaynaklanmalıdır.

(2) Kişilere veya mallara yönelik gerçek ve yakın bir tehdit olması ve Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluşun bu tehdidi önlemesine olanak tanıyan verilere erişim kısıtlamaları getirilmesi durumunda, Genel Sekreterlik, bu Kuralların 59'uncu maddesinde öngörülen acil durum prosedürünü uygulamaya yetkilidir.

BÖLÜM III:

ULUSLARARASI VE ÖZEL KURULUŞLARLA İLİŞKİLER

Madde 27: Uluslararası kuruluşlar tarafından verilerin işlenmesine ilişkin koşullar

(1) Teşkilat, uygun gördüğü takdirde ve Anayasa'da belirtilen amaç ve hedeflerle uyumlu olması halinde, veri işleme konusunda uluslararası kuruluşlarla düzenli olarak iş birliği yapmak amacıyla ilişkiler kurabilir. Teşkilat ile uluslararası bir kuruluş arasında düzenli ilişkilerin kurulması bir sözleşme ile düzenlenir.

(2) Genel Sekreterlik, kişisel verilerin işlenmesine ilişkin her türlü sözleşme taslağı hakkında INTERPOL Dosyalarının Denetimi Komisyonunun görüşünü ister.

(3) Genel Sekreterlik, tüm taslak anlaşmaları onaylanmak üzere Genel Kurula sunar. Genel Sekreterlik, talebini gerekçelendirmek için şunları belirtir:

(a) Anlaşmanın amaçları, koşulları ve sonuçları,

(b) Genel Sekreterlik tarafından yapılan testlerin sonuçları,

(c) Taslak anlaşma kişisel veri işlenmesini içeriyorsa, INTERPOL Dosyalarının Kontrol Komisyonu'nun görüşü,

(d) Taslak anlaşmanın metni.

(4) Uluslararası kuruluşlar tarafından veri işlenmesi aşağıdaki tüm koşullara tabidir:

(a) Uluslararası kuruluş, uluslararası, hükümetler arası veya kamu yararına faaliyet gösteren bir sivil toplum kuruluşu olmalıdır,

(b) Bu işleme, uluslararası kuruluş ile INTERPOL arasında öngörülen işbirliği amaçlarıyla sınırlı olmalıdır,

(c) Kişisel veri işleme, yalnızca kuruluşun bu verilere dair bilme ihtiyacı ile sınırlı olmalıdır,

(d) Uluslararası kuruluş, anlaşmada, bu Kurallarda belirtilen işleme ilkelerine ve her kaynağın genel yükümlülüklerine uymayı taahhüt etmelidir;

(e) Uluslararası kuruluş ve INTERPOL, her iki taraf arasında iletilen verilerin işlenme prosedürleri konusunda bir anlaşma yapmış olmalıdır.

(5) Uluslararası kuruluşların INTERPOL Bilgi Sisteminin bir kısmına doğrudan erişimi aşağıdaki ek koşullara tabidir:

(a) Uluslararası kuruluş, bu Kurallara ve anlaşmanın özel hükümlerine uyacağını kabul eder ve bunu taahhüt eder,

(b) Uluslararası kuruluş, INTERPOL Genel Sekreterliği tarafından, bu Kurallara uygun olarak INTERPOL Bilgi Sistemi'ne erişim ve kullanım için belirlenebilecek güvenlik kurallarına ve idari prosedürlere uyacağını kabul eder ve bunu taahhüt eder,

(c) Uluslararası kuruluş, INTERPOL tarafından iletilen verilerin işlenmesi üzerinde düzenli denetimlerin, ya uzaktan ya da kuruluşun tesislerinde yapılabileceğini kabul eder,

(d) Erişim yalnızca söz konusu kuruluşun tek bir birim veya departmanına verilecektir,

(e) Erişim, işbirliği talepleri ve uyarıların iletiminde veya Ulusal Merkezi Büroların bu taleplere ve uyarılara erişiminde kesinti veya gecikmeye yol açmamalıdır,

(f) Veri iletimi amacıyla bir veya birkaç Ulusal Merkezi Büroya ya da bir veya birkaç uluslararası kuruluşa mesaj göndermek isteyen uluslararası kuruluş, ceza soruşturması ve kovuşturma yetkilerine sahip olmalıdır,

(g) INTERPOL bültenlerinin yayımlanmasını talep etmek veya difüzyon iletmek isteyen uluslararası kuruluş, ceza soruşturması ve/veya kovuşturma yetkilerine sahip olmalıdır. Ancak özel bülten sisteminin kullanımı, duruma göre ayrı ayrı değerlendirilecektir.

(6) Kuruluşun, INTERPOL Bilgi Sistemine yeni bir uluslararası kuruluşun erişimini yetkilendirme kararı, Genel Sekreterlik tarafından Ulusal Merkez Bürolarına ve diğer uluslararası kuruluşlara bildirilir. Erişim, ancak bu Kuralların 109'uncu maddesinde belirtilen koşullar altında, diğer Ulusal Merkez Büroları ve diğer uluslararası kuruluşların, yeni kuruluşa kendi verilerini işleme hakkı tanıyan haklar üzerindeki denetimini güvence altına almaya yönelik bir prosedürün tamamlanmasından sonra geçerlilik kazanır.

(7) Yapılan anlaşmaların listesi her yıl Yürütme Kuruluna, INTERPOL Dosyalarının Denetimi Komisyonuna ve Genel Kurula sunulur.

Madde 28: Özel kuruluşlar tarafından verilerin işlenmesine ilişkin koşullar

(1) Kuruluş, amaçlarının gerçekleştirilmesiyle ilgili olduğu ölçüde, veri işleme konularında kendisiyle işbirliği yapmak isteyen özel kuruluşlarla ilişkiler kurabilir. INTERPOL ile özel kuruluş arasındaki ilişkilerin kurulması ve yürütülmesi bir sözleşme ile düzenlenir.

(2) Genel Sekreterlik, kişisel verilerin işlenmesine ilişkin her türlü sözleşme taslağı hakkında INTERPOL Dosyalarının Denetimi Komisyonunun görüşünü ister.

(3) Genel Sekreterlik, tüm taslak anlaşmaları onaylanmak üzere Genel Kurula sunar. Genel Sekreterlik, talebini gerekçelendirmek için şunları sunar:

(a) Anlaşmanın amaçları, koşulları ve sonuçları,

(b) Genel Sekreterlik tarafından yapılan testlerin sonuçları,

(c) Taslak anlaşma kişisel veri işlenmesini içeriyorsa INTERPOL Dosyalarının Kontrol Komisyonu'nun görüşü,

(d) Taslak anlaşmanın metni.

(4) Özel kuruluşla işbirliği:

(a) INTERPOL Anayasası'na ve özellikle ulusal egemenlik ilkesine saygı göstermek. INTERPOL Bilgi Sistemi'ne veri kaydeden veya adına sisteme veri kaydedilen herhangi bir Ulusal Merkez Bürosu, söz konusu verilerin özel bir kuruluşa iletilmesine itiraz edebilir,

(b) Yürütme Kurulu tarafından daha önce yetkilendirilmiş ve daha sonra Genel Kurul tarafından onaylanmış olan anlaşmalara tabi olabilir.

(5) Bu tür bir işbirliği yalnızca aşağıdaki durumlarda değerlendirilebilir:

a) Özel kuruluş, özel hukuka tabi tüzel kişilik olmalıdır,

(b) İşleme, Teşkilatın amaç ve faaliyetleriyle uyumlu olmalıdır,

(c) İşbirliğinin amacı açıkça belirtilmeli ve adi suçlarla ilgili önleme faaliyetlerinden biriyle bağlantılı olmalıdır,

(d) Amaçla ilgili olarak uluslararası polis işbirliği açısından faydalı olmalıdır,

(e) Sürekli bir işbirliği öngörülmelidir,

(f) Erişim sağlanan veri türü özel olarak belirlenmelidir,

(g) Özel kuruluş tarafından sağlanan veriler açıkça tanımlanmalı ve diğer kaynaklardan elde edilen verilerle karıştırılamamalıdır,

(h) Özel kuruluşla işbirliğinde Teşkilatın bağımsızlığı garanti edilmelidir,

(i) Özel kuruluşla işbirliği, uluslararası işbirliği talepleri ve uyarıların iletimini engellememelidir,

(j) Özel kuruluş, anlaşmada, işleme ilkelerine ve tüm kaynaklar için geçerli genel yükümlülüklere uymayı taahhüt etmelidir, bu ilkeler mevcut Kurallarda belirtilmiştir.

(6) Özel kuruluşlara sağlanan veriler analitik verilerle sınırlı olmalı ve kişisel nitelikte olmamalıdır. Bununla birlikte, istisnai durumlarda, özel kuruluşlara sağlanan veriler, belirli bir projenin parçası olarak, kişisel verileri (ancak Ulusal Merkez Büroları veya verileri sağlayan uluslararası kuruluşlar açık yetki vermedikçe, nominal veriler hariç) ve/veya operasyonel bir bağlamda kullanılan verileri kapsayacak şekilde genişletilebilir. Bu durumda, aşağıdaki ek koşulların karşılanması gerekir:

(a) Projenin kapsamı açıkça tanımlanmalıdır,

(b) Proje, ilgili kuruluşlarla önceden yapılmış bir anlaşma konusu olmalıdır,

(c) Bu verilere erişim, yalnızca kuruluşun söz konusu verileri bilme ihtiyacı ile sınırlı olmalıdır,

(d) Verilerin kullanım amacı, mevcut Kuralların Madde 10(2)'de belirtilen hedeflerle orantılı olmalıdır.

(7) Verilerin özel kuruluşlar tarafından işlenmesine ilişkin şartlar, özel hukuk kişileri ile Kurum arasında akdedilen sözleşmede düzenlenir.

(8) Genel Sekreterlik, anlaşma kapsamındaki yetki ve koşullara uygun olarak özel kişilere veri sağlamadan önce, söz konusu verinin kaynağını bilgilendirir. Kaynak, bu veri iletişimine itirazını bildirim tarihinden itibaren 45 gün içinde bildirir.

(9) INTERPOL Bilgi Sisteminde işlenen verilerin güvenliğinin ve bütünlüğünün garanti altına alınması amacıyla, verilerin özel kişilere iletilme biçimlerinin sözleşmede belirlenmesi gerekmektedir.

(10) Genel Sekreterlik, özel kuruluşların INTERPOL Bilgi Sisteminde işlenen verileri sağlamak veya elde etmek için kullandıkları araçların, bu kuruluşlarca bu amaçla yapılan anlaşmalara uygun olarak yalnızca yetkilendirilen verilere erişebilmesini sağlar. Genel Sekreterlik, özel kuruluşların operasyonel verilere erişmesini, bunları tehlikeye atmasını veya polis haberleşmelerine müdahale etmesini engeller.

(11) INTERPOL Bilgi Sistemi hiçbir koşulda, polisin özel kuruluşlarla işbirliğini düzenleyen ulusal yasaların getirdiği kısıtlamaları aşmak için kullanılamaz.

(12) Yapılan anlaşmaların listesi her yıl Yürütme Kuruluna, INTERPOL Dosyalarının Denetimi Komisyonuna ve Genel Kurula gönderilir.

BAŞLIK 3:

VERİ İŞLEME USULLERİ

BÖLÜM I:

POLİS VERİ TABANLARI

KISIM 1: YETKİLENDİRME

Madde 29: Veri tabanı oluşturulması

(1) Genel Sekreterlik, polis veri tabanı oluşturulmasına ilişkin her türlü öneriyi onay için Yürütme Kuruluna sunar.

(2) Talebini gerekçelendirmek için Genel Sekreterlik şunları belirtir:

(a) Bu projeyi geliştirmesine yol açan nedenler ve söz konusu projenin mali etkileri,

(b) Bu veri tabanının genel özelliklerinin listesi, Ulusal Merkez Bürolar veya bu amaçla kurulan danışma organlarındaki temsilcileri ile istişare edilerek hazırlanır,

(c) Genel Sekreterlik tarafından yapılan testlerin sonuçları,

(d) Veri tabanı kişisel veri içeriyorsa veya bu verilerle bağlantılı ise INTERPOL Dosyalarını Kontrol Komisyonu'nun görüşü.

(3) Polis veri tabanı oluşturulması halinde, durum derhal Ulusal Merkez Bürolarına bildirilir. Ayrıca, INTERPOL Bilgi Sistemine erişim haklarına sahip uluslararası kuruluşlara da bildirimde bulunulur.

Madde 30: Mevcut bir veri tabanının değiştirilmesi

(1) Genel Sekreterlik, polis veri tabanlarını değiştirme yetkisine sahiptir.

(2) Veri tabanı kişisel veri içeriyorsa veya bu verilerle bağlantılı ise, genel özelliklerinde değişikliğe yol açacak her değişiklik önerisi için Genel Sekreterlik, INTERPOL Dosyalarını Kontrol Komisyonu'nun görüşünü talep eder.

(3) Genel Sekreterlik, bir veri tabanının genel özelliklerinde değişikliğe yol açacak herhangi bir değişiklik önerisini onay için Yürütme Komitesi'ne sunar.

(4) Bu amaçla Genel Sekreterlik şunları belirtir:

(a) Bu veri tabanında değişiklik önerme nedenleri ve söz konusu değişikliğin mali etkileri,

(b) Veri tabanının gözden geçirilmiş özellik listesi, Ulusal Merkez Bürolar veya bu amaçla kurulan danışma organlarındaki temsilcileri ile istişare edilerek hazırlanır,

(c) Genel Sekreterlik tarafından yapılan testlerin sonuçları,

(d) Veri tabanı kişisel veri içeriyorsa veya bu verilerle bağlantılı ise INTERPOL Dosyalarını Kontrol Komisyonu'nun görüşü.

(5) Polis veri tabanının genel özelliklerinde meydana gelen her türlü değişiklik derhal Ulusal Merkez Bürolarına bildirilir. Ayrıca, INTERPOL Bilgi Sistemine erişim haklarına göre uluslararası kuruluşlara da bildirilir.

Madde 31: Mevcut bir veri tabanının silinmesi

(1) Genel Sekreterlik, INTERPOL Dosyalarını Kontrol Komisyonuna, bir veri tabanının silinmesine ve söz konusu veri tabanında yer alan verilerin işlenmesine ilişkin her türlü niyeti bildirir.

(2) Genel Sekreterlik, bir veri tabanının silinmesine ilişkin her türlü talebini Yürütme Kurulunun onayına sunar.

(3) Bu amaçla Genel Sekreterlik şunları belirtir:

(a) Silme önerisini getiren nedenler ve silmenin mali etkileri,

(b) INTERPOL Dosyalarını Kontrol Komisyonu'na sunulan rapor ve Komisyon'un görüşü.

(4) Bir polis veri tabanının silinmesi derhal Ulusal Merkez Bürolara bildirilir. Ayrıca, Uluslararası kuruluşlara, INTERPOL Bilgi Sistemi'ne verilen erişim haklarına göre bildirim yapılır.

Madde 32: Yürütme Komitesi tarafından verilen yetkiler

(1) Yürütme Kurulu, her yıl, Teşkilata ait polis veri tabanlarının oluşturulması, değiştirilmesi veya silinmesi için verdiği yetkileri, özellikle bunların INTERPOL Bilgi Sistemi'ndeki konumlarını, her birinin amacını, sakladıkları verilerin niteliğini ve her bir veri tabanına ilişkin işleme haklarını belirterek Genel Kurul'a bildirir.

(2) Yürütme Kurulu, INTERPOL Bilgi Sisteminde işlenen her bir veri türü için belirlediği azami saklama süresini gerekçelerini de belirterek Genel Kurula bildirir.

Madde 33: Mevcut veri tabanlarının kaydı

(1) Genel Sekreterlik, Teşkilatın polis veri tabanlarının güncel bir kaydını tutar. Sicilde her veri tabanının genel özellikleri belirtilir.

(2) Ulusal Merkez Büroları bu sicile istedikleri zaman başvurabilirler. Uluslararası kuruluşlar, INTERPOL Bilgi Sistemine erişim haklarına göre bu sicilin bir bölümüne başvurabilirler.

BÖLÜM 2: İŞLEYİŞ

Madde 34: Teşkilat Anayasasına Uyum

(1) Bu Kuralların 5'inci maddesi uyarınca, bir polis veri tabanına herhangi bir veri kaydedilmeden önce, Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, verilerin Teşkilat Anayasası'nın 2'inci maddesine uygun olduğundan ve ayrıca söz konusu verileri geçerli ulusal yasalar ve uluslararası sözleşmeler ile söz konusu Maddenin atıfta bulunduğu İnsan Hakları Evrensel Beyannamesi'nde yer alan temel insan hakları uyarınca kaydetmeye yetkili olduğundan emin olacaktır.

(2) Bu Kuralların 5'inci maddesi uyarınca, bir polis veri tabanına herhangi bir veri kaydedilmeden önce, Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, verilerin Teşkilat Anayasası'nın 3'üncü maddesine uygun olmasını sağlar.

(3) Verilerin Anayasa'nın 3'üncü maddesine uygun olup olmadığını belirlemek için, aşağıdaki tüm ilgili unsurlar incelenir:

(a) Suçun niteliği, yani suçlamalar ve temel olaylar,

(b) İlgili kişilerin statüsü,

(c) Verilerin kaynağının kimliği,

(d) Diğer bir Ulusal Merkez Bürosu veya uluslararası kuruluşun görüşü,

(e) Uluslararası hukuk kapsamındaki yükümlülükler,

(f) Teşkilatın tarafsızlığına ilişkin etkiler,

(g) Olayın genel bağlamı.

(4) Genel Kurul'un direktifleri ve uluslararası hukuktaki gelişmeler ışığında, Genel Sekreterlik, Anayasa'nın 2 ve 3 üncü maddelerinin uygulanmasına ilişkin uygulama rehberleri derleyebilir ve bunları Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşların kullanımına sunabilir.

Madde 35: Verilerin uluslararası polis işbirliği amaçları açısından önemi

(1) Bu Kuralların 5(3) Maddesi uyarınca, bir polis veri tabanına herhangi bir veri kaydedilmeden önce, Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, verilerin uluslararası polis işbirliği amaçları açısından ilgili olduğundan emin olacaktır.

(2) Verilerin kaydedilmesine ilişkin bu koşula uyum aşağıdaki hususlar açısından değerlendirilecektir:

(a) Mevcut Kuralların Madde 10(2)'sinde belirtilen uluslararası polis işbirliğine özgü amaçlar,

(b) Verilerin uluslararası niteliği ve özellikle, verilerin kaynağı dışında diğer Ulusal Merkez Büroları, ulusal kuruluşlar veya uluslararası kuruluşlar tarafından kullanılabilirliği.

Madde 36: Veri tabanlarının genel özellikleri

(1) Her polis veri tabanı aşağıdaki özelliklere göre tanımlanacaktır:

(a) Veri tabanının özel amacı,

(b) İçerdiği verilerin niteliği, özellikle kişisel veya özellikle hassas veriler,

(c) Veri tabanına katkıda bulunması muhtemel kaynaklar,

(d) Uygulanacak gizlilik seviyeleri,

(e) Uygulanacak kısıtlama türleri,

(f) Uygulanacak güvenlik önlemleri,

(g) Veri tabanına veri kaydetmesi muhtemel Ulusal Merkez Büroları, ulusal veya uluslararası kuruluşlar,

(h) Verilerin kaydedilmesi için asgari koşullar,

(i) Verilerin kaydedilmesine ilişkin prosedürler, özellikle doğaları gereği kaydedilen veriler üzerinde yapılan özel işlemler,

(j) Kaydedilen verilerin güncellenmesine ilişkin prosedürler,

(k) Verilerin saklama süresi ve bu sürenin uzatılması veya silinmesine ilişkin özel yöntemler,

(l) Verilerin uygunluğunu kontrol etmek için kullanılan prosedürler ve mekanizmalar;

(m) Veri tabanını kullanması muhtemel Ulusal Merkez Büroları veya ulusal/uluslararası kuruluşlar,

(n) Veri tabanının kullanımıyla ilgili prosedürler, özellikle doğrudan erişim veya herhangi bir bağlantı ve yükleme işlemleri,

(o) Verilerin kullanımına ilişkin prosedürler,

(p) Veritabanındaki kaydedilen veriler temel alınarak olumlu bir sorgu sonucu oluştuğunda izlenecek prosedürler,

(q) Mevcut Kuralların 61'inci maddesi uyarınca halka açıklanabilecek veriler.

(2) Yukarıdaki genel özelliklerin tümü, Teşkilatın her bir veri tabanına uygulanacak yasal çerçeveyi belirler.

Madde 37: Veri tabanlarına veri kaydedilmesine ilişkin asgari koşullar

(1) Her veri tabanında verilerin kaydedilmesi için asgari koşullar belirlenir.

(2) Veri tabanından bağımsız olarak, bir kişi, nesne veya olaya ilişkin verilerin kaydı şunları içermelidir:

(a) Verinin kaynağının kimliği,

(b) Verinin kaydedildiği tarih,

(c) Kaydın yapılma amacı,

(d) Herhangi bir kişisel veri için, kişinin statüsü ve bu kişiyi bir olaya bağlayan veriler,

(e) Verinin gizlilik seviyesi,

(f) Verinin saklama süresi,

(g) Erişim kısıtlamaları,

(h) Tüm verilerin amaca uygun ve uluslararası polis işbirliği amaçları için ilgili olduğunu garanti eden diğer bilgiler.

(3) Bu koşullar, Genel Sekreterlik tarafından Ulusal Merkez Büroları veya bu amaçla kurulan danışma organlarındaki temsilcileriyle istişare edilerek belirlenir ve tüm Ulusal Merkez Bürolarına bildirilir. Ayrıca, kendilerine verilen erişim haklarına göre uluslararası kuruluşlara da bildirilir.

(4) Tüm Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, bir polis veri tabanına veri kaydederken asgari kayıt koşullarının karşılanmasını sağlar.

(5) Tüm Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, verilerin kaydedilmesine temel teşkil eden veya bilgilerin veri tabanında tutulmasını haklı kılan tüm öğeleri saklayacaktır.

Madde 38: Kişilere ilişkin verilerin kaydedilmesine ilişkin ek koşullar

(1) Kişilere ilişkin verilerin kaydedilmesine ilişkin ek koşullar aşağıdaki hallerde uygulanır:

(a) ölen kişilerle ilgili veriler,

(b) mağdurlar veya tanıklarla ilgili veriler,

(c) reşit olmayan kişilerle ilgili veriler,

(d) özellikle hassas veriler.

(2) Tüm Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, bir polis veri tabanına bilgi kaydederken bu ek kayıt koşullarına uyacaktır.

Madde 39: Ölen kişilere ilişkin verilerin kaydedilmesine ilişkin ek koşullar

(1) Ölen kişilere ilişkin veriler yalnızca aşağıdaki hallerde kaydedilir:

(a) kimlik tespiti amacıyla,

(b) kişi, Teşkilatın polis veri tabanlarında kayıtlı bir ceza davasında veya olayda rol oynamışsa ve bu kişiyle ilgili veriler, davayı veya olayı anlamak için gerekli ise,

(c) suç analizi amacıyla.

(2) Veriler, yukarıda belirtilen işleme amaçlarından birini gerçekleştirmek için kesinlikle gerekli olan süre boyunca kaydedilir.

(3) Bu kişilerin statüsü ve verilerin kaydedilme amacı, verilerin hiçbir şekilde işbirliğine konu kişilere ait verilerle karıştırılmayacak şekilde belirtilir.

Madde 40: Mağdur veya tanık olan kişilere ilişkin verilerin kaydedilmesine ilişkin ek koşullar

(1) Mağdur veya tanık olan kişilere ilişkin veriler, yalnızca mağduru oldukları veya tanığı oldukları olay veya eylemler bağlamında kaydedilir ve başka olay veya eylemlerle bağlantılı olarak kullanılamaz. Bu kişilerin statüsü ve verilerin kaydedilme amacı, bu eylemlerden şüphelenilen, sanık veya hükümlü kişilere ilişkin verilerle hiçbir şekilde karıştırılmayacak şekilde belirtilir.

(2) Bunlara karşı hiçbir kısıtlayıcı tedbir alınamayacağına dair ek bir gösterge eklenir.

Madde 41: Küçüklere ilişkin verilerin kaydedilmesine ilişkin ek koşullar

(1) Kişinin, kaydedilmekte olan olay veya eylemin gerçekleştiği sırada reşit olmadığı durumlarda ek olarak "KÜÇÜK" ibaresi eklenmelidir. Küçüklerin reşit olma yaşı, Ulusal Merkez Bürosunun veya verileri kaydeden ulusal kuruluşun ulusal yasalarına veya uluslararası bir kuruluş söz konusu olduğunda geçerli kurallara göre belirlenir.

(2) Bu durumda, verileri kaydeden Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, geçerli ulusal yasalarca konulan özel koşulları belirtecektir.

Madde 42: Özellikle hassas verilerin işlenmesine ilişkin ek koşullar

(1) Özellikle hassas veriler, INTERPOL Bilgi Sistemi'nde yalnızca aşağıdaki durumlarda işlenebilir:

(a) Veriler, Teşkilatın amaçlarının ve veri işleme amaçlarının (Madde 10(2) uyarınca) gerçekleştirilmesi açısından ilgili ve özellikle önemli adli değere sahip olmalıdır,

(b) Veriler nesnel bir şekilde tanımlanmalı ve herhangi bir yargı veya ayrımcı yorum içermemelidir.

(2) Biyometrik veriler, INTERPOL Bilgi Sistemi'nde işlendiğinde özellikle önemli adli değere sahip ve ilgili olarak kabul edilir:

(a) Bir kişinin, kimliği belirlenmemiş bir cesedin veya insan kalıntısının kimliğini tespit etmek veya doğrulamak için;

(b) Uluslararası polis iş birliği bağlamında bir bireyin yanlış tanınmasını önlemek için ve/veya

(c) Suçlar ile suç mahalleri arasında bağlantı kurulmasını sağlamak için.

(3) Teşkilatın veri tabanlarından birine kaydedildiğinde, özellikle hassas veriler, sorgulandıklarında bu özellikleriyle tanınabilecek şekilde kaydedilmelidir.

(4) Herhangi bir özellikle hassas verinin iletimi, mevcut Kuralların 67'inci maddesine uygun olarak gerçekleştirilmelidir.

(5) Özellikle hassas veriler, hiçbir şekilde herhangi bir ayrımcı amaç için işlenemez.

Madde 43: Kopyalanan veya yüklenen verilerin kaydedilmesine ilişkin ek koşullar

(1) Teşkilatın bir polis veri tabanındaki veriler, yalnızca aşağıdaki tüm koşullar sağlandığında başka bir polis veri tabanına veya INTERPOL Bilgi Sistemi'nin bir bölümüne kopyalanabilir:

(a) Veriler aynı amaç için kopyalanıyorsa, verilerin kaynağı 10 gün içinde itiraz etmemiş olmalıdır,

(b) Veriler başka bir amaç için kopyalanıyorsa, kaynağın bu yeni amaç için işlenmesine onay vermiş olması gerekir,

(c) Verilerin kopyalanmasının, kopyalanan verilerin bütünlüğüne ve gizliliğine zarar verme olasılığı düşük olmalıdır,

(d) Veriler tam olarak kopyalanmalıdır,

(e) Veriler düzenli olarak güncellenmelidir.

(2) Genel Sekreterlik, Teşkilatın bir polis veritabanındaki veriler başka bir polis veri tabanına kopyalandığında bu ek kayıt koşullarına uyulmasını sağlayacaktır.

(3)Veriler yalnızca aşağıdaki tüm koşulların yerine getirilmesi halinde INTERPOL Bilgi Sistemine yüklenebilecektir:

(a) Yükleme, bir Ulusal Merkez Bürosu, ulusal bir birim, uluslararası bir kuruluş veya Genel Sekreterlik tarafından yapılmalı ve bu Kuralların hükümlerine uygun şekilde gerçekleştirilmelidir,

(b) Veriler eksiksiz ve tam olarak kopyalanmalıdır,

(c) Verileri yükleyen Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, verilerin düzenli olarak güncellendiğinden emin olmalıdır.

Madde 43A: Büyük veri setlerinin geçici olarak işlenmesine ilişkin ek koşullar

(1) Genel Sekreterlik, uluslararası polis işbirliği amaçları doğrultusunda potansiyel ilgiyi belirlemek ve bu Kurallara uyumlarını değerlendirmek amacıyla büyük veri kümelerini geçici olarak işleyebilir.

(2) Verilerin kaynağıyla istişare edilerek, bu geçici işleme, diğerlerinin yanı sıra, verilerin yapılandırılması, biçimlendirilmesi, değerlendirilmesi, kategorize edilmesi ve INTERPOL Bilgi Sisteminde daha önce işlenmiş verilerle karşılaştırılması dahil olabilir.

(3) Geçici işleme aşağıdaki koşulların sağlanması zorunludur:

(a) Veriler, bu Kuralların Başlık 1'inde tanımlanan genel ilkelere uygun olmalıdır,

(b) Veriler, INTERPOL Bilgi Sistemi içinde korumalı bir veri işleme ortamında işlenmelidir. Veriler diğer operasyonel veya analitik verilerden ayrı tutulmalı ve diğer kaynaklardan sağlanan verilerden ayırt edilmelidir,

(c) Bu ortamda verilerin saklama süresi, kaynağı tarafından belirlenir, ancak Yürütme Komitesi tarafından belirlenen azami saklama süresini aşamaz,

(d) Verilere erişim, özel erişim izni verilen Genel Sekreterlik birimleri veya personel üyeleri ile sınırlı olmalıdır,

(e) Verinin kaynağı tarafından belirlenen diğer tüm koşullar.

(4) Genel Sekreterlik, verilerin değerlendirilmesi sonucunda değerlendirme sonuçlarını veri kaynağına bildirir ve uygun olmayan verileri derhal siler.

(5) Verinin kaynağı, uyumlu verileri bu Kuralların 10'uncu maddesinde listelenen bir veya daha fazla işleme amacı için işleyebilir.

(6) Genel Sekreterlik, geçici işleme ortamında kalan verileri silecek ve kaynağı bilgilendirecektir.

Madde 44: Kişilerin statüsü

(1) Uluslararası polis işbirliğinin konusu olan bir kişiye ilişkin herhangi bir veriyi kaydederken, Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, söz konusu kişinin statüsünü aşağıdaki listeden belirtmelidir:

(a) Hükümlü: Bir mahkeme kararıyla, adi suç işlediği tespit edilen kişi,

(b) Sanık: Hakkında adi suç işlediği iddiasıyla cezai kovuşturma başlatılan kişi,

(c) Şüpheli: Cezai soruşturma kapsamında suç işlediği düşünülen ancak hakkında hiçbir suçlama yöneltilmemiş kişi,

(d) Sabıka kaydı: Önceki bir mahkumiyet veya aklanmamış önceki suç davranışı nedeniyle kolluk kuvvetleri tarafından bilinen kişi,

(e) Tanık: Şüpheli olmayan ve ceza soruşturması veya kayıp soruşturması ile ilgili bilgi sağlayabilecek kişi,

(f) Mağdur: Kendisine karşı suç işlenen kişi,

(g) Kayıp: Nerede olduğu bilinmeyen ve kayıp olarak bildirilen kişi,

(h) Kimliği belirsiz kişi: Suçlu olsun veya olmasın, kimliği tespit edilmeye çalışılan, hayatta olan kişi,

(i) Kimliği belirsiz ceset: Suçlu olsun veya olmasın, kimliği tespit edilmeye çalışılan ölü kişi,

(j) Ölü: Ölümünün teyidinden sonra INTERPOL polis veri tabanlarında verisi tutulan kişi;

(k) Olası tehdit: Kamu güvenliğine zarar verebilecek veya verebileceği muhtemel kişi;

l) BM yaptırımlarına tabi: Birleşmiş Milletler Güvenlik Konseyi tarafından alınan yaptırımlara tabi kişi.

(2) Genel Sekreterlik, Ulusal Merkez Büroları ve uluslararası kuruluşlarla veya bu amaçla kurulan danışma organlarındaki temsilcileriyle istişare ederek diğer statüleri belirleyebilir.

Madde 45: Verilerin kaydedilmesinde özel kullanım koşullarının tanımlanması

Mevcut Kuralların 12(1) maddesi uyarınca, veri kaydeden herhangi bir Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, bu verilerin INTERPOL Bilgi Sistemine girilmesinden sonra bunların kullanımına ilişkin koşulları ve özellikle de verilerin cezai kovuşturmalarda delil olarak kullanılmasına ilişkin koşulları belirtecektir.

Madde 46: Güncellemeler

(1) Verileri kaydeden Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş bunları düzenli olarak günceller.

(2) Verilerin kaydedildiği amaç gerçekleştiğinde, bu veriler yalnızca bunları kaydeden Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, bunların kaydedilmesi için yeni bir amaç belirleyip gerekçelendirirse, Kuruluşun polis veri tabanında güncellenebilir veya saklanabilir.

(3) Verileri güncelleyen Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, söz konusu verilerin kaydedilmesine ilişkin koşulların karşılanmasını sağlar.

(4) Verileri güncelleyen Ulusal Merkezi Büro, ulusal kuruluş veya uluslararası kuruluş, bu verilerin kaydedilme koşullarının sağlandığını temin etmelidir. Verileri kaydeden Ulusal Merkezi Büro, ulusal kuruluş veya uluslararası kuruluş ayrıca her zaman aşağıdakileri değiştirebilir:

(a) verilerin saklama süresi;

(b) gizlilik seviyesi;

(c) verilere erişim kısıtlamaları;

(d) danışma koşulları;

(e) kullanım koşulları.

Madde 47: Kamuya açık bilgilerin ve gerçek kişilerden veya kuruluşlardan alınan diğer bilgilerin kaydedilmesine ilişkin ek koşullar

(1) Kamuya açık bilgilerin ve Genel Sekreterlik, Ulusal Merkez Bürolar, uluslararası kuruluşlar veya özel birimlerle temas kuran kişilerden ya da birimlerden alınan bilgilerin kaydedilmesine aşağıdaki ek koşullar uygulanır:

(a) Bilgilerin kaydı, Teşkilatın amaç ve faaliyetleriyle uyumlu olmalı ve Teşkilatın 10(2) maddesinde tanımlanan uluslararası polis iş birliği amaçları için uygun ve ilgili olmalıdır,

(b) Bilgi, INTERPOL Bilgi Sistemi'nde hali hazırda kaydedilmiş verileri tamamladığı durumlarda, mevcut Kuralların 10(2) maddesine uygun olarak işlenecektir,

(c) Bilginin kaynağı açıkça belirtilmeli ve söz konusu bilgi, INTERPOL Bilgi Sistemi'nde kaydedilen ve Kuralların 1(2) maddesinde tanımlanan verilerden net bir şekilde ayrılacak şekilde işlenmelidir,

(d) Kaydedilmeden önce, Genel Sekreterlik bu bilgiyi bu Kuralların 11 ve 12'inci maddeleri ışığında değerlendirecektir,

(e) Genel Sekreterlik tarafından belirlenen politikalar ve mevcut Kuralların 50'inci maddesi uyarınca, bu tür bilgiler kaydedilme zamanı itibarıyla zaman damgalı olacak, ilgili şekilde güncellenecek veya düzeltilecek ve Yürütme Komitesi tarafından belirlenen azami saklama süresi sonunda otomatik olarak silinecektir,

(f) Bu bilgileri Ulusal Merkez Bürolarına, ulusal kuruluşlara, uluslararası kuruluşlara veya özel birimlere sunarken, Genel Sekreterlik bilgilerin kaynağını ve bu bilgilerin kalitesi ile güvenilirliği konusundaki değerlendirmesini açıkça belirtecektir,

(g) Genel Sekreterlikten alınan ve tamamen veya kısmen bu bilgilere dayalı rapor veya diğer çıktıları kullanmadan önce, Ulusal Merkez Büroları, ulusal kuruluşlar, uluslararası kuruluşlar veya özel birimler, yürürlükteki mevzuatlarına uygun olarak, bu çıktının dayandığı bilginin kalitesi ve güvenilirliği konusunda kendi değerlendirmelerini yapmalıdır,

(h) Bu hüküm kapsamındaki bilgiler, herhangi bir Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş tarafından zorlayıcı önlemlerin uygulanması için tek başına temel oluşturamaz.

(2) Bu Madde kapsamındaki bilgilerin kaynağı şunlar olacaktır:

(a) Genel Sekreterliktir, eğer:

(i) kamuya açık bilgiler Genel Sekreterlik tarafından veya onun girişimiyle toplanmışsa veya

(ii) bilgi, mevcut Kuralların 1(6) maddesinde belirtilen kaynaklar dışındaki kişilerden veya birimlerden geliyorsa.

(b) Mevcut Kuralların 1(6) maddesinde belirtilen kaynak, eğer söz konusu bilgi bu kaynaktan alınmışsa.

Madde 48: Ek bilgi ve düzeltmeler

(1) Verileri kaydeden dışında bir Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, verilerin yanlış olduğunu düşünmek için belirli ve ilgili nedenlere sahipse, verileri kaydeden veya ulusal kuruluşun verileri kimin adına kaydettiğini veya verileri kaydeden uluslararası kuruluşu derhal bilgilendirir.

(2) Verileri kaydeden dışında bir Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş bunları tamamlamak isterse, tamamlayıcı bilgileri Büroya veya ilgili uluslararası kuruluşa gönderebilir.

(3) Kayıt yapan Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, bilgileri derhal inceleyecek ve gerekirse verileri derhal değiştirecek, düzeltecek veya silecektir.

Madde 49: Saklama süresi

(1) Bu Kuralların 10'uncu maddesi uyarınca, veriler, yalnızca kaydedildikleri amacın gerçekleştirilmesi için gereken süre boyunca Teşkilatın polis veri tabanlarında saklanabilir.

(2) Veriler, kaynak tarafından daha kısa bir saklama süresi belirlenmediği veya amaç gerçekleşmediği takdirde, başlangıçta Yürütme Kurulu tarafından bu tür veriler için belirlenen azami süre boyunca kaydedilir.

(3) Saklama süresi, verilerin kaydedildiği tarihten itibaren başlar.

(4) Bu Kuralların 81'inci ve 100'üncü maddelerinde belirtilen işbirliği talebinin veya uyarının askıya alınması, verilerin saklama süresi üzerinde etkili olmayacaktır.

Madde 50: Periyodik değerlendirmeler

(1) Verilerin işleme amacını ve kalitesini yeniden değerlendirmek amacıyla, bu Kuralların 10'uncu ve 12'inci maddelerine uygun olarak, Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, saklama süresi dolduğunda bu verilerin saklanma gerekliliğini incelemeli ve gerekirse verilerin kaydedilme koşullarının hâlâ yerine getirilip getirilmediğini kontrol etmelidir.

(2) Genel Sekreterlik, verilerin saklanması gerekliliğini incelemek üzere, verileri kaydeden Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluştan, sürenin dolmasından en geç altı ay önce talepte bulunur.

(3) Genel Sekreterlik özellikle şunları belirleyecektir:

(a) verilerin aynı Ulusal Merkez Bürosu veya aynı birimden gelen diğer verilerle bağlantılı olup olmadığı,

(b) verilerin bir analiz projesi kapsamında işlenip işlenmediği,

(c) verilerin ciddi suç türlerinden veya Genel Kurul tarafından uygulanan özel bir saklama politikası olan özel suç alanlarından birine ilişkin olup olmadığı.

(4) Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, verileri saklamaya karar verirse, saklamanın nedenlerini belirtir.

(5) Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, verilerin kaydedilme amacının gerçekleştiğine ancak verilerin Teşkilatın polis veri tabanlarında saklanmasının uluslararası polis iş birliği amaçları açısından, özellikle de söz konusu veriler yukarıda belirtilen üç kategoriden birine aitse, ilgili olmaya devam ettiğine karar verirse, söz konusu verilerin kaydedilmesi için yeni bir amaç belirleyip gerekçelendirmelidir. Veriler, kaynak tarafından daha kısa bir saklama süresi belirlenmediği veya amaç gerçekleştirilmediği sürece, bu yeni amaç için belirlenen azami saklama süresini aşmayan ek bir süre boyunca kaydedilir.

(6) Verileri saklamaya karar veren Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, verilerin kaydedilmesine ilişkin koşulların karşılanmaya devam etmesini sağlar.

(7) Teşkilatın belirli bir veri tabanı için Yürütme Komitesi, gerektiğinde, yukarıdaki yeniden değerlendirme koşullarını muaf tutma yetkisine sahiptir.

Madde 51: Verilerin silinmesi

(1) Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, 10'uncu maddede belirtilen amaçlardan birine hizmet eden verileri saklamamaya karar verirse, bu veriler o özel amaç için silinir.

(2) Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, verilerin hizmet ettikleri amaç için saklanması gerektiğini belirtmemişse, veriler saklama süresinin sona ermesiyle otomatik olarak silinir.

(3) Verilerin kaydedilme amacı gerçekleştiğinde, verileri kaydeden Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, bunların kaydedilmesi için yeni bir amaç belirlemeye ve gerekçelendirmeye karar vermediği sürece, bunları polis veri tabanlarından siler.

(4) Genel Sekreterlik, verilerin kaydedilme amacının gerçekleştiğini veya verilerin artık kayıt için gereken asgari koşulları karşılamadığını düşünmek için belirli ve geçerli nedenlere sahip olduğunda, verileri kaydeden Ulusal Merkez Bürodan, ulusal kuruluştan veya uluslararası kuruluştan bu verilerin saklanması gerekliliğini incelemesini derhal talep eder.

(5) Genel Sekreterlik, uluslararası işbirliği talebi veya uyarı konusu olan bir kişiyle ilgili olarak bir Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş tarafından kaydedilen verileri sildiğinde, bu verileri kaydeden Ulusal Merkez Büro veya uluslararası kuruluşu bilgilendirir ve eyleminin gerekçelerini açıklar.

(6) Veriler, Kuruluşun polis veri tabanlarından birinden silindiğinde, INTERPOL Bilgi Sisteminde bulunan bu verilerin tüm kopyaları da silinir; ancak veriler, 10'uncu maddede

belirtilen ayrı bir amaç için saklanıyorsa ve verileri ilk kaydeden Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşun önceden onayı varsa silinir.

(7) Maliyet ve iş yoğunluğu nedeniyle verilerin silinmesinin mümkün olmadığı durumlarda, Genel Sekreterlik, verilerin kullanılamamasını sağlamak, bu verilere erişimi ve bunların cezai soruşturma amacıyla kullanılmasını engellemek veya verilerin var olmadığının açıkça belirtilmesi için gerekli tüm adımları atar ve bu önlemleri INTERPOL Dosyalarını Kontrol Komisyonuna bildirir.

Madde 52: Sabıka kaydının geçici olarak saklanması

(1) Hükümlü, sanık, şüpheli veya potansiyel tehdit oluşturan bir kişiyle ilgili uluslararası uyarı veya iş birliği talebini geri çeken Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, bu kişinin sabıka kaydı hakkında bilgi sağlamak amacıyla bu kişiye ait verileri geçici olarak saklamayı seçebilir.

(2) Hükümlü, sanık, şüpheli veya tehdit oluşturduğu için ilk kez veri kaydedilmesine neden olan ancak hakkındaki suçlamalardan aklanmış bir kişinin sabıka kaydının geçici olarak saklanması yasaktır.

(3) Verileri referans amaçlı saklayan Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, saklamanın ulusal mevzuat uyarınca yasal olmasını sağlar. Uluslararası kuruluş ise saklamanın kendi geçerli kuralları uyarınca yasal olmasını sağlar.

(4) Bu kaydın amacı ve ilgili kişinin statüsü, bu Kuralların sırasıyla 10 ve 44(1) maddelerine uygun olarak, söz konusu verilerin, uyarı veya uluslararası işbirliği taleplerine konu olan kişilere ilişkin verilerle karıştırılmayacak şekilde belirtilir. İlgili kişiye başlangıçta atfedilen statünün kaydı tutulur.

(5) Bu veriler, Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluşun başlangıçtaki amacın gerçekleştirildiğini bildirdiği andan itibaren Yürütme Kurulu tarafından belirlenen azami saklama süresini aşmayan bir süre boyunca saklanabilir; ancak kaynak tarafından daha kısa bir saklama süresi belirlenebilir. Saklama süresinin sona ermesi üzerine, Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş, aşağıdaki 53'üncü madde uyarınca soruları yeniden yönlendirmek amacıyla verileri saklamaya karar vermediği sürece veriler otomatik olarak imha edilir.

Madde 53: Soruşturmaların yönlendirilmesi amacıyla verilerin saklanması

(1) Şüpheli, sanık veya hükümlü bir kişi hakkında kaydettiği verileri silen Ulusal Merkez Bürosu veya kuruluş, bu kişi hakkında daha sonra kendisine yöneltilebilecek herhangi bir soruşturmayı başka bir Ulusal Merkez Bürosu veya kuruluşun kendisine yöneltmesine olanak sağlayacak veri öğelerini saklamak isteyip istemediğini belirtmelidir.

(2) Genel Sekreterlik, Ulusal Merkez Bürosu veya verileri kaydeden birimin açık izni olmaksızın, polis veri tabanlarından sildiği verileri soruşturmaların yönlendirilmesi amacıyla saklayamaz.

(3) Soruşturmaların yönlendirilmesi amacıyla saklanabilecek veriler sadece şunlardır: verileri kaydeden Ulusal Merkez Bürosu veya biriminin adı; kaydın referansı; kişinin adı ve soyadları; kimlik belgesi numarası ve bu belgenin türü; doğum tarihi ve yeri; parmak izleri ve DNA profili.

(4) Bu veriler, kaynak tarafından daha kısa bir saklama süresi belirlenmediği takdirde, Yürütme Kurulu tarafından belirlenen azami saklama süresi boyunca saklanabilir.

BÖLÜM 3: DANIŞMA

Madde 54: Doğrudan erişim

(1) Bu Kuralların 6'ıncı maddesi uyarınca, Ulusal Merkez Büroları, kaynak tarafından belirlenen kısıtlamalara ve gizlilik kurallarına tabi olarak, Teşkilatın polis veri tabanlarına doğrudan başvurabilirler. Ulusal kuruluşlar ve uluslararası kuruluşlar da, aynı kısıtlamalara ve gizlilik kurallarına tabi olarak ve kendilerine verilen erişim haklarına göre, Teşkilatın polis veri tabanlarına doğrudan başvurabilirler.

(2) Madde 36(1, n) uyarınca, doğrudan danışılabilecek veri türü, bu veri tabanının genel özellikleri listesinde belirtilir.

Madde 55: Bağlantı

Veri tabanlarının birbirine bağlanması işlemleri, aşağıdaki tüm koşulları karşılamalıdır:

(a) Bağlantının amacı, niteliği ve kapsamı belirli, açık ve Teşkilatın amaç ve faaliyetleriyle uyumlu olmalıdır,

(b) Bağlantı, uluslararası polis işbirliği amaçları açısından ilgili olmalıdır,

(c) Birbirine bağlanacak bilgi sistemi, en az INTERPOL Bilgi Sistemi ile eşdeğer bir güvenlik düzeyi sunmalıdır,

(d) Bağlantı, INTERPOL Bilgi Sistemi ve birbirine bağlanacak bilgi sisteminde yer alan verilerin kaynakları tarafından belirlenen işleme koşullarına uyumu sağlamalıdır,

(e) Bağlantı, INTERPOL Bilgi Sistemi'ne veri girişi yapan Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş ile Genel Sekreterlik'in, birbirine bağlanan verilerden uluslararası polis işbirliği amaçları için ilgili olabilecek herhangi bir unsurdan derhal haberdar edilmesini sağlamalıdır.

(2) Ulusal bir kuruluştan gelen tüm bağlantı talepleri, Ulusal Merkez Bürosu aracılığıyla gönderilmelidir.

(3) Genel Sekreterlik, tüm bağlantı taleplerini onay için Yürütme Komitesi'ne sunacaktır. Bunun için:

(a) Bağlantı talebinin bir kopyasını sunacak ve Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş da bağlantıyı denetlemekle sorumlu olacak kişiyi belirtecektir,

(b) Genel Sekreterlik tarafından yapılan talep değerlendirmesi ve bu talebin Teşkilat için finansal etkilerini sağlayacaktır,

(c) Genel Sekreterlik tarafından yürütülen herhangi bir testin sonuçlarını sunacaktır,

(d) Veri tabanı kişisel veri içeriyorsa veya kişisel verilerle bağlantılıysa, INTERPOL Dosya Kontrol Komisyonu'nun görüşünü sunacaktır.

(4) Yürütme Komitesi bağlantıya izin verirse, Genel Sekreterlik, birbirine bağlanacak veri tabanında yer alan verilerin kaynaklarını önceden bilgilendirecektir. Sekreterlik, bağlantının koşullarını belirtecektir.

(5) Genel Sekreterlik, her bir işlemin şartlarını belirten güncel bir bağlantı işlemleri sicilini tutar. Ulusal Merkez Büroları bu sicile istedikleri zaman başvurabilirler. Uluslararası kuruluşlar da kendilerine verilen erişim haklarına göre bu sicile başvurabilirler.

(6) Yürütme Kurulu, her yıl, bağlantı faaliyetleri için verdiği yetkileri Genel Kurula bildirir.

Madde 56: Uluslararası polis işbirliği amacıyla indirme

(1) Tüm veri indirme işlemleri aşağıdaki tüm koşulları karşılamalıdır:

(a) Veri indirme amacının belirli, açık ve Teşkilatın amaç ve faaliyetleriyle uyumlu olması,

(b) Talebin uluslararası polis işbirliği amaçları açısından ilgili olması,

(c) Bir bağlantı işlemi, maliyet ve birbirine bağlanacak bilgi sisteminin fonksiyonel veya teknik özellikleri nedeniyle gerçekleştirilemiyorsa,

(d) Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşun bilgi sistemi, INTERPOL Bilgi Sistemi ile en az eşdeğer bir güvenlik düzeyi sunmalıdır.

(e) İndirilen verilerin işlenmesi ve kullanımı için kaynaklar tarafından belirlenen koşullara kesinlikle uyulması,

(f) Veri indirme işleminin, altı ayı geçmeyecek şekilde belirli bir süreyle sınırlı olması,

(g) İndirilen verilerin, veri silinmesini gerektirse bile, en az haftada bir güncellenmesi,

(h) Verilerin, indirildikleri bilgi sistemi içinde kopyalanmaması,

(i) İndirilen verilerin, indirilmelerinin amacına ulaşılması durumunda ve en geç yukarıda belirtilen altı aylık sürenin sonunda sistematik olarak silinmesi,

(j) Verileri indiren Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, indirilen verilerden uluslararası polis işbirliği amaçları için ilgili olabilecek herhangi bir öğeyi, veriyi INTERPOL Bilgi Sistemi'ne kaydeden Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşa ve Genel Sekreterliğe derhal bildirecektir.

(2) Ulusal bir kuruluştan gelen tüm indirme talepleri, Ulusal Merkez Bürosu aracılığıyla gönderilmelidir.

(3) Genel Sekreterlik, aşağıdaki koşullar çerçevesinde veri indirme işlemini yetkilendirebilir:

(a) Yukarıdaki koşullara uyum,

(b) Veri indirme işlemini gerçekleştirmek isteyen Ulusal Merkez Bürosu veya uluslararası kuruluş tarafından sağlanan yazılı taahhütler; bu taahhütler, söz konusu koşullara, indirme amacına, niteliğine ve kapsamına uyulacağını garanti eder,

(c) Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşta veri indirmeyi denetlemekle sorumlu bir kişinin atanması.

(4) Genel Sekreterlik, teknik veya diğer nedenlerle, indirilecek verilere ilişkin işleme koşullarından bir veya birkaçını karşılayamıyorsa, söz konusu verilerin indirilmesine izin vermez.

(5) Genel Sekreterlik, yetkilendirdiği herhangi bir indirme işlemi hakkında Ulusal Merkez Büroları ve uluslararası kuruluşları bilgilendirir. İndirme işleminin tüm koşullarını, özellikle de indirme işlemini gerçekleştirmesi için yetkilendirdiği Ulusal Merkez Büro veya uluslararası kuruluşun bilgi sisteminin özelliklerini belirtir. Genel Sekreterlik, Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş tarafından yapılan bildirimde, INTERPOL Bilgi Sistemine girilen verilerin talep eden Ulusal Merkez Büro veya kuruluş tarafından işlenmesi olasılığına itirazını bildirmek için 15 gün süre tanınır. Belirtilen sürenin sonunda, Genel Sekreterlik, itiraz edilen veriler hariç olmak üzere, indirme işlemine devam etme yetkisine sahiptir.

(6) Genel Sekreterlik, verdiği veri indirme yetkilendirmesi hakkında İcra Komitesini bilgilendirecek ve şunları sağlayacaktır:

(a) Talebin değerlendirmesi ve Teşkilat için finansal etkileri;

(b) Verilerin indirildiği Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşun bilgi sisteminin özellikleri;

(c) Veri indirme işlemini gerçekleştirmek isteyen Ulusal Merkez Bürosu veya uluslararası kuruluş tarafından sağlanan yazılı taahhütlerin bir kopyası;

(d) İndirilen veriler kişisel veri içeriyorsa veya bu tür verilerle bağlantılıysa, INTERPOL Dosya Kontrol Komisyonunun görüşü.

(7) Genel Sekreterlik, indirmeye izin verilen süre boyunca indirme koşullarının yerine getirildiğini denetlemekle yükümlüdür ve bu denetimleri gerçekleştirmek için gerekli ve uygun tüm tedbirleri alır.

(8) Genel Sekreterlik, her indirme işleminin koşullarını belirten, indirilen verilerin bir kaydını tutar. Ulusal Merkez Büroları bu sicile istedikleri zaman başvurabilirler. Uluslararası kuruluşlar da kendilerine verilen erişim haklarına göre bu sicile başvurabilirler.

Madde 57: Dolaylı erişim

(1) Bir polis veri tabanına doğrudan başvurulamaması veya uluslararası bir kuruluşun veri tabanına yalnızca dolaylı erişimi olması durumunda, Genel Sekreterlik, söz konusu veri tabanına başvuru prosedürlerini belirler ve Ulusal Merkez Bürolarını bu konuda bilgilendirir. Ayrıca, uluslararası kuruluşlara, kendilerine verilen erişim haklarına göre bilgi verir.

(2) Bir polis veri tabanına doğrudan erişim mümkün olduğunda, Genel Sekreterlik, aşağıdaki durumlarda bu veritabanındaki verilere dolaylı erişim talebini yetkilendirebilir:

(a) Uluslararası kuruluşun doğrudan erişim hakkı yoksa veya

(b) Doğrudan erişim geçici olarak kullanılamıyorsa veya

(c) Talep özel veya karmaşıksa ve veriler doğrudan sorguyla elde edilemiyorsa.

(3) Ulusal bir kuruluştan gelen tüm dolaylı erişim talepleri, Ulusal Merkez Bürosu aracılığıyla yapılmalıdır.

(4) Dolaylı erişim talebini incelerken, Genel Sekreterlik şunları sağlamalıdır:

(a) Talebin bir Ulusal Merkez Bürosu, ulusal kuruluş, uluslararası kuruluş veya özel birim tarafından yapılmış olması,

(b) Uluslararası kuruluş veya özel birim tarafından yapılmışsa, talebin INTERPOL Bilgi Sistemine erişim için verilen amaca uygun olması,

(c) Talebin açık ve gerekçeli olması,

(d) Talebe karşılık gelebilecek verileri kaydeden Ulusal Merkez Bürosu veya uluslararası kuruluş tarafından, talepte bulunan Ulusal Merkez Bürosu, uluslararası kuruluş veya özel birim üzerinde herhangi bir erişim kısıtlaması uygulanmamış olması.

Madde 58: Erişim kısıtlamaları

(1) Bu Kuralların 7(1) maddesi uyarınca, herhangi bir Ulusal Merkez Bürosu veya uluslararası kuruluş, herhangi bir zamanda, diğer Ulusal Merkez Bürolarının, uluslararası kuruluşların veya özel kuruluşların, bir polis veri tabanına kaydettiği verilere erişimine genel kısıtlamalar getirebilir. Bir Ulusal Merkez Bürosu tarafından getirilen genel erişim kısıtlamaları, yetkilendirdiği ulusal kuruluşlar tarafından kaydedilen verilere uygulanır.

(2) Herhangi bir Ulusal Merkez Büro veya uluslararası kuruluş, herhangi bir zamanda, diğer Ulusal Büroların, uluslararası kuruluşların veya özel kuruluşların bir kişi, nesne veya olayla ilgili kayıtlı verilere erişimine ek kısıtlamalar getirebilir.

(3) Ulusal Merkez Büroları ve uluslararası kuruluşlar, yalnızca diğer Ulusal Merkez Bürolarının ulusal kuruluşlarına uygulanan erişim kısıtlamaları koyamaz. Bir Ulusal Merkez Bürosu tarafından erişime getirilen kısıtlamalar, yetkilendirdiği tüm ulusal kuruluşlar için geçerli olacaktır.

(4) Polis veri tabanına başvurmak için kullanılan yöntem ne olursa olsun, verilere erişim kısıtlamaları uygulanır.

(5) Ulusal Merkez Büro veya uluslararası bir kuruluş bir veri tabanına başvurduğunda ve aramasına uygun olabilecek verilere erişemediğinde, Genel Sekreterlik, talebi erişim kısıtlamasını koyan Ulusal Merkez Büro veya uluslararası kuruluşa iletebilir.

(6) Ulusal Merkez Büro veya uluslararası bir kuruluşun, Kuruluşun veri tabanlarından birinde kaydedilmesine yetki verdiği mesajlar, söz konusu Büro veya kuruluş tarafından aksi belirtilmediği takdirde, yalnızca ilk alıcılarıyla sınırlı kabul edilir.

(7) Genel Sekreterlik tarafından, acil durumlar, usulüne uygun olarak veya verilerin kamuya açıklanması dışında erişim kısıtlamaları kaldırılamaz.

(8) Erişim kısıtlamaları, bu Kuralların 112'nci maddesi uyarınca işlenecek gizli verilerdir.

Madde 59: Kısıtlamalara tabi verilerin açıklanması

Kısıtlamalara tabi verilerin açıklanması, yalnızca mevcut Kuralların 26(2)'inci maddesinde belirtilen acil durumlarda ve aşağıdaki prosedüre uygun olarak gerçekleştirilebilir:

(a) Genel Sekreterlik, söz konusu verileri kaydeden Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşa, 26(2)'inci maddesinde belirtilen koşulların yerine getirildiğini bildirir ve ilgili Ulusal Merkez Bürosu veya birimin kısıtlamaların kaldırılmasına itiraz etmesi için tehditle orantılı bir süre belirler,

(b) Ulusal kuruluşlara yönelik tüm kısıtlama kaldırma talepleri, ilgili Ulusal Merkez Bürosu aracılığıyla gönderilmelidir,

(c) Genel Sekreterlik tarafından belirlenen sürenin bitiminde ve verilerin kaydedildiği Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş tarafından açık bir itiraz yapılmadığı takdirde, kısıtlamalar kaldırılmış sayılır,

(d) Genel Sekreterlik, bu acil prosedürü uyguladığını mümkün olan en kısa sürede Yürütme Komitesine ve INTERPOL Dosyalarını Kontrol Komisyonuna bildirir.

Madde 60: Üçüncü kişilerin erişimi

(1) Genel Sekreterlik, veri işleme konusunda iş birliği ilişkisi kurmayı düşündüğü uluslararası kuruluşlar veya özel kuruluşlar tarafından iletilen erişim taleplerini işleme koyabilir.

(2) Polis veri tabanında bulunan verilere üçüncü bir kişi tarafından erişim talebinde bulunulması halinde, Genel Sekreterlik, söz konusu verileri ancak veri kaynağının açık ön izniyle iletebilir.

Madde 61: Verilerin kamuya açıklanması

(1) Genel Sekreterlik, kişisel verilerin işlenmesi söz konusu olduğunda, INTERPOL Bilgi Sisteminde işlenen verilerin kamuya açıklanması konusunda aşağıdaki 2'inci paragrafta belirtilen koşullara uygun olarak benimseyebileceği her türlü politika hakkında INTERPOL Dosyalarını Kontrol Komisyonunun görüşünü ister.

(2) INTERPOL Bilgi Sistemi'nde işlenen veriler ancak aşağıdaki tüm koşullar sağlanmışsa halka açıklanabilir:

(a) Açıklamanın amacı aşağıdakilerden en az biri olmalıdır:

(i) halkı uyarmak,

(ii) halktan yardım talep etmek,

(iii) uluslararası polis iş birliğini teşvik etmeyi amaçlayan diğer herhangi bir amaç,

(b) Verinin kaynağı, açıklamayı önceden yetkilendirmiş olmalı, açıklanacak veri türü, açıklama yöntemi ve olası alıcıları hakkında detaylar belirtilmiş olmalı ve kaynağın açıklamaya ilişkin özel koşulları varsa bunlar belirtilmiş olmalıdır,

(c) Açıklama, Teşkilatın amaç ve faaliyetlerine uygun olmalı ve uluslararası polis iş birliğinin konusu olan kişilerin temel haklarına saygı göstermelidir,

(d) Açıklama, Teşkilatın veya Üye ülkelerinin itibarına veya çıkarlarına zarar verecek nitelikte olmamalıdır,

(e) Açıklama, ilgili suç işleyen veya işlediği iddia edilen kişi hakkında, suçun işlendiği zamanda, verileri sisteme giren Ulusal Merkezi Büro veya uluslararası kuruluşun ülkesindeki geçerli yasaya göre reşit olmayan kişi olarak değerlendirilen kişiler hakkında olmamalıdır; bununla birlikte, söz konusu Ulusal Merkezi Büro veya uluslararası kuruluş ile Genel Sekreterlik, açıklamanın uluslararası polis iş birliği için gerekli olduğunu değerlendiriyorsa ve açıklama, ulusal yasaların ve uluslararası hukukun uygulanabilir ilkelerine uygunsa istisna yapılabilir.

(3) Bir bildirim veya içerdiği veriler, verinin kaynağı olmayan bir Ulusal Merkezi Büro, ulusal bir kuruluş veya uluslararası bir kuruluş tarafından açıklanırsa, yukarıdaki 2'inci paragrafta belirtilen koşullara ek olarak aşağıdaki koşullar da sağlanmalıdır:

(a) Genel Sekreterlik, bu tür bir açıklamayı önceden yetkilendirmiş olmalıdır,

(b) Bildirimdeki veriler birebir kopyalanmalı ve doğruluklarını korumak için düzenli olarak güncellenmelidir.

BÖLÜM 4: VERİLERİN KULLANIMI

Madde 62: Kullanım Şartları

INTERPOL Bilgi Sistemi'nde işlenen verileri kullanacak tüm Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar şunları belirleyecektir:

(a) Verilerin doğruluğu ve ilgisi;

(b) Verileri kullanma amaçlarını;

(c) Herhangi özel kullanım koşullarını;

(d) Bu veriler üzerinde başka bir Ulusal Merkez Bürosu veya iletilecekleri başka bir uluslararası kuruma uygulanacak herhangi bir erişim kısıtlaması.

Madde 63: Verilerin doğruluğunun ve uygunluğunun doğrulanması

(1) INTERPOL Bilgi Sisteminde işlenen verileri, gözaltı, tutuklama veya hareket kısıtlaması dahil ancak bunlarla sınırlı olmamak üzere zorlayıcı önlemler uygulamak amacıyla kullanacak olan tüm Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, bu verilerin hâlâ doğru ve ilgili olduğundan emin olmalıdır. Yukarıda belirtilenlere bakılmaksızın, ulusal mevzuat ve yürürlükteki uluslararası anlaşmalar kapsamında izin verilen bu tür önlemler, veri doğrulama süreci gerçekleştirilmeden önce veya gerçekleştirilirken alınabilir.

(2) Ulusal Merkez Bürosu, gerekli kontrolleri, verileri kaydeden Ulusal Merkez Bürosu ile doğrudan veya veriler ulusal bir kuruluş tarafından kaydedilmişse bu ulusal kuruluşun Ulusal Merkez Bürosu ile birlikte yürütür. Verilerin uluslararası bir kuruluş tarafından kaydedilmesi halinde, Genel Sekreterlik nezdinde gerekli kontroller yapılır.

(3) Bir ulusal kuruluş, bu kontrolleri kendi Ulusal Merkez Bürosu aracılığıyla gerçekleştirecektir.

(4) Bir uluslararası kuruluş, bu kontrolleri yalnızca Genel Sekreterlik aracılığıyla, ilgili Ulusal Merkez Bürosu veya uluslararası kuruluşla gerçekleştirecektir; aksi takdirde kendisine erişim hakkı verilmişse doğrudan erişim kullanabilir.

Madde 64: Verilerin ceza soruşturması amacı dışında veya idari amaçla kullanılması

(1) Bu Kuralların 10(6) maddesi uyarınca, Teşkilatın polis veri tabanlarında veriler başlangıçta kaydedildikleri uluslararası polis iş birliği amacından farklı bir cezai soruşturma amacıyla veya verilerin kaynağı tarafından aşağıdaki (2)'inci paragraf uyarınca belirtilen idari bir amaç için ya da böyle bir belirleme yoksa verileri kullanmayı amaçlayan birimin geçerli yasalarına göre kullanılacaksa, tüm Ulusal Merkezi Bürolar, ulusal kuruluşlar veya uluslararası kuruluşlar, bu amaç ve kullanımın şunları sağladığından emin olmalıdır:

(a) Teşkilatın amaç ve faaliyetleri ile uyumlu olduğunu,

(b) İlk amaçla çelişmediğini,

(c) Geçerli yasalar çerçevesinde yasal olduğunu,

(2) Her veri kaynağı, bu Kuralların 10(2)'inci maddesinde listelenenler dışında, hangi amaçların kendi yürürlükteki hukuku uyarınca idari amaç olarak kabul edileceğini belirtme hakkına sahip olacaktır.

(3) Yukarıdaki (1)'inici paragraf uyarınca verileri kullanmayı planlayan Ulusal Merkez Büroları veya diğer birimler, veri kaynağını önceden bilgilendirmek zorunda olup bunun şekli şu şekilde olacaktır:

(a) Bir Ulusal Merkez Bürosu, verileri kaydeden Ulusal Merkez Bürosunu veya veriler bir ulusal kuruluş tarafından kaydedilmişse o ulusal kuruluşun Ulusal Merkez Bürosunu doğrudan bilgilendirecektir. Veriler bir uluslararası kuruluş tarafından kaydedilmişse Genel Sekreterliği bilgilendirecektir,

(b) Bir ulusal kuruluş, verileri kaydeden Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, kendi Ulusal Merkez Bürosu aracılığıyla bilgilendirecektir,

(c) Bir uluslararası kuruluş, verileri kaydeden Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş Genel Sekreterlik aracılığıyla bilgilendirecektir; yetkili soruşturma ve kovuşturma yetkisine sahip uluslararası kuruluşlar, Madde 27(5, f) uyarınca verileri doğrudan mesaj olarak göndermeye yetkilendirilmişse bu madde uygulanmaz.

(4) Bildirim tarihinden itibaren, veri kaynağı, söz konusu verilerin öngörülen amaç için kullanılmasına itirazını belirtmek veya ek bilgi veya ek süre talep etmek için 10 gün süreye sahiptir. Bu süre, acil durumlarda Genel Sekreterlik tarafından kısaltılabilir.

Madde 65: İdari amaçlarla veri kullanımı [silinmiştir]

Madde 66: Kullanıma ilişkin özel koşullar

(1) Bu Kuralların 45'inci maddesi uyarınca, herhangi bir veriye başvurulması halinde Genel Sekreterlik, verilerin kaydedildiği tarihte Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluş tarafından belirlenen özel kullanım koşullarına, özellikle de ceza muhakemesinde delil olarak kullanılmasına ilişkin koşullara dikkat çeker.

(2) Polis veri tabanında kayıtlı verileri kullanacak olan herhangi bir Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, bunları kaydeden Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş tarafından belirlenen özel kullanım koşullarına uyacaktır.

(3) Genel Sekreterlik, verileri inceleyen herhangi bir Ulusal Merkez Büro, ulusal kuruluş veya uluslararası kuruluşun, söz konusu özel kullanım koşullarından haberdar olmasını sağlayarak, bunların gözetilmesini sağlamak için gerekli tedbirleri almasını sağlar.

Madde 67: Verilerin iletilmesi

(1) Bir Ulusal Merkez Bürosu veya uluslararası kuruluş, Teşkilatın polis veri tabanlarında bulunan veya bir mesaj yoluyla alınan verileri başka bir Ulusal Merkez Bürosuna veya uluslararası kuruluşa iletmeden önce, bu verilerin kısıtlamalara tabi olup olmadığını teyit etmek için Genel Sekreterlik veya verileri kaydeden ya da mesaj yoluyla gönderen Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş ile kontrol yapmalıdır:

(a) Bir Ulusal Merkez Bürosu, gerekli kontrolleri verileri kaydeden veya gönderen Ulusal Merkez Bürosu ile doğrudan yapar veya veriler bir ulusal kuruluş tarafından kaydedilmiş veya gönderilmişse, bu ulusal kuruluşun Ulusal Merkez Bürosu ile kontrol sağlar. Veriler bir uluslararası kuruluş tarafından kaydedilmiş veya gönderilmişse, gerekli kontrolleri Genel Sekreterlik ile yapar.

(b) Bir uluslararası kuruluş, gerekli kontrolleri yalnızca Genel Sekreterlik aracılığıyla yapar; ancak, ceza soruşturma ve kovuşturma yetkisine sahip ve mevcut Kuralların 27(5, f)'inci maddesi uyarınca verileri doğrudan mesaj yoluyla gönderme yetkisi verilmiş bir uluslararası kuruluş için bu durum geçerli değildir.

(2) Teşkilatın polis veri tabanlarında bulunan veya kendisine bir mesaj yoluyla iletilmiş özellikle hassas verileri iletmeden önce, bir Ulusal Merkez Bürosu, uluslararası kuruluş veya Genel Sekreterlik, iletilecek verilerin Teşkilatın amaçlarını gerçekleştirmek için ilgili ve özellikle önemli kriminalistik değere sahip olduğundan ve işleme amaçları doğrultusunda (Madde 10(2)) kesinlikle gerekli olduğundan emin olmalıdır.

(3) Veri iletirken, Ulusal Merkez Bürosu veya uluslararası kuruluş ile Genel Sekreterlik, dolaylı erişim durumlarında aşağıdakileri belirtmelidir:

(a) Verilerin kaynağı;

(b) Kaynak tarafından belirlenen özel kullanım koşulları;

(c) Verilerin gizlilik seviyesi;

(d) Verilerin kaydedildiği tarih ve polis veri tabanlarındaki saklama süresi;

(e) Kişisel veri söz konusu ise kişinin statüsü ve kendisi hakkında alınacak işlem türü;

(f) Verilerin işlenmesine ilişkin özel yöntemler.

(4) Gerektiğinde veya kaynağın talebi üzerine, iletilen verilerin tam bir kopyası verilerin kaynağına gönderilmelidir.

(5) Mevcut Kuralların 58(6)'inci maddesi uyarınca, Genel Sekreterlik, önceden izin alınmadan bir mesajı asıl gönderen Ulusal Merkez Bürosu veya uluslararası kuruluşun dışında başka bir Ulusal Merkez Bürosuna veya uluslararası kuruluşa iletemez.

BÖLÜM 5: SUÇ ANALİZİ DOSYALARIYLA İLGİLİ ÖZEL KURALLAR

Madde 68: Analiz dosyaları

(1) Analiz dosyaları, bu Kuralların 36(1)'inci maddesi temelinde ve ilgili suç analizi projesinde yer alabilecek Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlarla istişare edilerek hazırlanan genel özellikler listesine uygun olarak suç analizi amaçlarıyla oluşturulan geçici veri tabanlarıdır.

(2) Analiz dosyalarına, bu Kurallarda belirtilen Teşkilatın veri tabanlarına veri kaydedilmesine ilişkin işleme ilkeleri ve koşulları, aşağıdaki hükümlere tabi olmak üzere uygulanır.

(3) Analiz dosyaları, Genel Sekreterlik tarafından en fazla beş yıllık bir başlangıç süresi için oluşturulur.

(4) Genel Sekreterlik, bir analiz dosyasının oluşturulmasını içeren herhangi bir suç analiz projesi hakkında Yürütme Komitesini bilgilendirir ve şunları sağlar:

(a) Bu projeyi geliştirmeye yönelten gerekçeler ile projenin mali sonuçları,

(b) Projeye dahil olabilecek Ulusal Merkez Bürolar, ulusal kuruluşlar ve uluslararası kuruluşların listesi,

(c) Analiz dosyasının hukuki çerçevesini oluşturan genel özelliklerin listesi,

(d) Analiz dosyası kişisel veriler içeriyorsa veya bu verilerle bağlantılıysa, INTERPOL Dosyalarının Kontrol Komisyonu görüşü.

(5) Yürütme Kurulu, bu Kurallarda belirtilen şartların sağlanmadığını düşünürse, analiz dosyasının oluşturulmasını reddedebilir veya iptal edebilir.

(6) Analiz dosyasının oluşturulması, amacı ve geçerli yasal çerçeve, projede yer alabilecek Ulusal Merkez Bürolarına ve uluslararası kuruluşlara derhal bildirilir. Bir Ulusal Merkez Büro, ulusal bir kuruluş veya uluslararası bir kuruluşun suç analizi projesine daha sonra katılımı, projede hali hazırda yer alan tüm Ulusal Merkez Bürolarının uluslararası kuruluşlarının onayına tabidir.

(7) Ulusal Merkez Büroları, ilgili ulusal kuruluşlara gerekli bildirimleri yapmaktan sorumludur.

(8) Genel Sekreterlik, analiz dosyasının beş yılı aşmayan bir süre için uzatılmasına ilişkin teklifi, onay için Yürütme Kuruluna sunar.

Madde 69: Analiz dosyalarının kullanımı

(1) Analiz dosyalarına erişim, suç analizine katılan ve kendilerine özel erişim izni verilen Genel Sekreterliğin yetkili birimleri veya personeli ile sınırlıdır.

(2) Genel Sekreterlik, gerektiğinde, projeye katılan ve suç analizine dahil olan Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşların personeline, belirli bir analiz dosyasına erişim yetkisi verme ve erişim ve işleme haklarının kapsamını belirleme yetkisine sahiptir. Erişim ve işleme hakları, ilgili Ulusal Merkez Büroları ile istişare edilerek ulusal kuruluşların personeline verilir.

(3) Analiz dosyaları, söz konusu dosyaların amacına ve gerekli güvenlik ve gizlilik koşullarına bağlı olarak Teşkilatın polis veri tabanlarına bağlanabilir veya bağlanmayabilir.

(4) Bir analiz dosyasına kaydedilen veriler Teşkilatın bir veri tabanına kopyalanabilir veya tam tersi olarak, Teşkilatın bir veri tabanına kaydedilen veriler, söz konusu verilerin belirtilen veri tabanına bilgi kaydı için asgari koşulları sağlaması ve kopyalamanın verileri sağlayan Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşun açık onayına tabi olması şartıyla bir analiz dosyasına kopyalanabilir.

(5) Bir analiz dosyasında kayıtlı veriler veya diğer bilgi öğeleri, Teşkilatın diğer veri tabanlarından birinde veya birkaçında güncelleme yapılmasına olanak sağlayacak nitelikteyse veya tersine, diğer veri tabanlarında kayıtlı veriler bir veya birkaç analiz dosyasında güncelleme yapılmasına olanak sağlayacak nitelikteyse, Genel Sekreterlik bu amaçla tüm uygun önlemleri almalıdır

Madde 70: Suç analizi amacıyla veri kaydına ilişkin ek koşullar

(1) Bu Kuralların 1(2)'inci maddesinde belirtilen veriler ve suç analizi için gerekli olabilecek, kamuya açık bilgiler de dahil olmak üzere diğer bilgi öğeleri analiz dosyalarına kaydedilebilir.

(2) Analiz dosyalarında kayıtlı veriler ve diğer bilgi öğeleri, kaynak tarafından daha kısa bir saklama süresi belirlenmediği veya bunları içeren suç analiz dosyası daha erken kapatılmadığı takdirde, Yürütme Kurulu tarafından belirlenen azami saklama süresi boyunca saklanır.

(3) Veriler hem analiz dosyasında hem de Teşkilatın polis veri tabanlarından birinde kayıtlı ise, verilerin kaydedilme amaçları, verilerin karıştırılmasına yol açmayacak şekilde belirtilir.

(4) Uluslararası polis iş birliği kapsamında olan bir kişiyle ilgili herhangi bir veri veya diğer bilgi öğesi bir analiz dosyasına kaydedildiğinde, o kişinin statüsü aşağıdaki listeye atıfta bulunularak belirtilir, bu liste yalnızca suç analizi bağlamında kullanılır:

(a) Bu Kuralların Madde 44(1)'inde listelenen statüler,

(b) Bu Kuralların Madde 44(2)'sinin uygulanmasıyla oluşturulan diğer statüler:

(i) Bağlantılı Kişi: Suç soruşturmasında ilgilenilen kişiyle zaman zaman veya düzenli olarak temas halinde olan ve/veya aleyhine ceza davası açılmış kişi,

(ii) İlgili Kişi: Adi suçlar hakkında bilgi sağlayabilecek kişi.

Madde 71: Suç analiz raporları

(1) Analiz dosyaları için hazırlanan suç analizi raporları şunları sağlamalıdır:

(a) Genel Sekreterlik tarafından elde edilen bilgiler ile Genel Sekreterlik'in bu bilgilerden çıkardığı sonuçlar arasında net bir ayrım yapmak,

(b) Alıntılanan bilgilerin kaynaklarını, bahsedilen kişilerin statülerini ve analizin yapıldığı tarihi belirtmek,

(c) Bu raporların ve içerdiği veri ve diğer bilgi öğelerinin herhangi bir kullanımından önce, Genel Sekreterlik ve veri kaynaklarının, ilgili hak ve kısıtlamaları belirlemek amacıyla sorgulanması gerektiğini belirtmek,

(d) Genel Sekreterlik'in bu bilgilerden çıkardığı herhangi bir bilgi veya sonucun tamamen veya kısmen kamuya açık bilgilere dayandığı durumlarda, söz konusu bilgilerin zaman damgasını ve kaynağını belirtmek.

(2) Suç analizi raporları, ilgili suç analizi projesine katılan Ulusal Merkez Bürolarına, ulusal kuruluşlara ve uluslararası kuruluşlara açıklanır. Suç analizi raporları, Genel Sekreterliğin izni ve raporlarda yer alan verilerin kaynaklarına göre belirlenebilecek erişim kısıtlamaları saklı kalmak üzere diğer Ulusal Merkez Bürolarına, ulusal kuruluşlara ve uluslararası kuruluşlara açıklanabilir. Açıklama, Genel Sekreterlik tarafından analiz dosyasına atanan gizlilik düzeyine ve diğer geçerli güvenlik önlemlerine uygun olmalıdır.

(3) Suç analiz raporları, ilgili analiz projesinin tamamlanmasından sonra Yürütme Kurulu tarafından belirlenen azami saklama süresi boyunca, bu Kurallarda belirtilen işleme kurallarına uygun ve ilgili bir şekilde kullanılması koşuluyla saklanabilir.

Madde 72: Suç analiz projelerinin tamamlanması

(1) Bir suç analiz projesi tamamlandığında:

(a) İlgili analiz dosyaları ile bunlara kaydedilen veri ve diğer bilgi öğeleri imha edilmelidir;

(b) Suç analizi raporu, mevcut Kurallarda belirtilen veri işleme kurallarına aykırı veya ilgili olmayan herhangi bir kullanımın önlenmesi için gerekli önlemler alınmak kaydıyla muhafaza edilebilir.

(2) Bir suç analiz raporunun veya içerdiği herhangi bir verinin ifşası, kaynakları tarafından içerdiği veriler üzerinde uygulanabilecek kısıtlamalara ve güvenlik veya gizlilikle ilgili diğer önlemlere uygun olmalıdır.

BÖLÜM II:

BÜLTENLER VE DİFÜZYONLAR

BÖLÜM 1:

BÜLTENLERLE İLGİLİ ORTAK HÜKÜMLER

Madde 73: INTERPOL bülten sistemi

(1) INTERPOL bülten sistemi, belirli amaçlar için yayımlanan bir dizi renk kodlu bültenden ve önceki bülten kategorilerinde yer almayan belirli bir işbirliği çerçevesinde yayımlanan özel bültenlerden oluşur.

(2) Bülten veya özel bülten kategorisi, ancak Genel Kurul'un onayıyla oluşturulabilir; bülten kişisel veriler içeriyorsa veya kişisel verilerle bağlantılıysa, INTERPOL Dosyalarının Kontrol Komisyonu'nun görüşü alınmış olmalıdır.

(3) Bültenlerin yayımlanmasına ilişkin koşullar, her bir ilan veya özel ilan kategorisi için tanımlanmıştır. Bu koşullar, söz konusu verilerin Teşkilatın veri tabanlarına kaydedilmesi için gereken genel koşullarla en azından aynıdır.

(4) Her bir bülten kategorisinin yayımlanmasına ilişkin koşullar aşağıda tanımlanmıştır. Her bir özel bülten kategorisinin yayımlanmasına ilişkin koşullar belirtilmiştir.

Madde 74: Genel Sekreterliğin Rolü

(1) Genel Sekreterlik, Teşkilat adına INTERPOL bültenlerinin yayımlanmasından sorumludur.

(2) Özellikle, şunlardan sorumludur:

(a) Tüm bülten taleplerinin mevcut Kurallara uygunluğunu kontrol etmek ve uygun bulduğu bülten taleplerini en kısa sürede yayımlamak,

(b) Yayımlanan bültenleri, Ulusal Merkez Bürolar, ulusal kuruluşlar ve uluslararası kuruluşlar tarafından verilen erişim haklarına göre doğrudan sorgulanabilmesi için eş zamanlı olarak Teşkilatın bir veri tabanına kaydetmek;

(c) Tüm bültenleri, Genel Kurul tarafından kararlaştırılan yönergelere uygun olarak Teşkilatın çalışma dillerine çevirmek;

(d) Olumlu sorgu sonucunda Ulusal Merkez Bürolar ve uluslararası kuruluşlara yardım sağlamak;

(e) Yayımlanan bültenlerin yayımlanma koşullarına uygunluğunu sürdürmesini ve bunların yayımlanmasını talep eden Ulusal Merkez Bürosu veya uluslararası kuruluş tarafından düzenli olarak değerlendirilmesini sağlamak. Bu amaçla, Genel Sekreterlik yayımlanan bültenleri düzenli olarak gözden geçirir ve yayımlanmalarını talep eden Ulusal Merkez Bürolar ve uluslararası kuruluşların yanı sıra diğer Ulusal Merkez Bürolarla istişare eder.

Madde 75: INTERPOL bültenlerinin yapısı

(1) Genel Sekreterlik, Ulusal Merkez Büroları veya bu amaçla kurulan danışma organlarındaki temsilcileriyle istişare ederek, her bir bülten kategorisinin yapısını, bunların yayımlanmasına ilişkin koşullara ve Genel Kurul veya Yürütme Kurulu tarafından alınan diğer yönerge veya kararlara uygun olarak tanımlar ve gerektiğinde değiştirir.

(2) Bu Kuralların 1'inci Başlığında belirtilen ilkelere halel gelmeksizin, uluslararası kuruluş ve Teşkilat, özel bültenlerin yapısını bir anlaşmayla tanımlar.

(3) Bir bülten, tüm aşağıdaki koşullar sağlandığında farklı kaynaklardan veri içerebilir:

(a) Kaynaklar işleme yapılmasına onay vermiş olmalıdır;

(b) İşleme, bu iş birliği talebi veya uyarısı için talepte bulunan Ulusal Merkez Bürosu veya uluslararası kuruluş açısından özel bir öneme sahip olmalıdır;

(c) Veriler, farklı kaynaklar tarafından sağlandığı açıkça belirtilmiş olmalıdır;

(d) İşleme, önemli ek maliyetler doğurmamalıdır.

Madde 76: Bültenin yayımlanmasına ilişkin talepler

(1) Bülten talepleri, Teşkilatın çalışma dillerinden en az birinde yapılır.

(2) Bir bültenin yayımlanmasını talep etmeden önce, Ulusal Merkez Bürosu veya uluslararası kuruluş şunları sağlamalıdır:

(a) Talebini destekleyen verilerin kalitesi ve yasallığı,

(b) Yayımlama talebine ilişkin koşulların karşılanmış olması,

(c) Verilerin uluslararası polis iş birliği amacıyla ilgili olması,

(d) Talebin INTERPOL kurallarına uygun olması, özellikle Anayasa'nın 2(1) ve 3'üncü maddeleri ile talepte bulunan birime uluslararası hukuk uyarınca yüklenen yükümlülüklere uyum sağlaması.

Madde 77: Genel Sekreterlik tarafından taleplerin incelenmesi

(1) Tüm bülten talepleri, bu Kurallara uygunluk açısından Genel Sekreterlik tarafından incelenir.

(2) Genel Sekreterlik, aşağıdaki durumlarda Kuruluş adına bir bülten yayımlayamaz:

(a) sağlanan veriler bir bildirimin yayımlanması için gereken koşulları karşılamıyor,

(b) bültenin yayımlanması, söz konusu durumda, uluslararası polis iş birliği amaçları açısından ilgili değildir. Bu ilgi, talebin Teşkilatın tüm Üyeleri tarafından işleme alınabilme olasılığı göz önünde bulundurularak değerlendirilmektedir;

(c) duyurunun yayımlanması, Teşkilatın veya Üyelerinin çıkarlarına zarar verebilir.

(3) Bildirim talepleri Genel Sekreterlik tarafından incelenirken, geçici olarak Teşkilatın veri tabanında kayıt altına alınır. Başvuru sırasında bu taleplerin bildirim olarak tanımlanabilmesi ve yayımlanmış bildirimlerle karıştırılmaması için ek bir açıklama eklenmelidir.

Madde 78: Eksik veya uygun olmayan bülten talepleri

(1) Talep eksik olduğunda, talepte bulunan Ulusal Merkez Büro veya uluslararası kuruluş, Genel Sekreterliğe danıştıktan sonra en kısa sürede, bültenin yayımlanması için gerekli tüm ek verileri sağlar.

(2) Genel Sekreterlik, talep edilen bültenin yayımlanmasına olanak sağlamak için sağlanan verilerin yetersiz olması ancak başka bir bildirinin yayımlanmasının amaç ve koşullarına uyması halinde, mümkün olduğu takdirde, talep eden Ulusal Merkez Büroya veya uluslararası kuruluşa başka bültenlerin yayımlanmasını önerir.

(3) Genel Sekreterlik, talep edilen bültenin Teşkilatın tüm Üyelerine yönelik olmaması veya sağlanan verilerin talep edilen bültenin yayımlanması için yeterli olmaması ancak bir difüzyonun kaydedilmesinin amacına ve koşullarına uyması durumunda, mümkün olduğu takdirde, talep eden Ulusal Merkez Büroya veya uluslararası kuruluşa bir difüzyonun dağıtılmasını önerir.

Madde 79: Bültenlerin yayımlanması

(1) Bültenler, tüm Ulusal Merkez Büroların dikkatine sunulmak üzere Genel Sekreterlik tarafından aşağıdaki şekilde yayımlanır:

(a) Ulusal Merkez Bürolar, bir bültenin yayımlandığı gün yayımlanmasından haberdar edilir;

(b) Ulusal Merkez Bürolar, mevcut Kuralların 129'uncu maddesinde belirtilen geçici önlemlere tabi olmak kaydıyla, yayımlanan tüm bültenleri Teşkilatın bir polis veri tabanında doğrudan sorgulayabilir.

(2) Bültenleri ayrıca şunlar da sorgulayabilir:

(a) Kendi Ulusal Merkez Büroları tarafından kendilerine verilen erişim yetkilerine göre ulusal kuruluşlar;

(b) Teşkilat ile yapılan anlaşmada açıkça öngörülmüşse uluslararası kuruluşlar.

(3) Mevcut Kuralların 58'inci maddesine bakılmaksızın, bülten talep eden herhangi bir Ulusal Merkez Bürosu veya uluslararası kuruluş, bültenleri inceleme yetkisi verdiği herhangi bir Ulusal Merkez Bürosu veya ulusal kuruluşun sağladığı verilere erişimini kısıtlamamayı kabul eder. Cezai konularda soruşturma ve kovuşturma yetkisi olmayan uluslararası kuruluşların sağladığı verilere erişimini kısıtlama olanağını saklı tutar.

Madde 80: Bültenlerin uygulanması

(1) Ulusal Merkez Bürolar şunları iletmelidir:

(a) Aldıkları bültenlerde yer alan tüm verileri ve bu bültenlerle ilgili güncellemeleri, mümkün olan en kısa sürede ve ulusal yasalarına uygun olarak tüm ilgili ulusal mercilere,

(b) Bültenlerin yayımlanmasını talep eden Ulusal Merkez Bürosu veya uluslararası kuruluşa ve Genel Sekreterlik'e, bültenin yayımlandığı kişi veya amaca ilişkin mevcut tüm verileri, özellikle bu verilerin bültenin amacının gerçekleştirilmesini sağlayabilecek nitelikte olduğu durumlarda. Bir ulusal kuruluş, bu verileri kendi Ulusal Merkez Bürosu aracılığıyla sunmalıdır,

(c) Genel Sekreterlik'e, bir bültenin mevcut Kurallara uygunluğu hakkında şüphe doğurabilecek herhangi bir bilgiyi,

(2) Bülteni ilk talep eden Ulusal Merkez Bürosu veya uluslararası kuruluş şunları yapmalıdır:

(a) Bültende yer alan verilerin doğruluğunu ve ilgililiğini sürdürmeye devam etmek;

(b) Yayımlanan bültenin içeriğini değiştirecek herhangi bir veriyi Genel Sekreterlik'e iletmek ve bu değişikliklerin söz konusu bültenin geri çekilmesini gerektirip gerektirmediğini değerlendirmek.

Madde 81: Bir bültenin askıya alınması, geri çekilmesi veya iptali

(1) Talepte bulunan Ulusal Merkez Büro veya uluslararası kuruluş, işbirliği talebini veya uyarısını altı ayı aşmayan bir süre için askıya alabilir. Bu askıya almanın nedenlerini Genel Sekreterliğe bildirir ve Genel Sekreterlik de bildirimi askıya alır.

(2) Bülteni talep eden Ulusal Merkez Bürosu veya uluslararası kuruluş, iş birliği talebini veya uyarısını geri çekmeli ve Genel Sekreterlik'ten bülteni derhal iptal etmesini talep etmelidir:

(a) Bu talep veya uyarının amacı gerçekleştirilmişse,

(b) Bu talep veya uyarı, amacı gerçekleştirilmiş bir veya birkaç diğer talep veya uyarıyla bağlantılıysa ve bunlar olmadan sürdürülemezse,

(c) Artık talebi sürdürmek istemiyorsa,

(d) Bülten artık yayımlanma koşullarını karşılamıyorsa,

(3) Genel Sekreterlik, bir bülteni iptal eder, eğer:

(a) Bültenin yayımlanmasına dayanak oluşturan iş birliği talebi veya uyarının amacı gerçekleştirilmiş ve bu bilgi ilgili Ulusal Merkez Bürosu veya uluslararası kuruluş tarafından doğrulanmışsa,

(b) Bu talep veya uyarı, amacı gerçekleştirilmiş bir veya birkaç diğer talep veya uyarıyla bağlantılıysa ve bunlar olmadan sürdürülemezse,

(c) Bülten artık yayımlanma koşullarını karşılamıyorsa,

(d) Bülteni talep eden Ulusal Merkez Bürosu veya uluslararası kuruluş, gerekli işlemi gerçekleştirmesine olanak tanıyacak verilere sahip olmasına rağmen herhangi bir adım atmamışsa ve istişare edildikten sonra, eylemsizliğine makul bir gerekçe sunmamışsa.

BÖLÜM 2: KIRMIZI BÜLTENLERE İLİŞKİN ÖZEL HÜKÜMLER

Madde 82: Kırmızı bültenlerin amacı

Kırmızı bültenler, aranan bir kişinin yerinin bulunması, yakalanması, gözaltına alınması veya hareketlerinin kısıtlanması amacıyla iade, teslim veya benzeri yasal bir işlem amacıyla Ulusal Merkez Bürosu veya cezai konularda soruşturma ve kovuşturma yetkisine sahip uluslararası kuruluşun talebi üzerine yayımlanır.

Madde 83: Kırmızı bültenlerin yayımlanmasına ilişkin özel koşullar

(1) Asgari kriterler

(a) Kırmızı bültenler yalnızca aşağıdaki kümülatif kriterler karşılandığında yayımlanabilir:

(i) Suç, ağır bir suç olmalıdır.

Kırmızı bültenler aşağıdaki suç kategorileri için yayımlanamaz:

- Çeşitli ülkelerde davranışsal veya kültürel normlarla ilgili tartışmalı konular doğuran suçlar;
- Aile/özel yaşamla ilgili suçlar;
- İdari nitelikteki kanun veya tüzük ihlallerinden veya özel uyuşmazlıklardan doğan suçlar, ancak suç teşkil eden fiilin ağır bir suçun işlenmesini kolaylaştırmaya yönelik olması veya organize suçla bağlantılı olduğundan şüphelenilmesi halinde.

  Genel Sekreterlik, yukarıdaki kategorilere giren belirli suçların bir listesini tutar, günceller ve Ulusal Merkez Bürolar ile uluslararası kuruluşlarla paylaşır.

(ii) Ceza eşiği:

- Kişi kovuşturma amacıyla aranıyorsa, suçu oluşturan davranış en az iki yıl hapis veya daha ağır bir ceza ile cezalandırılabilir,
- Kişi cezasını çekmek üzere aranıyorsa, en az altı ay hapis cezasına çarptırılmış olmalı ve/veya cezanın en az altı aylık kısmı henüz infaz edilmemiş olmalıdır.

(iii) Talep, uluslararası polis iş birliği amacıyla ilgilidir.

(b) Genel Sekreterlik, (i) ve/veya (ii) kriterleri karşılanmasa bile, talepte bulunan Ulusal Merkez Bürosu veya uluslararası kuruluş ile istişare sonrasında, talep edilen kırmızı bültenin yayımlanmasının uluslararası polis iş birliği açısından özel önem taşıdığı kanaatine varırsa, kırmızı bülteni yayımlamaya karar verebilir.

(c) Birden fazla suç: Talep birden fazla suçu içeriyorsa, kırmızı bülten, en az bir suç yukarıdaki kriterleri karşılamak koşuluyla INTERPOL Kurallarına uygun olan tüm suçlar için yayımlanabilir.

(2) Asgari veriler

(a) Kimlik bilgileri: Kırmızı bültenler yalnızca yeterli ayırt edici bilgiler sağlandığında yayımlanabilir. Yeterli bilgiler, aşağıdaki iki kombinasyondan en az birini içermelidir:

(i) Soyadı, adı, cinsiyet, doğum tarihi (en az yılı) ve aşağıdaki tanımlayıcılardan biri:

- Fiziksel tanım veya
- DNA profili veya
- Parmak izleri veya
- Kimlik belgelerinde yer alan veriler (ör. Pasaport, ulusal kimlik kartı).

(ii) İyi kalitede bir fotoğraf ile bazı ek veriler (ör. Takma ad, ebeveyn(ler)in adı, ek fiziksel tanım, DNA profili, parmak izleri vb.).

(b) Adli veriler:

Kırmızı bültenler yalnızca yeterli adli veriler sağlandığında yayımlanabilir. Yeterli adli veriler, en az şunları içermelidir:

(i) Olay özetleri: Aranan kişinin suç faaliyetlerini özlü ve net bir şekilde açıklayan, iddia edilen suçun zamanı ve yerini de içeren vaka özetleri,

(ii) Suçlamalar,

(iii) Suçu kapsayan yasa (mümkünse ve ulusal yasalar veya uluslararası kuruluşun, talepte bulunan Ulusal Merkez Bürosu veya uluslararası kuruluşun işleyiş kuralları uyarınca, ilgili ceza hükmünün metni sağlanmalıdır),

(iv) Verilebilecek azami ceza, verilen ceza veya infaz edilmesi gereken ceza süresi,

(v) Geçerli bir yakalama emri veya aynı etkiye sahip adli karara atıf (mümkünse ve ulusal yasalar veya uluslararası kuruluşun, talepte bulunan Ulusal Merkez Bürosu veya uluslararası kuruluşun işleyiş kuralları uyarınca, yakalama emri veya adli kararın bir kopyası sağlanmalıdır).

Madde 84: Talepte bulunan Ulusal Merkez Bürosu veya uluslararası kuruluş tarafından verilen güvenceler

Talepte bulunan Ulusal Merkez Bürosu veya uluslararası kuruluş şunları sağlamalıdır:

(a) Yakalama emrini veren veya adli kararı veren merciin gerekli yetkiye sahip olduğunu,

(b) Kırmızı bülten talebinin, kişinin yakalanması halinde iadenin talep edileceğine dair güvenceler verilmek kaydıyla, iade işlemlerinden sorumlu ilgili mercilerle koordine edildiğini ve bunun ulusal yasalar ve/veya geçerli ikili ve çok taraflı anlaşmalara uygun olduğunu;

(c) Yakalama emri bir adli merci tarafından verilmemişse, talepte bulunan ülkenin yasaları veya uluslararası kuruluşun işleyiş kuralları uyarınca, bir adli merci önünde temyiz mekanizmasının öngörüldüğünü.

Madde 85: İade veya teslim işlemlerini destekleyebilecek belgelerin sağlanması

Talepte bulunan Ulusal Merkez Bürosu veya uluslararası kuruluş, bunu faydalı ve uygun gördüğünde, iade veya teslim işlemlerini destekleyebilecek ek belgeleri Genel Sekreterlik'e sağlar. Genel Sekreterlik, bu belgelerin saklanabileceği bir merkez olarak hizmet verebilir ve ilgili ülkelere talep üzerine iletebilir.

Madde 86: Genel Sekreterlik tarafından hukuki inceleme

Genel Sekreterlik, tüm kırmızı bültenleri yayımlanmadan önce hukuki incelemeden geçirir ve INTERPOL Anayasası ve Kurallarına, özellikle Anayasa'nın 2 ve 3'üncü maddelerine uygunluğunu temin eder.

Madde 87: Kişinin tespiti sonrasında atılacak adımlar

Bir kırmızı bülten kapsamındaki kişi tespit edildiğinde, aşağıdaki adımlar atılır:

(a) Kişinin tespit edildiği ülke şunları yapar:

(i) Kişinin tespit edildiği gerçeğini, ulusal yasalar ve geçerli uluslararası anlaşmalardan kaynaklanan sınırlamalar saklı kalmak kaydıyla, derhal talepte bulunan Ulusal Merkez Bürosu veya uluslararası kuruluş ile Genel Sekreterlik'e bildirir,

(ii) Ulusal yasalar ve geçerli uluslararası anlaşmalar çerçevesinde izin verilen tüm diğer önlemleri alır, örneğin aranan kişiyi geçici olarak tutuklamak veya hareketlerini izlemek ya da kısıtlamak.

(b) Talepte bulunan Ulusal Merkez Bürosu veya uluslararası kuruluş, kişinin başka bir ülkede tespit edildiği bilgisi kendisine ulaştığında derhal harekete geçmeli ve özellikle, kişinin bulunduğu ülke veya Genel Sekreterlik tarafından talep edilen veri ve destekleyici belgelerin ilgili dava için belirlenen süreler içinde hızlı bir şekilde iletilmesini sağlamalıdır.

(c) Genel Sekreterlik, ilgili Ulusal Merkez Bürolar veya uluslararası kuruluşlara, özellikle geçici tutuklama veya iade işlemleriyle ilgili belgelerin ilgili ulusal yasalar ve uluslararası anlaşmalar çerçevesinde aktarımını kolaylaştırmak suretiyle destek sağlar.

BÖLÜM 3: DİĞER DUYURULARA İLİŞKİN ÖZEL HÜKÜMLER

Madde 88: Mavi Bültenler

(1) Mavi Bültenler, aşağıdaki amaçlarla yayımlanır:

(a) Bir suç soruşturmasında şüpheli kişi hakkında bilgi elde etmek ve/veya

(b) Bir suç soruşturmasında şüpheli kişinin yerini tespit etmek ve/veya

(c) Bir suç soruşturmasında şüpheli kişiyi tanımlamak.

(2) Mavi bültenler yalnızca aşağıdaki koşullar sağlandığında yayımlanabilir:

(a) Bültenin konusu, hükümlü, sanık, şüpheli, tanık veya mağdurdur,

(b) Kişinin suç geçmişi, konumu veya kimliği ya da suç soruşturmasıyla ilgili diğer bilgileri hakkında ek bilgiler,

(c) Talep edilen iş birliğinin etkin olmasını sağlayacak şekilde, suç soruşturması veya kişiyle ilgili yeterli bilgiler.

(3) Bir mavi bülten yalnızca yeterli ayırt edici bilgiler içeriyorsa yayımlanabilir. Yeterli bilgiler en az şunları ifade eder:

(a) Kişi tanımlanabiliyorsa:

(i) Soyadı, adı, cinsiyet, doğum tarihi (en az yılı) ile birlikte fiziksel tanım, DNA profili, parmak izleri veya kimlik belgelerindeki veriler (ör. Pasaport veya ulusal kimlik kartı); veya

(ii) İyi kalitede bir fotoğraf ile birlikte en az bir tanımlayıcı, örneğin takma ad, ebeveynlerden birinin adı veya fotoğrafta görünmeyen belirli bir fiziksel özellik.

(b) Kişi tanımlanamıyorsa:

(i) İyi kalitede bir fotoğraf ve/veya

(ii) Parmak izleri ve/veya

(iii) DNA profili.

Madde 89: Yeşil Bültenler

(1) Yeşil bültenler, bir kişinin suç faaliyetleri hakkında uyarıda bulunmak amacıyla yayımlanır.

(2) Yeşil bültenler yalnızca aşağıdaki koşullar sağlandığında yayımlanabilir:

(a) Kişi, kamu güvenliği için olası bir tehdit olarak değerlendiriliyorsa,

(b) Bu sonuç, ulusal bir kolluk kuvveti veya uluslararası kuruluş tarafından yapılan bir değerlendirmeden çıkarılmış olmalıdır,

(c) Bu değerlendirme, kişinin önceki ceza mahkûmiyetleri veya diğer makul gerekçelere dayalı olmalıdır,

(d) Uyarının ilgili olmasını sağlamak için tehdide ilişkin yeterli veri sağlanmalıdır.

(3) Bir yeşil bülten yalnızca yeterli ayırt edici bilgiler sağlıyorsa yayımlanabilir. Yeterli bilgiler en az şunları ifade eder:

(a) Soyadı, adı, cinsiyet, doğum tarihi (en az yılı) ile birlikte fiziksel tanım, DNA profili, parmak izleri veya kimlik belgelerindeki veriler (ör. pasaport veya ulusal kimlik kartı) veya

(b) İyi kalitede bir fotoğraf ile birlikte en az bir tanımlayıcı, örneğin takma ad, ebeveynlerden birinin adı veya fotoğrafta görünmeyen belirli bir fiziksel özellik.

(4) Yeşil bültenleri alan Ulusal Merkez Bürolar ve ulusal kuruluşlar, ulusal yasalarına uygun olarak gerekli önlemleri almalıdır.

Madde 90: Sarı Bültenler

(1) Sarı bültenler, kayıp bir kişinin yerinin tespit edilmesi veya kendini tanıtamayan bir kişinin kimliğinin belirlenmesi amacıyla yayımlanır.

(2) Sarı bültenler yalnızca aşağıdaki koşullar sağlandığında yayımlanabilir:

(a) Kişinin kaybolması veya bulunması polise bildirilmiş ve kayda geçirilmiş olmalıdır,

(b) Kayıp kişinin nerede olduğu veya bulunan kişinin kimliği polisin bilmediği bir durumda olmalıdır,

(c) Kişi yetişkinse, geçerli ulusal gizlilik yasaları talepte bulunulmasını engellememelidir,

(d) Kişinin veya kişinin kaybolması ya da bulunmasıyla ilgili koşulların tespitini sağlamak için yeterli veri sağlanmalıdır.

(3) Sarı bülten yalnızca yeterli ayırt edici bilgiler sağlandığında yayımlanabilir. Yeterli bilgiler en az şunları ifade eder:

(a) Kayıp bir kişi ile ilgiliyse:

(i) Soyadı, adı, cinsiyet, doğum tarihi (en az yılı) ve

(ii) Fiziksel tanım, iyi kalitede bir fotoğraf, DNA profili veya parmak izleri.

(b) Kişinin kendini tanıtmaya muktedir olmadığı durumlarda:

(i) Fiziksel tanım, kişinin cinsiyeti ve

(ii) İyi kalitede bir fotoğraf, parmak izleri veya DNA profili.

Madde 91: Siyah bültenler

(1) Siyah bültenler, ölü bedenlerin tespit edilmesi amacıyla yayımlanır.

(2) Siyah bültenler yalnızca aşağıdaki koşullar sağlandığında yayımlanabilir:

(a) Ölü bedenin keşfi polise kaydedilmiş olmalıdır,

(b) Bu ölü beden henüz tanımlanmamış olmalıdır,

(c) Ölü beden veya keşfiyle ilgili koşullar hakkında, kimliğinin belirlenmesini sağlayacak yeterli veri sağlanmalıdır.

(3) Siyah bülten yalnızca yeterli tanımlayıcılar sağlandığında yayımlanabilir. Yeterli tanımlayıcılar en az şunları ifade eder:

(a) İyi kalitede bir fotoğraf ve/veya

(b) Parmak izleri ve/veya

(c) DNA profili.

Madde 92: Mor bültenler

(1) Mor bültenler, aşağıdaki amaçlarla yayımlanır:

(a) Suçlular tarafından kullanılan çalışma yöntemi (modus operandi), nesneler, cihazlar veya gizleme yöntemleri hakkında uyarıda bulunmak ve/veya

(b) Suçların çözülmesine veya soruşturmalarına yardımcı olmak amacıyla bu suçlarla ilgili bilgi talep etmek.

(2) Mor bülten yalnızca aşağıdaki koşullar sağlandığında yayımlanabilir:

(a) Olaylar artık soruşturma aşamasında değilse:

(i) Modus operandi ayrıntılı şekilde biliniyor, karmaşık veya benzer suçlar için daha önce tanımlanan çalışma yöntemlerinden farklı ise;

(ii) Bültenin yayımlanması, bu suçların tekrarlanmasını önlemeyi amaçlıyorsa;

(iii) Talep, suçlular tarafından kullanılan modus operandi, nesneler, ekipman veya gizleme yerleri hakkında, etkili önlem alınmasını sağlayacak yeterli veri içeriyorsa;

(iv) Talep, benzer suçlarla eşleştirme yapılmasını sağlayacak yeterli tanımlayıcılar içeriyorsa, böylece suçların çözülmesine yardımcı oluyorsa.

(b) Olaylar hâlâ soruşturma aşamasındaysa:

(i) Suçlar ciddi niteliktedir,

(ii) Suçlar, Teşkilat üyelerinin dikkatini belirli bir modus operandi, nesne, cihaz veya gizleme yöntemine çeker,

(iii) Talep, bu modus operandi ve ilgili nesneler, ekipman veya gizleme yerleri hakkında eşleştirme yapılmasına yetecek kadar veri içerir.

Madde 93: Turuncu bültenler

(1) Turuncu bültenler, kamu güvenliği açısından yakın bir tehdidi temsil eden ve mal kaybına veya kişilere ciddi zarar gelme olasılığı yüksek olan bir olay, kişi, nesne, süreç veya modus operandi hakkında bildirim yapmak amacıyla yayımlanır.

(2) Turuncu bültenler yalnızca aşağıdaki koşullar sağlandığında yayımlanabilir:

(a) Bir kişi söz konusu ise:

(i) Kişi, kamu güvenliği için yakın bir tehdit olarak değerlendiriliyorsa veya özellikle ciddi bir suçu işlemeye hazırlanıyor ya da işlemek üzereyse,

(ii) Bu çıkarım, ulusal bir kolluk kuvveti veya uluslararası kuruluş tarafından yapılan bir değerlendirmeye dayanıyorsa,

(iii) Bu değerlendirme, kişinin önceki ceza mahkûmiyetleri ve/veya diğer makul gerekçelere dayanıyorsa.

(b) Bir nesne, olay veya modus operandi söz konusu ise:

(i) Kamu güvenliği için yakın bir tehdit olarak değerlendiriliyorsa,

(ii) Bu çıkarım, ulusal bir kolluk kuvveti tarafından yapılan bir değerlendirmeye dayanıyorsa.

(3) Turuncu bülten yalnızca, uyarının ilgili olmasını sağlamak için yakın tehditle ilgili yeterli veri sağlandığında yayımlanabilir.

(4) Turuncu bültenleri alan Ulusal Merkez Bürolar ve ulusal kuruluşler, ulusal yasalarına uygun olarak gerekli önlemleri almalıdır.

(5) Turuncu bültenin yayımlanmasına yol açan tehdit artık yakın bir tehdit oluşturmadığında, Genel Sekreterlik, bültenin yayımlanmasını talep eden Ulusal Merkez Bürosu veya uluslararası kuruluş ile istişare ederek, bunu uygun başka bir bültenle değiştirebilir.

Madde 94: Çalıntı eser bildirimleri

(1) Çalınan sanat eseri bildirimleri, çalınan sanat eserlerini veya kültürel değere sahip eşyaları bulmak veya şüpheli koşullarda keşfedilen bu tür nesneleri tanımlamak için yayımlanır.

(2) Çalınmış sanat eseri bültenleri yalnızca aşağıdaki koşullar sağlandığında yayımlanabilir:

(a) Sanat eseri veya kültürel değeri olan nesne, bir suç soruşturması kapsamındadır;

(b) Eserde bazı benzersiz özellikler bulunmalı ve/veya önemli ticari değere sahip olmalıdır.

(3) Çalınmış bir sanat eseriyle ilgili bülten yalnızca, eserin tanımlanmasını sağlayacak yeterli veri sağlandığında yayımlanabilir.

Madde 95: INTERPOL-Birleşmiş Milletler Güvenlik Konseyi Özel Bültenleri

(1) INTERPOL-Birleşmiş Milletler Güvenlik Konseyi Özel Bildirimleri, INTERPOL Üyelerini bir bireyin veya kuruluşun BM Güvenlik Konseyi Yaptırımlarına tabi olduğu konusunda bilgilendirmek amacıyla yayımlanmaktadır.

(2) INTERPOL-Birleşmiş Milletler Güvenlik Konseyi Özel Duyuruları, Birleşmiş Milletler Güvenlik Konseyi Yaptırım Komiteleri ile ilgili olarak Uluslararası Adli Polis Teşkilatı-INTERPOL ile Birleşmiş Milletler Arasındaki İşbirliğine Dair Düzenlemeye uygun olarak yayımlanmaktadır.

(3) Bu özel duyuruların yayımlanmasına ilişkin koşullar, Birleşmiş Milletler Sekreterliği ve INTERPOL tarafından ilgili Komitelerle istişare edilerek kararlaştırılan usullere uygun olarak belirlenir.

Madde 96: Diğer özel bildirimler

(1) Herhangi bir diğer özel bülten kategorisinin amacı, yayımlanma koşulları ve yapısı, bu Kuralların 28'inci maddesinde bahsedilen anlaşma çerçevesinde ve Teşkilatın, bu Kuralların 1'inci Başlığı altında belirtilen amaç ve faaliyetlerine uygun olarak belirlenir.

(2) Bir özel bülten, yalnızca veriler, söz konusu özel bülten kategorisinin yayımlanma koşullarını, bahsi geçen anlaşmada öngörüldüğü şekilde karşılıyorsa yayımlanabilir.

BÖLÜM 4: DİFÜZYONLAR

Madde 97: Difüzyon sistemi

(1) Difüzyon sistemi, her biri belirli bir amaca karşılık gelen standartlaştırılmış iş birliği talepleri ve uyarılardan oluşur:

(a) Hükümlü veya sanık bir kişinin yakalanması, gözaltına alınması veya hareketlerinin kısıtlanması;

(b) Yer tespiti ve izleme,

(c) Ek bilgi elde etme,

(d) kimlik tespiti amacıyla,

(e) Bir kişinin suç faaliyetleri hakkında uyarı,

(f) Bilgi edinme amacıyla.

(2) Bir difüzyonun gönderilme koşulları, Teşkilatın polis veri tabanlarında veri kaydı için belirlenen genel koşullarla aynıdır.

(3) Genel Sekreterlik, yeni bir difüzyon kategorisi oluşturulmasına ilişkin herhangi bir teklifi onay için Yürütme Komitesine sunar. Talebini gerekçelendirmek için Genel Sekreterlik şunları sağlar:

(a) Bu talebe yol açan sebepler ve böyle bir oluşturmanın mali etkileri,

(b) Bu yeni difüzyon kategorisinin belirli amacı, dolaşım koşulları ve içereceği veri türü,

(c) Genel Sekreterlik tarafından yapılan testlerin sonuçları,

(d) Yeni difüzyon kategorisi kişisel veri içeriyor veya bu tür verilerle bağlantılıysa, INTERPOL Dosyalarını Kontrol Komisyonunun görüşü.

Madde 98: Difüzyon formları

(1) Genel Sekreterlik, Ulusal Merkez Bürolar ve uluslararası kuruluşların, INTERPOL Bilgi Sistemi'nde difüzyonları otomatik ve standart bir şekilde işleyebilmelerini ve doğrudan sorgulayabilmelerini sağlamak amacıyla araçlar ve mekanizmalar temin eder.

(2) Genel Sekreterlik, Ulusal Merkez Bürolar ve uluslararası kuruluşlara, bir difüzyon aracılığıyla iş birliği talepleri ve uyarılar göndermelerini sağlayacak gerekli formları temin eder.

(3) Genel Sekreterlik, Ulusal Merkez Bürolar veya bu amaçla oluşturulan danışma organlarındaki temsilcileri ile istişare ederek, her formun yapısını belirler ve gerektiğinde değiştirir.

Madde 99: Difüzyonların dolaşımı

(1) Difüzyonlar, Teşkilatın çalışma dillerinden en az birinde dolaşıma sokulur.

(2) Bir difüzyonu dolaşıma sokmadan önce, Ulusal Merkez Bürosu veya uluslararası kuruluş şunları sağlamalıdır:

(a) Difüzyonu desteklemek amacıyla sağladığı verilerin kalitesi ve yasallığı,

(b) Difüzyonun, veri kaydı için genel koşullara uygunluğu,

(c) Verilerin, uluslararası polis iş birliği amacıyla ilgililiği,

(d) Talebin, INTERPOL kurallarına, özellikle Anayasa'nın 2(1) ve 3'üncü maddelerine ve talepte bulunan birime uluslararası hukuk tarafından yüklenen yükümlülüklere uygunluğu.

(3) Bir Ulusal Merkez Bürosu veya uluslararası kuruluş, şu durumlarda bülten yerine difüzyon kullanmak zorundadır:

(a) İş birliği talebinin veya uyarısının dolaşımını seçilmiş Ulusal Merkez Büroları veya uluslararası kuruluşlarla sınırlamak istediğinde,

(b) İş birliği talebi veya uyarısı içindeki verilere erişimi, sınırlı sayıda Ulusal Merkez Bürosu veya uluslararası kuruluşla kısıtlamak istediğinde,

(c) Talebi, bir bültenin yayımlanmasını haklı çıkarmadığında veya buna uygun olmadığında.

Madde 100: Bir difüzyonun askıya alınması veya geri çekilmesi

(1) Bir uyarıyı veya iş birliği talebini difüzyon yoluyla gönderen Ulusal Merkez Bürosu veya uluslararası kuruluş, difüzyonu en fazla altı ayı geçmeyecek bir süreyle askıya alabilir. Askıya alma gerekçelerini Genel Sekreterliğe bildirmekle yükümlüdür.

(2) Bir uyarıyı veya iş birliği talebini difüzyon yoluyla gönderen Ulusal Merkez Bürosu veya uluslararası kuruluş, difüzyonda yer alan verilere ilişkin herhangi bir değişiklik yapıldığında, difüzyonun sürdürülmesine olan ihtiyacı değerlendirmek zorundadır.

(3) Bir uyarıyı veya iş birliği talebini difüzyon yoluyla gönderen Ulusal Merkez Bürosu veya uluslararası kuruluş, difüzyonun amacına ulaşıldığında veya talebi sürdürmek istemediğinde, difüzyonun geri çekildiğini Ulusal Merkez Bürolarına, uluslararası kuruluşlara ve Genel Sekreterliğe bildirmek zorundadır.

Madde 101: Mesajlarla yayımlanan iş birliği taleplerinin veya uyarıların kaydedilmesi

(1) Bu Kuralların 9(4)'üncü maddesine uygun olarak, bir Ulusal Merkez Bürosu veya uluslararası kuruluş, başlangıçta Genel Sekreterliğin alıcısı olmadığı bir mesajla yayımladığı bir iş birliği talebinin veya uluslararası uyarının, Genel Sekreterlik tarafından Teşkilatın polis veri tabanlarından birine kaydedilmesini isteyebilir.

(2) Genel Sekreterlik, iş birliği talebini veya uyarıyı, işbu Kurallar ve Ulusal Merkez Bürosu veya uluslararası kuruluş tarafından belirlenmiş olabilecek sınırlı erişim ve veri kullanım koşullarına ilişkin kurallar çerçevesinde kaydedecektir.

BÖLÜM 5: GENEL SEKRETERLİĞİN İNİSİYATİFİYLE YAYIMLANAN BÜLTENLER VE DAĞITIMLAR

Madde 102: Bilgi talepleri

(1) Genel Sekreterlik, aşağıdaki durumlarda iş birliği amacıyla kaynaklardan bilgi talep edebilir:

(a) Talep, uluslararası polis iş birliği açısından özel bir ilgi taşıyan belirli bir proje veya olay kapsamında yapılmışsa,

(b) Bunun Teşkilatın amaçlarına ulaşmak için gerekli olduğuna inanmak için gerekçeleri varsa ve güdülen amaçlarla uyumluysa.

(2) Genel Sekreterlik, bir ulusal kuruluştan bilgi talep etmek isterse, ilgili Ulusal Merkez Bürosu'nun önceden onayını almak zorundadır. Genel Sekreterliğin yetki talebine, Ulusal Merkez Bürosu'nun 30 gün içinde yanıt vermemesi halinde, bu onayın verilmiş olduğu kabul edilir. Bununla birlikte, Ulusal Merkez Bürosu'nun kendi ulusal kuruluşlarından bilgi talebine her zaman karşı çıkma hakkı saklıdır.

Madde 103: Bültenlerin yayımlanması

(1) Bu Kuralların 25(4)'üncü maddesine uygun olarak, Genel Sekreterlik kendi inisiyatifiyle bülten yayımlayabilir:

(a) Bir uyarı yayımlamak amacıyla;

(b) Bilgi talep etmek amacıyla.

(2) Genel Sekreterlik, kendi inisiyatifiyle bir bülten yayımlamadan önce şu hususları temin eder:

(a) Bültenin yayımlanmasının, yayımlanma koşullarına uygun olması;

(b) Verilerin kaynağının/bilgiyi sağlayanların bu yayımı kabul etmiş olması ve özellikle erişim kısıtlamalarının kaldırılmış olması ile bu veriler için belirlenen gizlilik seviyesinin yayıma izin vermesi;

(c) Bültenin yayımlanmasının, devam eden bir iş birliği talebine müdahale etmemesi ve herhangi bir Ulusal Merkez Bürosu ya da uluslararası bir kuruluş tarafından benzer bir bülten talebinin sunulmamış olması.

BÖLÜM 6: OLUMLU SORGULAMA SONUÇLARI

Madde 104: Olumlu sorgulama sonuçlarının üretilmesi

(1) INTERPOL Bilgi Sisteminde, bir sorgu ile Teşkilatın kalıcı operasyonel polis veri tabanlarında kayıtlı veriler arasında yeterli bir eşleşme tespit edildiğinde olumlu sorgulama sonucu üretilir. Yeterli eşleşmenin tespiti, her bir veri tabanının özelliklerine bağlıdır.

(2) Bir olumlu sorgulama sonucu üretildiğinde, her bir veri tabanının özelliklerine tabi olarak, veri tabanını sorgulayan Ulusal Merkez Bürosuna veya uluslararası kuruluşa ve Genel Sekreterliğe bir bildirim gönderilir. Ayrıca, başlangıçtaki verileri kaydeden Ulusal Merkez Bürosuna veya uluslararası kuruluşa, olumlu sorgulama sonucu bildirimlerini almayı tercih edip etmediğine bağlı olarak, bildirim yapılır.

(3) Olumlu sorgu sonucunun bildiriminde, en azından veri tabanına başvuran Ulusal Merkez Büro veya uluslararası kuruluşun ve ilk verileri kaydeden Ulusal Merkez Büro veya uluslararası kuruluşun referansları ile kaydedilen kişi, nesne veya olaya ilişkin temel veriler yer alır.

(4) Veriler, belirli projeler kapsamında özel kuruluşlar tarafından işlendiğinde, olumlu sorgulama sonuçlarına ilişkin tüm koşullar ve usuller, mevcut Kuralların 28'inci maddesi uyarınca Teşkilat ile özel kuruluşlar arasında imzalanan anlaşmalarda düzenlenir.

Madde 105: Olumlu sorgulama sonuçlarının yönetim usulü

(1) Olumlu sorgulama sonucunu üreten Ulusal Merkez Bürosu veya uluslararası kuruluş, 63(1)'inci madde uyarınca, ilk verileri kaydeden Ulusal Merkez Bürosu veya uluslararası kuruluş ile temasa geçer.

(2) İlk verileri kaydeden Ulusal Merkez Bürosu veya uluslararası kuruluş, olumlu sorgulama sonucunun uygunluğunu mümkün olan en kısa sürede inceler.

(3) Genel Sekreterlik, Ulusal Merkez Bürolarıyla veya bu amaçla oluşturulan danışma organlarındaki temsilcileriyle istişare ederek, işbirliği talebinin niteliğine göre alınacak önlemleri ve cevap sürelerini belirlemek amacıyla uygulanacak usulleri düzenler.

(4) Ulusal Merkez Büroları, geçerli ulusal mevzuata uygun olarak, olumlu sorgulama sonuçlarının ulusal kuruluşlara bildirilmesine ilişkin usulleri belirler.

Madde 106: Olumlu sorgulama sonuçlarının kaydı

(1) Genel Sekreterlik, belirli bir işbirliği talebi için üretilen olumlu sorgulama sonuçlarının kaydını tutar. Bu kayıt, veriler polis veri tabanlarında kayıtlı olduğu sürece saklanır.

(2) İlk verileri kaydeden Ulusal Merkez Bürosu veya uluslararası kuruluş bu kaydı inceleyebilir.

BÖLÜM III:

VERİ GÜVENLİĞİ

KISIM 1: INTERPOL BİLGİ SİSTEMİNE ERİŞİM HAKLARININ YÖNETİMİ

Madde 107: Yeni bir Ulusal Merkez Bürosunun atanması

(1) Genel Sekreterlik, Teşkilata yeni üyelik ve Ulusal Merkez Büro atamalarını Ulusal Merkez Bürolarına ve uluslararası kuruluşlara bildirir.

(2) Genel Sekreterliğin bildirim tarihinden itibaren, Ulusal Merkez Büro veya uluslararası kuruluş, polis veri tabanlarına kaydettiği verileri işleme hakkının bu yeni Ulusal Merkez Büroya verilmesine karşı itirazını bildirmek için 45 güne sahip olacaktır.

Madde 108: Yeni bir ulusal kuruluşa erişim hakkının verilmesi

(1) Yeni bir ulusal kuruluşa INTERPOL Bilgi Sistemine erişim hakkı tanımadan önce, Ulusal Merkez Bürosu, söz konusu ulusal kuruluşun mevcut Kurallardan doğan yükümlülüklere uyduğunu temin etmek için gerekli tüm önlemleri alır.

(2) Her Ulusal Merkez Bürosu, yeni bir ulusal kuruluşa INTERPOL Bilgi Sistemine erişim hakkı tanıdığı durumları Genel Sekreterliğe bildirir.

(3) Verilen yetkilerin kapsamını belirtir.

Madde 109: Yeni bir uluslararası kuruluşa erişim hakkı tanınması

(1) Genel Sekreterlik, Teşkilat tarafından yeni bir uluslararası kuruluşa tanınan herhangi bir erişim hakkını Ulusal Merkez Bürolarına ve uluslararası kuruluşlara bildirir.

(2) Teşkilatla imzalanan anlaşma kapsamında verilen yetkilerin kapsamını belirtir.

Genel Sekreterlik tarafından yapılan bildirimin tarihinden itibaren, bir Ulusal Merkez Bürosu veya uluslararası kuruluş, kendi kaydettiği verilerin polis veri tabanlarında bu uluslararası kuruluşa erişim hakkı tanınmasına karşı çıktığını bildirmek için 45 gün süreye sahiptir.

Madde 110: INTERPOL Bilgi Sistemine Erişim Hakları Kaydı

Genel Sekreterlik, INTERPOL Bilgi Sisteminde doğrudan veya dolaylı olarak veri işleme yetkisine sahip tüm Ulusal Merkez Bürolarının, ulusal kuruluşların, uluslararası kuruluşların ve özel kuruluşların güncel bir kaydını tutar ve bu kaydın sürekli olarak sorgulanabilir olmasını sağlar. Bu kayıt, işleme haklarının amacını, niteliğini ve kapsamını belirtir ve bu haklarda yapılan son değişiklikleri kaydeder.

Madde 111: INTERPOL Bilgi Sistemine Bireysel Erişim Hakları

(1) Mevcut Kuralların 15(4) ve (5)'inci maddesine uygun olarak, INTERPOL Bilgi Sistemine erişim hakları yalnızca açıkça yetkilendirilmiş kişilere, gizlilik seviyeleri dikkate alınarak "bilmesi gerekenler" prensibi çerçevesinde verilir.

(2) Bu haklar şunlar tarafından tanımlanır:

(a) Ulusal Merkez Büroları, kendi personeli ve ulusal kuruluşlarının personeli için,

(b) Genel Sekreterlik, kendi personeli ve uluslararası kuruluşların personeli için.

(3) Ulusal Merkez Büroları ve uluslararası kuruluşlar, INTERPOL Bilgi Sisteminin yetkili kullanıcılarının mevcut Kurallara uymasını sağlamak için gerekli tüm önlemleri almakla yükümlüdür.

(4) Ulusal Merkez Büroları ve uluslararası kuruluşlar:

(a) Yetkili kullanıcıların mevcut Kuralları bildiğinden, uygulayabildiğinden ve bu amaçla gerekli eğitimi aldığından emin olmak için tüm uygun araçları kullanır,

(b) Genel Sekreterlik tarafından iletilen bilgileri yetkili kullanıcılara iletir.

(5) Ulusal Merkez Büroları, uluslararası kuruluşlar ve Genel Sekreterlik, yetkilendirilen kişilerin adlarını ve kendilerine verilen erişim haklarını kaydeder. Hangi veri tabanlarına ve verilere erişim izni verildiğini belirtirler.

(6) Bir Ulusal Merkez Bürosu, ulusal kuruluşa, kendi kullanıcılarının erişim haklarının yönetimini devretmeyi seçebilir. Bu ulusal kuruluşun yukarıda belirtilen yükümlülüklere uymasını sağlar. Devretme düzenlemeleri, Ulusal Merkez Bürosu ile ulusal kuruluş arasında 21(3)'üncü maddesi uyarınca yapılan anlaşmada tanımlanır. Ulusal Merkez Bürosu, bu yükümlülüklerin ve belirlenen düzenlemelerin ilgili birim tarafından yerine getirilip getirilmediğini düzenli olarak denetler.

BÖLÜM 2: GİZLİLİK

Madde 112: Gizlilik seviyeleri

(1) Üç gizlilik seviyesi vardır; bunlar, verilerin yetkisiz ifşasından doğabilecek risklerin artışını yansıtır:

a) "INTERPOL SADECE RESMİ KULLANIM İÇİN"

b) "INTERPOL SINIRLI"

c) "INTERPOL GİZLİ"

(2) Veriler sınıflandırılır:

a) "INTERPOL SADECE RESMİ KULLANIM İÇİN": Yetkisiz ifşası, kolluk faaliyetlerini olumsuz etkileyebilir veya Teşkilatı, personelini, Üyelerini, Ulusal Merkez Bürolarını, ulusal ve uluslararası kuruluşları veya verilerle ilgili kişileri dezavantajlı duruma sokabilir veya itibarlarını zedeleyebilir.

b) "INTERPOL SINIRLI": Yetkisiz ifşası, kolluk faaliyetlerini tehlikeye atabilir veya Teşkilatı, personelini, Üyelerini, Ulusal Merkez Bürolarını, ulusal ve uluslararası kuruluşları veya verilerle ilgili kişileri zarara uğratabilir.

c) "INTERPOL GİZLİ": Yetkisiz ifşası, kolluk faaliyetlerini ciddi şekilde tehlikeye atabilir veya Teşkilatı, personelini, Üyelerini, Ulusal Merkez Bürolarını, ulusal ve uluslararası kuruluşları veya verilerle ilgili kişilere ciddi zarar verebilir.

(3) Kaynak tarafından verilerin gizlilik seviyesi belirtilmemişse, veriler "INTERPOL SADECE RESMİ KULLANIM İÇİN" olarak sınıflandırılır.

(4) Bir Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, belirli bir durumda verileri yukarıdaki seviyelerden daha yüksek bir gizlilik seviyesinde sınıflandırması gerekirse, Genel Sekreterlik, ilgili Ulusal Merkez Bürosu veya birimle birlikte bunun mümkün olup olmadığını değerlendirir. Eğer mümkünse, bu verilerin işlenmesine ilişkin koşulları tanımlayan özel bir düzenleme yapılır.

(5) Bir Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, verilerin korunması açısından daha düşük bir gizlilik seviyesi gerektiğini düşünüyorsa, her zaman daha düşük bir gizlilik seviyesi atayarak önceden belirlenmiş seviyeyi değiştirebilir.

Madde 113: Genel Sekreterlik tarafından alınan ek önlemler

(1) Genel Sekreterlik, verileri kaydeden Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşun onayıyla kaynağın atadığı seviyeden daha yüksek bir gizlilik seviyesi atayabilir. Bu, verilerin işlenmesi ve özellikle ifşası nedeniyle uluslararası polis işbirliği veya Teşkilat, personeli ve Üyeleri açısından doğabilecek riskler göz önünde bulundurularak yapılır.

(2) Genel Sekreterlik, veri üzerinde gerçekleştirdiği analiz çalışmaları veya yayımladığı bir bülten gibi durumlarda eklediği değerlerin gizlilik seviyesini de aynı şekilde belirler ve bu ek önlemi veri kaynağına bildirir.

(3) Genel Sekreterlik, aynı koşullar altında bir veri tabanını da sınıflandırabilir.

(4) Genel Sekreterlik, bir Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş tarafından atanan seviyeden daha yüksek bir gizlilik seviyesi belirlediğinde, bu yüksek gizlilik seviyesini istediği zaman değiştirebilir.

Madde 114: INTERPOL Bilgi Sisteminde Gizliliğe Saygı

(1) Genel Sekreterlik, her veri-gizlilik seviyesi için yetkilendirme prosedürlerini veya bir güvenlik izni sistemini belirlemekten sorumludur. Belirli bir gizlilik seviyesine erişim, Ulusal Merkez Büroları, uluslararası kuruluşlar veya Genel Sekreterlik tarafından belirlenen herhangi bir kısıtlamaya tabi olacaktır.

(2) Verilerin işlenmesinde kullanılan iletişim araçları ve altyapısı, veriye atanan gizlilik seviyesine bağlı olarak, yetkisiz ifşanın riskini önleyecek veya böyle bir ifşayı tespit edecek uygun güvenlik kontrolleri ile donatılmalıdır.

(3) Genel Sekreterlik, her gizlilik seviyesi için personelinin uyması gereken idari ve teknik işleme prosedürlerini geliştirecektir.

(4) Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, verileri kaydeden Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş tarafından talep edilen gizlilik seviyesinin usulüne uygun şekilde gözlemlenmesini sağlamak için, Genel Sekreterlik tarafından belirlenenlere en az eşdeğer iç idari ve teknik işleme prosedürlerini uygulayacaklardır.

(5) Genel Sekreterlik, gerektiğinde, Ulusal Merkez Büroları ve ilgili birimlerle koordinasyon içinde, kendi sınıflandırma seviyeleri ile Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar tarafından kullanılan seviyelerin eşdeğerlik tablolarını hazırlayacaktır.

BÖLÜM 3: GÜVENLİK SİSTEMİNİN YÖNETİMİ

Madde 115: Güvenlik kuralları

(1) Mevcut Kuralların 15'inci maddesine uygun olarak, Genel Sekreterlik, INTERPOL Bilgi Sistemi için uygun düzeyde gizlilik, bütünlük ve erişilebilirliği sağlayan usule ilişkin, teknik ve idari güvenlik kontrollerini tanımlayan güvenlik kurallarını belirleyecektir.

(2) Genel Sekreterlik gerekli risk değerlendirmesini gerçekleştirecektir.

(3) Genel Sekreterlik, verilerin güvenliğinin korunmasını sağlamak için uygun kontrol mekanizmaları geliştirecektir.

(4) Genel Sekreterlik, gerekli görülmesi halinde, iletişim altyapısının bir bölümü, bir veri tabanı veya belirli bir departman için özel güvenlik kuralları oluşturabilir.

Madde 116: Ulusal Merkez Büroları ve birimler tarafından uygulanması

Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, Genel Sekreterlik tarafından belirlenen güvenlik kurallarında öngörülen asgari güvenlik düzeyine en az eşdeğer olacak uygun bir güvenlik düzeyini benimsemekten sorumlu olacaktır.

Madde 117: Güvenlik görevlisinin atanması

(1) Her Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, INTERPOL Bilgi Sistemi'nde kendi ülkesi veya uluslararası örgütü için güvenlik işlemlerini yürütmek üzere bir veya birden fazla güvenlik görevlisi atayacaktır.

(2) Güvenlik görevlisi özellikle:

(a) Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşu tarafından belirlenen güvenlik prosedürlerine uyulmasını sağlamalıdır.

(b) Bu prosedürleri, özellikle Genel Sekreterlik tarafından kabul edilen kurallar ışığında güncellemelidir.

(c) Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluştaki personel için veri güvenliği konusunda ek eğitimler vermelidir.

(3) Gerektiğinde, güvenlik görevlisi veri koruma görevlisi ile koordinasyon sağlayacaktır.

(4) Güvenlik görevlisi, güvenlikle ilgili konularda Genel Sekreterlik ile gerekli koordinasyonu sağlayacaktır.

BÖLÜM 4: GÜVENLİK OLAYLARI

Madde 118: Güvenlik olaylarına ilişkin bilgi

(1) Teşkilatın ağını veya veri tabanlarından birini etkileyen sızma ya da ciddi sızma girişimi, ya da verilerin bütünlüğü veya gizliliğinin ihlali ya da ihlal girişimi durumunda, Genel Sekreterlik; bu verilerin kaynağını, kaynak birim yetkilendirilmişse Ulusal Merkez Bürosunu, İcra Komitesini ve INTERPOL Dosyalarının Kontrol Komisyonunu bilgilendirecektir.

(2) İlk olarak INTERPOL Bilgi Sistemi'nde işlenen ve ardından bir Ulusal Merkez Bürosu veya uluslararası kuruluş bilgi sisteminde işlenen verilerin bütünlüğü veya gizliliğinin ihlali ya da ihlal girişimi durumunda, ilgili birim verilerin kaynağını ve Genel Sekreterliği bilgilendirecek ve güvenlik olayı kişisel verileri ilgilendiriyorsa INTERPOL Dosyalarının Kontrol Komisyonuna da bildirecektir. Ulusal kuruluş bilgi sisteminde herhangi bir ihlal veya ihlal girişimi meydana geldiğinde, INTERPOL Bilgi Sistemine erişim izni veren Ulusal Merkez Bürosu, veri kaynağını ve Genel Sekreterliği bilgilendirecektir.

Madde 119: INTERPOL Bilgi Sisteminin kısmi veya tam olarak geri yüklenmesi

Genel Sekreterlik, zarar durumunda INTERPOL Bilgi Sisteminin, özellikle veri tabanları ve iletişim altyapısının, en kısa sürede düzgün çalışır hale getirilmesini sağlamak için gerekli ve uygun tüm adımları atacaktır.

BÖLÜM I:

DENETİM TÜRLERİ

Madde 120: Kullanıcıların denetimi

(1) Tüm Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, kullanıcılarının bu Kurallara uyduğunu özellikle sisteme girilen verilerin kalitesi ve bu verilerin kullanımını düzenli olarak kontrol edeceklerdir. Denetim, ani kontroller ve işleme olayları çerçevesinde yürütülecektir.

(2) Bu Kurallarla belirlenen sınırlar dahilinde, olası işleme hatalarını düzeltmek veya düzeltilmesini sağlamak için gerekli tüm önlemleri alacaklardır.

Madde 121: Ulusal Merkez Büroları ve ulusal ve uluslararası kuruluşlar içinde veri koruma görevlisi atanması

(1) Tüm Ulusal Merkez Büroları, ulusal kuruluşlar ve uluslararası kuruluşlar, bu denetimi organize etmek ve yürütmekten sorumlu bir veri koruma görevlisi atayacaklardır. Veri koruma görevlisinin görevleri, genel olarak güvenlik görevlisinin görevlerinden ayrı yürütülecektir.

(2)Veri koruma görevlisi özellikle:

(a) Ulusal Merkez Bürosu, ulusal kuruluşu veya uluslararası kuruluşta, mevcut Kurallara uygun işleme prosedürleri oluşturur,

(b) Söz konusu Kurallara ve prosedürlere uyumu garanti altına almak amacıyla ani kontroller veya işleme olayları çerçevesinde denetim gerçekleştirir,

(c) Söz konusu prosedürleri ve mekanizmaları günceller,

(d) Ulusal Merkez Bürosu, ulusal kuruluşu veya uluslararası kuruluşun personeli için uygun sürekli veri işleme eğitim programlarını uygular.

(3) Gerekli olduğunda, veri koruma görevlisi güvenlik görevlisi ve INTERPOL veri koruma görevlisi ile işbirliği yapacaktır.

Madde 121A: Genel Sekreterlik içinde veri koruma görevlisi atanması

(1) Anayasa'nın 29'uncu maddesi ve mevcut Kuralların 17(5,6) ve 22(1,5)'inci maddeleri uyarınca, Yürütme Komitesi ve INTERPOL Dosyalarının Kontrol Komisyonu ile istişare ettikten sonra, Genel Sekreter bir veri koruma görevlisi atayacaktır. Bundan sonra bu görevliden "INTERPOL Veri Koruma Görevlisi(IDPO)" olarak söz edilecektir.

(2) IDPO beş yıllığına atanacak olup, bir kez daha atanabilir.

(3) Görevlerini yerine getirirken, IDPO bağımsız olacak ve doğrudan Genel Sekretere rapor verecektir.

(4) IDPO özellikle:

(a) INTERPOL Bilgi Sisteminde verilerin işlenmesinin yasallığını ve Teşkilat Anayasası ile kurallarına uygunluğunu denetler,

(b) Kendi inisiyatifiyle veya Genel Sekreterlik, Ulusal Merkez Büroları ya da INTERPOL Bilgi Sistemini kullanan diğer birimlerin talebi üzerine, bireylerin hak ve özgürlükleri açısından yüksek risk oluşturabilecek işleme faaliyetleri hakkında, veri koruma etki değerlendirmeleri dahil, tavsiye verir ve bu tavsiye doğrultusunda alınan önlemleri izler,

(c) Mevcut Kuralların 121'inci maddesi uyarınca atanmış tüm veri koruma görevlileri ile iletişim kurar, işbirliği yapar ve koordinasyonu sağlar, buna veri koruma konularında eğitim verilmesi ve farkındalık yaratılması da dahildir,

(d) Mevcut Kuralların 17(4,5,6) ve 123(3)'üncü maddeleri uyarınca sunulan veri koruma görevlilerinin yıllık raporlarını inceler,

(e) Genel Sekreterlik personeline veri işleme konularında eğitim verir ve farkındalık sağlar,

(f) Veri işleme konularında INTERPOL Dosyalarının Kontrol Komisyonu ile iletişim kurar,

(g) Diğer kurum ve kuruluşların veri koruma görevlileri ile özellikle deneyim ve en iyi uygulamaların paylaşılması yoluyla iletişim kurar.

(5) Görevlerini etkin bir şekilde yerine getirebilmesi için, IDPO, INTERPOL Bilgi Sisteminde işlenen tüm verilere ve bu verilerin işlendiği herhangi bir sisteme, yer, form veya ortam fark etmeksizin, serbest ve sınırsız erişime sahip olacaktır.

(6) Görevlerini yerine getirirken, IDPO Genel Sekreterliğe şunları sunabilir:

(a) İşleme hatalarının düzeltilmesi de dahil olmak üzere Genel Sekreterlik içindeki veri işleme konularıyla ilgili alınacak önlemler hakkında öneriler,

(b) Mevcut Kuralların 131'inci maddesi uyarınca düzeltici önlemlerin uygulanması gerekliliği ile ilgili öneriler,

(c) IDPO'nun önerilerinin Genel Sekreterlik içinde uygulanmamasına ilişkin raporlar.

(7) IDPO, kendi inisiyatifiyle veya INTERPOL Dosyalarının Kontrol Komisyonunun talebi üzerine, yaptığı önerileri ve düzenlediği raporları bilgi amaçlı olarak INTERPOL Dosyalarının Kontrol Komisyonu ile paylaşabilir ve Komisyon tarafından uygun görülen herhangi bir işlem için iletebilir.

(8) IDPO, görevleriyle ilgili genel konularda uzman görüşü talep edebilir.

(9) IDPO, Yürütme Komitesine yıllık bir rapor sunar. Bu rapor, INTERPOL Dosya Kontrol Komisyonuna da sunulur.

(10) Genel Sekreter, IDPO'nun çalışmalarına ilişkin uygulama kurallarını benimser; bu kurallar, IDPO'nun yetki alanındaki özel görevler, iç prosedürler ve IDPO'nun bağımsızlığını koruyacak önlemleri kapsar.

Madde 122: Verilerin kullanımının denetlenmesi

(1) Herhangi bir Ulusal Merkez Bürosu, kendisi veya ulusal kuruluşları tarafından INTERPOL Bilgi Sisteminde işlenen verilerin başka bir Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş tarafından nasıl kullanıldığını öğrenmek amacıyla bilgi talep edebilir. Veriler bir ulusal kuruluş tarafından incelenmiş veya kullanılmışsa, denetimler ilgili ulusal kuruluşun Ulusal Merkez Bürosu aracılığıyla yapılır.

(2) Genel Sekreterlik, uluslararası kuruluşların aynı denetim haklarını kullanmalarına yardımcı olur.

(3) Bu tür bir denetime tabi olan herhangi bir Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, talep edilen verileri sağlamakla yükümlüdür.

Madde 123: Ulusal kuruluşların değerlendirilmesi

(1) Bu Kuralların 17(4)'üncü maddesine uygun olarak, Ulusal Merkez Büroları, INTERPOL Bilgi Sistemine doğrudan erişim yetkisi verdikleri ulusal kuruluşların faaliyetlerini, bu Kurallar ışığında değerlendireceklerdir.

(2) Bir ulusal kuruluşun, işbu Kurallarda belirlenen yükümlülüklere riayet etmesi, söz konusu ulusal kuruluşun INTERPOL Bilgi Sistemine doğrudan erişimini sürdürmesi için temel bir koşuldur.

(3) Her yıl, her Ulusal Merkez Bürosu, gerçekleştirdiği denetimleri, ele aldığı işleme olaylarını, personeline sağladığı eğitim kaynaklarını ve bu Kuralların yükümlülüklerini karşılamak amacıyla benimsenen yeni tedbirleri Genel Sekreterliğe raporlayacaktır.

(4) Genel Sekreterlik, bir ulusal kuruluşun verileri tekrar tekrar uyumsuz bir şekilde işlemesi, ilgili Ulusal Merkez Bürosu tarafından herhangi bir değerlendirme yapılmamış olması veya yapılan değerlendirmelerin yetersiz olması durumunda, ya Ulusal Merkez Bürosundan söz konusu ulusal kuruluşa düzeltici önlemler uygulamasını talep etme ya da ulusal kuruluşun INTERPOL Bilgi Sistemine erişimini sonlandırma yetkisine sahip olacaktır.

Madde 124: Ulusal Merkez Bürolarının değerlendirilmesi

Bu Kuralların 17(5)'inci maddesi uyarınca, Genel Sekreterlik, Ulusal Merkez Bürolarının işleyişini bu Kurallar çerçevesinde değerlendirecektir.

Ulusal Merkez Bürolarının bu Kurallar ışığında değerlendirilmesi, Genel Sekreterlik tarafından, Genel Kurul tarafından kararlaştırılan yönergeler doğrultusunda gerçekleştirilecektir.

BÖLÜM II: DENETİM ARAÇLARI

Madde 125: Uyum yönetimi veri tabanı

(1) Bu Kuralların 10(4)'üncü maddesi uyarınca, Genel Sekreterlik, Teşkilatın polis veri tabanlarına kaydedilen verilerin bu Kurallara uygunluğunu sağlamak ve veri tabanlarında yetkisiz veya hatalı veri işlenmesini önlemek amacıyla herhangi bir veri tabanı kurabilir.

(2) Bir uyum yönetimi veri tabanı, aşağıdaki koşullar altında kurulacaktır:

(a) Yalnızca yetkisiz veya hatalı veri işlenmesini önlemek için gerekli verileri içerecektir;

(b) Bu veri tabanında verilerin tutulma süresi, Yürütme Komitesi tarafından belirlenen azami süre ile sınırlı olacaktır. Bu süre, Uyuşmazlıkların Kontrolü Komisyonu bilgilendirildikten sonra, uyum yönetimi incelemesi bu sürenin sonunda tamamlanmamışsa uzatılabilir;

(c) Bu veri tabanlarına erişim, yalnızca veri işleme sürecine dahil olan ve kendilerine özel erişim hakkı tanınmış Genel Sekreterlik departmanları ve/veya personeli ile sınırlı olacaktır.

(3) Genel Sekreterlik, bir polis veri tabanından veya uyum yönetimi veri tabanından verileri sildiğinde, yine de, söz konusu verilerin yetkisiz veya hatalı işlenmesini önlemeye olanak sağlayan verileri, Yürütme Komitesi tarafından belirlenen azami süre boyunca tutabilir.

Madde 126: İşleme işlemleri sicili

(1) Bu Kuralların 13'üncü maddesi uyarınca, Genel Sekreterlik, INTERPOL Bilgi Sistemi'ndeki işleme işlemlerinin güncel bir sicilini tutacaktır; bu sicil şunları kaydedecektir:

(a) Kullanıcıların INTERPOL Bilgi Sistemi'ne erişimleri,

(b) Kullanıcılar tarafından kaydedilen veriler,

(c) Kullanıcılar tarafından yapılan güncellemeler,

(d) Kullanıcıların verileri tutma kararları,

(e) Kullanıcıların verileri silme kararları,

(f) Doğrudan erişime sahip kullanıcıların sorgulamaları,

(g) Alınan bilgi talepleri ve gönderilen yanıtlar.

(2) Sicil, yalnızca işleme işlemlerinin mevcut Kurallara uygunluğunu doğrulamak için gerekli verileri içerecektir. Bu amaçla, kullanıcı tanımlayıcısı, kullanıcının Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşun adı, işleme işleminin türü, tarih, ilgili veri tabanı ve izleme amaçlı diğer ek veri öğeleri dahil edilecektir.

(3) Bu kayıtlar, Yürütme Komitesi tarafından belirlenen azami saklama süresinden daha uzun süre tutulmayacaktır.

(4) Bu kayıtlara erişim şu amaçlarla yapılabilir:

(a) Yalnızca izleme ve denetim amaçları için,

(b) Denetim işlemlerini yürütmekle yetkilendirilmiş Genel Sekreterlik personeli tarafından,

(c) Kaynak tarafından, izleme amaçlı olarak, Genel Sekreterlikten talepte bulunulduğunda.

(5) Bu kayıtlar, mevcut Kurallara uygunluğu denetlemekle bağlantılı olmadıkça, ceza soruşturmaları amacıyla kullanılamaz.

Madde 127: Doğrulama amaçlı veri karşılaştırması

(1) Kendi bilgi sisteminde, öncelikle INTERPOL Bilgi Sistemi'nde işlenmiş verileri işleyen herhangi bir Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş, verilerin kalitesini doğrulamak amacıyla mevcut INTERPOL Bilgi Sistemi verileri ile karşılaştırılmasını talep etmek üzere Genel Sekreterliğe başvurabilir. Ulusal kuruluştan gelen tüm talepler, ilgili Ulusal Merkez Bürosu aracılığıyla gönderilmelidir.

(2) Doğrulama amaçlı herhangi bir veri karşılaştırması, ya verilerin yüklenmesi ya da indirilmesi yoluyla gerçekleştirilebilir:

(a) Verilerin yüklenmesi yoluyla yapılan herhangi bir veri karşılaştırması, aşağıdaki tüm koşulları sağlamalıdır:

(i) Yükleme işlemi, yalnızca Genel Sekreterliğin, talebi gönderen Ulusal Merkez Bürosu veya uluslararası kuruluş adına, kendi bilgi sistemine girdiği verilerin kalitesini doğrulamasına olanak sağlamak amacıyla yapılır,

(ii) Yüklenen veriler, INTERPOL Bilgi Sistemi içinde başka bir şekilde kopyalanmaz,

(iii) Yüklenen veriler, veri karşılaştırma işlemi tamamlandıktan sonra sistematik olarak silinir.

(b) Verilerin indirilmesi yoluyla yapılan herhangi bir veri karşılaştırması, aşağıdaki tüm koşulları sağlamalıdır:

(i) İndirme işlemi, yalnızca Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşun kendi bilgi sistemine girdiği verilerin kalitesini doğrulamasına olanak sağlamak amacıyla yapılır,

(ii) Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşun bilgi sistemi, INTERPOL Bilgi Sistemi ile eşdeğer en az bir güvenlik seviyesine sahip olmalıdır,

(iii) İndirilen veriler, indirildikleri bilgi sistemi içinde başka bir şekilde kopyalanmaz,

(iv) İndirilen veriler, veri karşılaştırma işlemi tamamlandıktan sonra sistematik olarak silinir.

(3) Genel Sekreterlik, doğrulama amaçlı veri karşılaştırmalarına yetki vermeye yetkilidir; bu yetki aşağıdaki koşullara tabidir:

(a) Yukarıda belirtilen koşullara uyulması,

(b) Veri karşılaştırma işlemi gerçekleştirmek üzere talepte bulunan Ulusal Merkez Bürosu veya uluslararası kuruluş tarafından verilen yazılı teminatla söz konusu koşullara, işlemin amacına, niteliğine ve kapsamına uyulacağını taahhüt eder;

(c) Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluşta, veri karşılaştırmasını denetlemekle sorumlu bir kişinin belirlenmesi.

(4) Genel Sekreterlik, veri karşılaştırma işlemlerinin (yükleme veya indirme yoluyla) güncel bir kaydını tutar.

BÖLÜM III:

DENETİM TEDBİRLERİ

Madde 128: İnceleme prosedürü

(1) Veriler, bir Ulusal Merkez Bürosu, ulusal kuruluş veya uluslararası kuruluş tarafından INTERPOL Bilgi Sistemine girildiğinde ve Teşkilatın polis veri tabanına kaydedildiğinde, önceden doğru ve ilgili kabul edilir.

(2) Veri işleme koşullarına uyum konusunda bir şüphe ortaya çıkarsa, bu ulusal kuruluş tarafından işlenen veriler de dahil olmak üzere, Genel Sekreterlik, şüpheyi ortadan kaldırabilecek açıklama veya ek verileri almak için ilgili Ulusal Merkez Bürosu ile istişare eder. Genel Sekreterlik ayrıca, veri işleme koşullarına uyum konusunda herhangi bir şüphe varsa, uluslararası kuruluşla da istişare eder.

(3) Genel Sekreterlik, bu koşulların gerçekten yerine getirilmesini sağlamak için diğer uygun adımları atar.

(4) İnceleme prosedürü, Genel Sekreterlik verilerin işlenmesi konusunda şu sonuçlara vardığında kapatılmış sayılır:

(a) Mevcut Kurallara uyum sağlanmış ve veri kaydı doğrulanmışsa,

(b) Mevcut Kurallara uyum sağlanmamış ve veri işleme düzeltilmeye veya veriler silinmeye karar verilmişse.

(5) Genel Sekreterlik, inceleme prosedürünün sona erdiğini ilgili Ulusal Merkez Bürosu veya uluslararası kuruluşa bildirir. Verilerin düzeltilmesine veya silinmesine karar verirse, söz konusu Ulusal Merkez Bürosu veya uluslararası kuruluşa eylemin gerekçelerini ve yapılan düzeltmeleri bildirir.

Madde 129: Geçici tedbirler

(1) Veri işleme koşullarına uyum konusunda bir şüphe ortaya çıkarsa, Genel Sekreterlik, verilerin Teşkilat, personeli, Üyeleri, Ulusal Merkez Büroları, ulusal kuruluşlar, uluslararası kuruluşlar veya verilerle ilgili kişiler açısından doğurabileceği doğrudan veya dolaylı herhangi bir zararı önlemek için tüm uygun adımları atar.

(2) Genel Sekreterlik, alınan geçici tedbirleri ilgili Ulusal Merkez Bürosu veya uluslararası kuruluşa bildirir ve bu tedbirlerin gerekçelerini açıklar.

Madde 130: Kullanıcılara uygulanacak tedbirler

Kullanıcılar, INTERPOL Bilgi Sistemi'nde veri işleme ile ilgili kuralları ihlal ederlerse, Genel Sekreterlik:

(a) ilgili Ulusal Merkez Bürosu veya uluslararası kuruluştan, kendilerine verdiği erişim haklarını askıya almasını veya geri çekmesini isteyebilir,

(b) hakları kendisi askıya alabilir veya geri çekebilir. Bu durumda, ilgili Büroyu veya uluslararası kuruluşu askıya alma veya geri çekme konusunda bilgilendirir.

Madde 131: Ulusal Merkez Büroları ve uluslararası kuruluşlara uygulanacak düzeltici tedbirler

(1) Bir Ulusal Merkez Bürosu veya uluslararası kuruluş, INTERPOL Bilgi Sistemi'nde veri işlerken güçlük yaşar veya mevcut Kurallar uyarınca yükümlülüklerini yerine getirmezse, Genel Sekreterlik aşağıdaki düzeltici tedbirleri alma hakkına sahiptir:

(a) veri işleme hatalarının düzeltilmesi,

(b) Ulusal Merkez Bürosu veya uluslararası kuruluş tarafından yürütülen veri işleme işlemlerinin en fazla üç ay süreyle denetlenmesi,

(c) Ulusal Merkez Bürosu veya uluslararası kuruluşun kullanıcılarına verilen erişim haklarının askıya alınması,

(d) Ulusal Merkez Bürosu veya uluslararası kuruluşa bir değerlendirme ekibi gönderilmesi.

(2) Genel Sekreterlik, Ulusal Merkez Büroları ve uluslararası kuruluşlara, mevcut Kuralların uygulanmasıyla ilgili öneriler gönderebilir; bu öneriler, örneğin personel eğitimi veya çalışma prosedürlerinin geliştirilmesi yoluyla, karşılaşılan güçlüklerin çözülmesine veya veri işleme olaylarının sonlandırılmasına yardımcı olmayı amaçlar.

(3) Genel Sekreterlik, bir Ulusal Merkez Bürosu veya uluslararası kuruluşun aşağıdaki veri işleme haklarının uzun süreli askıya alınmasına yol açabilecek tüm düzeltici tedbir önerilerini karara bağlanmak üzere Yürütme Komitesine sunar:

(a) Teşkilatın bir veya birkaç polis veri tabanına veri kaydetme hakkı,

(b) Bir veya birkaç veri tabanını görüntüleme hakkı,

(c) Veri tabanları arası bağlantı veya indirme yetkileri.

(4) Gerektiğinde ve en az yılda bir kez, Genel Sekreterlik, Ulusal Merkez Büroları ve uluslararası kuruluşlara, INTERPOL Bilgi Sistemi'nde işledikleri verilerle ilgili rollerini ve sorumluluklarını hatırlatır.

BAŞLIK 5: SON HÜKÜMLER

BÖLÜM I: HERHANGİ BİR DİĞER MEŞRU AMAÇLA İŞLEME

Madde 132: Herhangi bir diğer meşru amaç için işlemenin tanımı

(1) Bu Kuralların 10(7)'inci maddesine uygun olarak, veriler Teşkilatın bir polis veri tabanından veya uyum yönetimi veri tabanından silindiğinde, Genel Sekreterlik, herhangi bir diğer meşru amacın yürütülmesi için gerekli verileri yine de saklayabilir.

(2) Herhangi bir diğer meşru amaç şunları ifade eder:

(a) Teşkilatın çıkarlarının savunulması, özellikle dava ve dava öncesi prosedürler ile işlemler kapsamında,

(b) bilimsel, tarihsel veya gazetecilik araştırmaları ve yayımları,

(c) istatistik derlemeleri.

(3) Polis işbirliği amacıyla işlenen veriler, herhangi bir diğer meşru amaçla yeniden işlendiğinde, artık hiçbir şekilde polis işbirliği amacıyla kullanılamaz ve Teşkilatın polis veri tabanlarında yer alamaz.

(4) Yalnızca 2(b) paragrafı kapsamında gerçekleştirilen kişisel veri işlemleri, verilerin kaynağından önceden izin alınmasına tabidir. Ancak, yukarıdaki 2(a) paragrafı kapsamında kişisel veriler işlendiğinde, Genel Sekreterlik bu verilerin kullanımı veya iletimi hakkında kaynağı bilgilendirecektir.

(5) Genel Sekreterlik, özellikle güvenlik açısından, bu ek işlemenin ilk işlemle çelişmemesini garanti etmek için gerekli teknik ve organizasyonel önlemleri alacaktır.

Madde 133: İşleme koşulları

(1) Herhangi bir diğer meşru amaçla işlem yapıldığında, gerekçeler belirtilmelidir. Bu işlemenin özel amacı açıkça gösterilmeli ve işlem yalnızca söz konusu amaç için kesinlikle gerekli olan veri öğeleriyle sınırlı olmalıdır.

(2) İşleme, mümkün olduğunda, veriler anonim hâle getirilerek veya bu mümkün değilse şifrelenerek yapılmalıdır; amaç bu yollarla gerçekleştirilebiliyorsa bu yöntemler tercih edilmelidir.

(3) Herhangi bir diğer meşru amaç için işlenen verilere erişim, yalnızca belirli erişim hakkı verilmiş Genel Sekreterlik'in yetkili departmanları veya personeli ile sınırlı olmalıdır.

Madde 134: Verilerin saklanması

(1) Herhangi başka meşru bir amaçla işlenen veriler, işlendiği amaca ulaşmak için gerekli olan süre boyunca saklanır ve bu süre, Yürütme Komitesi tarafından belirlenen azami saklama süresini aşamaz.

(2) Bu süre yalnızca veriler tarihsel amaçlarla saklandığında veya işleme için anonimleştirilmiş ya da şifrelenmiş olduğunda uzatılabilir; uzatma, işleme amacının gerçekleştirilmesi için gerekli olduğu sürece geçerlidir.

BÖLÜM II:

ANLAŞMAZLIKLARIN ÇÖZÜMÜ

Madde 135: Anlaşmazlıkların çözümü

(1) Ulusal Merkez Büroları, uluslararası kuruluşlar, ulusal kuruluşlar, özel birimler veya Genel Sekreterlik arasında, mevcut Kuralların uygulanmasıyla bağlantılı olarak ortaya çıkan uyum kararlarına ilişkin anlaşmazlıklar, aşağıdaki usule tabi olacaktır:

(a) Anlaşmazlıklar öncelikle karşılıklı danışma yoluyla çözülmelidir. Bu başarısız olursa, nihai bir uyum kararı Genel Sekreterlik tarafından verilir;

(b) Nihai bir uyum kararı verildikten sonra, anlaşmazlıktaki taraflardan biri, anlaşmazlıktan kaynaklanan Anayasa, Veri İşleme Kuralları ve/veya ilgili Genel Kurul Kararlarının uygulanması veya yorumlanmasıyla ilgili bir politika sorusunu Yürütme Komitesine sunabilir. Politika sorusu Yürütme Komitesinin yetkisi dışında ise veya Yürütme Komitesi gerekli görürse, politika sorusu Genel Kurula iletilir.

(2) İlgili tarafların, bu anlaşmazlık çözüm prosedürü dışında, anlaşmazlıklarını dostane bir şekilde çözmelerine engel hiçbir şey yoktur.

(3) Genel Kurul, anlaşmazlıkların çözümünü düzenleyen Uygulama Kurallarını kabul eder.

EK: ULUSAL BİRİMLERİN INTERPOL BİLGİ SİSTEMİNE ERİŞİMİNE İLİŞKİN ŞARTNAME

Mevcut Şartnamenin amacı, ulusal kuruluşların, INTERPOL'un Veri İşleme Kuralları'nın 21. Maddesi uyarınca, kendi ülkelerinin Ulusal Merkez Büroları tarafından, INTERPOL Bilgi Sistemi'nde işlenen verilere doğrudan erişim sağlama veya bu Sistem'de işlenmek üzere doğrudan veri sağlama yetkisi alabileceği koşulları açık bir şekilde belirlemektir.

(1) INTERPOL Bilgi Sistemi'ne doğrudan erişim, aşağıdaki koşullara tabi olacaktır:

(a) INTERPOL Bilgi Sistemi'ne doğrudan erişim ve kullanım, INTERPOL'un Veri İşleme Kuralları'na tabi olacaktır,

(b) Ulusal kuruluş, bu Kuralların hükümlerini ve söz konusu Kurallar uyarınca INTERPOL Bilgi Sistemi'ne erişim ve kullanım sağlamak için oluşturulan prosedürleri kabul edecek ve bunlara uyacağını taahhüt edecektir,

(c) Ulusal kuruluş, bir güvenlik görevlisi ve bir veri koruma görevlisi atayacak ve kullanıcılarının mevcut Kurallara uygun hareket etmelerini sürekli olarak sağlayacak prosedürleri uygulayacaktır,

(d) Ulusal kuruluş, özellikle kendisine yetki veren Ulusal Merkez Bürosu'nun aşağıdakileri yapmasına izin vereceğini kabul edecektir:

(i) INTERPOL Bilgi Sistemi'ne girilen veya bu sistemde sorgulanan verilerin işlenmesinin Kurallara uygunluğunu sağlamak amacıyla düzenli kontroller yapmak, ister uzaktan ister yerinde;

(ii) bir işleme olayı meydana geldiğinde gerekli önleyici veya düzeltici önlemleri almak;

(iii) bu Kurallar uyarınca yükümlülüklerini yerine getirmemesi veya verilerin tekrarlayan biçimde Kurallara aykırı işlenmesi durumunda ulusal kuruluşun INTERPOL Bilgi Sistemi'ne erişimini geri çekmek.

Ulusal kuruluş ayrıca, INTERPOL Genel Sekreterliği'nin:

(i) INTERPOL Bilgi Sistemi'nin genel yönetiminden sorumlu olacağını ve Teşkilatın veri tabanlarında veri işleme koşullarının yerine getirilmesini sağlayacağını kabul edecektir,

(ii) Bu Kurallar kapsamında, INTERPOL Bilgi Sistemi'ne erişimin geri çekilmesi de dahil olmak üzere, verilerin Kurallara aykırı işlenmesini sonlandırmak için gerekli tüm uygun önlemleri alabilir.

(2) Ulusal kuruluşun INTERPOL Bilgi Sistemi'ne erişim yetkilerinin kapsamı, INTERPOL'ün Veri İşleme Kurallarına uygun olarak, kendi Ulusal Merkez Bürosu tarafından belirlenecektir.

KAYNAKÇA

Christopher, D. ve Hearn, N., (2018). A Practical Guide to INTERPOL and Red Notices, Great Britain: Bloomsbury Professıonal.

INTERPOL, (1973). 50 th anniversary 1923-1973, https://www.ojp.gov/pdffiles1/Digitization/40713NCJRS.pdf adresinden 20.08.2025 tarihinde alınmıştır.

INTERPOL, (2025a). Our 19 databases,https://www.interpol.int/How-we-work/Databases/Our-19-databases adresinden 10.08.2025 tarihinde alınmıştır.

INTERPOL, (2025b). Data protection, https://www.interpol.int/Who-we-are/Legal-framework/Data-protection adresinden 22.08.2025 tarihinde alınmıştır.

Kaşlı, E., (2023), Kolluk Faaliyetlerinde Kişisel Verilerin Korunması: Avrupa Birliği 2016/794 Sayılı Europol Tüzüğü Ve 2016/680 Sayılı Kolluk-Ceza Adaleti Direktifi Işığında Bir İnceleme. Ankara Avrupa Çalışmaları Dergisi, 22(1), 97-115. https://doi.org/10.32450/aacd.1327043.

Kaya, S. (2009). Uluslararası Alanda Polisiye İşbirliğinin Gelişimi: Avrupa Örneği. Uludağ Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, XXVIII, 49-69.