İSTANBUL BİLGİ ÜNİVERSİTESİ
BİLİŞİM VE TEKNOLOJİ HUKUKU ENSTİTÜSÜ

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü olarak kişisel verilerin korunması alanındaki önemli bir Avrupa Birliği Hukuku düzenlemesi olan "**Suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla yetkili makamlarca kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımı ile ilgili, 2008/977/Aİİ sayılı Konsey Çerçeve Kararı yerine geçen 27 Nisan 2016 tarihli (AB) 2016/680 SAYILI AVRUPA PARLAMENTOSU ve KONSEY DİREKTİFİ"*** isimli direktife ilişkin hazırladığımız bilgi notunu bilgilerinize sunarız.

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitümüzün çalışmalarını **https://itlaw.bilgi.edu.tr** adresinden takip edebilirsiniz.

* Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ 04.05.2016 L 119.

Avrupa Parlamentosu ve Konseyi'nin 2016/680 Sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA Sayılı Konsey Çerçeve Kararı'nı Yürürlükten Kaldıran Direktif Hakkında Bilgi Notu

YÖNETİCİ ÖZETİ

Bilindiği üzere Avrupa Parlamentosu ve Konseyi'nin 2016/680 Sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması Veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA Sayılı Konsey Çerçeve Kararı'nı Yürürlükten Kaldıran Direktif, Avrupa Birliği Genel Veri Koruma Regülasyonu'nun de içerisinde bulunduğu veri koruma reform paketi kapsamında 2012'de teklif edilerek 2016 yılında yürürlüğe girmiştir. 2008/977/JHA sayılı Konsey Çerçeve Kararı'nı yürürlükten kaldıran bu direktif, getirdiği hükümler ile hem kapsamını genişletmiş hem de gelişen veri koruma hukukuna (dolayısıyla Avrupa Birliği Genel Veri Koruma Regülasyonu'a) uyumlu bir sistem tanımlamıştır.

Direktifin Avrupa Birliği Genel Veri Koruma Regülasyonu ile temelde benimsediği prensipler (risk temelli yaklaşım, kişi hak ve özgürlüklerinin korunması, yeterli güvenlik önlemleri…) ile müesseseler (veri koruma etki değerlendirmesi, veri koruma görevlisi, tasarımdan itibaren veri koruması ve başlangıçtan itibaren veri koruması…) aynı olmakla beraber düzenlediği alanın spesifik koşulları gereği farklı düzenlemelere yer verilmesi gerekmiştir. Kolluk ve adli birimlerce suç ve cezalara ilişkin işleme faaliyetleri için ayrı bir düzenleme ihtiyacı da paydaşlar tarafından sıkça dile getirilmiştir.

Avrupa Parlamentosu, Avrupa Konseyi, Avrupa Komisyonu, Avrupa Veri Koruma Gözetçisi ve Article 29 Working Party görüşleri ve önerileri ile şekillenen teklif metninin kabulü ile Avrupa Birliği üye devletleri bu düzenlemeleri iç hukuklarına aktarmak için çalışmalara başlamış ve birtakım ülkeler ilgili düzenlemeleri yürürlüğe koymuştur.

Bu bilgi notu kapsamında direktife ilişkin genel bilgilerin sunulmasını takiben metnin hazırlanma süreci ve bu dönemde paydaşlardan iletilen görüşler genel hatları ile incelenmiş, direktifin içeriği ve

getirdiği düzenlemeler kısaca açıklanmış ve son olarak kolluk ve adli birimlerce gerçekleştirilen veri işleme faaliyetlerine ilişkin Türkiye'nin mevcut pozisyonu, düzenlemeleri ve buna ilişkin Avrupa Birliği gözünden değerlendirmelere yer verilmiştir.

Giriş

Avrupa Parlamentosu ve Konseyi'nin 2016/680 Sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması Veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA Sayılı Konsey Çerçeve Kararı'nı Yürürlükten Kaldıran Direktif ("**2016/680 sayılı Direktif**"), 4 Mayıs 2016 tarihinde Avrupa Birliği'nin ("**AB**") Resmi Gazetesi'nde yayınlanarak 5 Mayıs 2016 tarihinde yürürlüğe girmiştir.

2016/680 sayılı Direktif'in temel iki amacı; (i) gerçek kişilerin, başta kişisel verilerin korunmasına ilişkin hakları olmak üzere temel hak ve özgürlüklerini korunması ve (ii) ilgili mevzuat uyarınca kişisel verilerin yetkili otoritelerce paylaşılmasının gerekli olması durumunda, bu paylaşımın kişisel verilerinin işlenmesiyle ilgili gerçek kişilerin korunmasına ilişkin gerekçelerle sınırlandırılmaması veya yasaklanmamasıdır.

2016/680 sayılı Direktif, ilgili alanı düzenlemekte olan 2008/977/JHA sayılı Konsey Çerçeve Kararı'nın ("**2008/977/JHA sayılı Karar**") kapsamını genişleterek[1] kişisel verilerin, kamu güvenliğine karşı tehditlerin önlenmesi ve kamu güvenliğinin bu tehditlere karşı korunması amaçlı işlendiği hallerde de uygulanmaktadır. Yine 2008/977/JHA sayılı Karar'ın uygulanacağı alan değiştirilerek 2016/680 sayılı Direktif sadece sınır ötesi kişisel veri işleme faaliyetleri için değil, tamamen ulusal seviyede kolluk ve adli birimlerce yapılan işlemeler için de uygulanacak şekilde kaleme alınmıştır[2]. Üçüncü ülkelere kişisel verilerin aktarımına ek olarak uluslararası organizasyonlarla işbirliği ve bunlara aktarım da 2016/680 sayılı Direktif kapsamında düzenlenmiştir.

[1] 2008/977/JHA sayılı Karar'ın kapsamı sadece sınır ötesi veri işlemeleri ile sınırlı olup tamamen ulusal seviyedeki kolluk ve yargılama makamlarının faaliyetlerini kapsamamaktaydı. Avrupa Komisyonu, bu ayrımın uygulamadaki belirsizlikler nedeniyle hukuka aykırı uygulamalara sebep olduğunu belirtmiştir.
[2] Çekya tarafından iletilen çekinceler kapsamında 2016/680 sayılı Direktif kapsamına hiçbir sınır ötesi unsuru bulunmayan tamamen ulusal seviyedeki veri işlemelerin bir Avrupa Birliği direktifi ile düzenlenmesinin uygun olmadığı belirtilmiştir. Bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7921_2016_INIT&from=EN

Mevcut kişisel verilerin korunması mevzuatı haricinde bu hususlara ilişkin düzenleme yapılması, Lizbon Sözleşmesi'nin kabulü sırasında da belirtildiği üzere[3] suça ilişkin konularda kolluk ve yargılama makamlarının işbirliğinin özellikli yapısından kaynaklanmaktadır.

2016/680 sayılı Direktif ile getirilen düzenlemelere genel anlamda bakıldığında gerçek kişilerin gizlilik hakları ve kişisel verilerinin korunması ile kolluk ve adli birimlerin kişisel veri işleme (ve bazı hallerde verinin işlendiğinin ifşa edilmemesi) ihtiyaçları arasındaki denge gözetilmektedir.

2016/680 sayılı Direktif düzenlemelerine uygunluğun sağlanması adına çeşitli araçlar tanıtılmış, veri koruma görevlisi ve etki analizi uygulamaları bu çerçevede zorunlu kılınmıştır.

Avrupa Birliği hukukunda direktiflerin bağlayıcı nitelikleri olmakla beraber bu metinler temel olarak ulaşılmak istenen sonucun belirtilmesi için kullanılmakta ve hukuken uygulanabilir olmaları için iç (ulusal) hukuka aktarılmaları gerekmektedir. Dolayısıyla direktif ile düzenlenen hususların nasıl uygulanacağı Üye Devletler'in takdirine bırakılmaktadır. 2016/680 sayılı Direktif'i iç hukuk düzenine aktarılması için ise Üye Devletler'e 6 Mayıs 2018 tarihine kadar süre tanınmıştır. Bu yükümlülük uyarınca Üye Devletlerce gerek tek bir düzenleme ile gerek birden çok kanunda değişiklikler yapılarak gerekli düzenlemeler gerçekleştirilmiş[4]. Belçika, Bulgaristan, İrlanda, İtalya, Kıbrıs, Lüksemburg ve Birleşik Krallık 2016/680 sayılı Direktif'i tek bir bağlayıcı metin olarak iç hukukuna aktarmıştır. Çekya, Almanya, Estonya, Fransa, Hırvatistan, Letonya, Litvanya, Macaristan, Malta, Hollanda, Avusturya, Polonya, Portekiz, Romanya, Slovenya, Slovakya, Finlandiya ve İsveç ise birden çok kanun, tebliğ ve benzeri araçlarla iç hukuklarında ilgili düzenlemeleri gerçekleştirmiştir. Üye Devletler'in iç hukuklarında yaptıkları düzenlemeler bu bilgi notunun ekinde örneklendirilmiştir.

2016/680 sayılı Direktif'in Hazırlanması, Görüşler ve Kabulü

2016/680 sayılı Direktif, Avrupa Birliği'ndeki kişisel veri koruma reformu kapsamında gündeme gelmiş, Avrupa Birliği Genel Veri Koruma Regülasyonu (95/46/EC sayılı Direktifi kaldıran düzenleme) için hazırlanan teklif metni ile beraber bir kanun paketi ile sunulmuş ve Avrupa Parlamentosu tarafından kabul edilmiştir.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12007L/AFI/DCL/21&from=EN
[4] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=12946

Direktifin hazırlanması aşamasındaki ilk adım, Avrupa Komisyonu tarafından 2009, 2010 ve 2011 tarihlerinde yürütülen görüş kabul süreçleridir[5]. 2016/680 sayılı Direktif'e ilişkin ilk teklif metni ise 25 Ocak 2012 tarihinde Avrupa Komisyonu tarafından sunulmuş, 9 Ocak 2015 tarihinde Avrupa Konseyi tarafından kabul edilerek Avrupa Parlamentosu ile görüşmeler başlamıştır. Avrupa Parlamentosu ile anlaşmaya iki ay içerisinde varılmıştır. 2016/680 sayılı Direktif, 2016'da yürürlüğe girmekle beraber Avrupa Birliği üye devletleri ("**Üye Devletler**") tarafından iç hukuka yansıtılması için son tarih belirtildiği üzere 6 Mayıs 2018 idi.

2016/680 sayılı Direktif'e ilişkin teklif metninin yayınlanması ile Avrupa Birliği'nin çeşitli organlarınca iletilen görüşler ve teklifler aşağıda genel hatlarıyla incelenmektedir. Burada değinilen görüşler ve dikkat çekilen hususların 2016/680 sayılı Direktif'in teklif edilen ile kabul edilen versiyonlarına etkisi, "*2016/680 sayılı Direktif'in İçeriği*" başlığı altında da ortaya konmuştur.

2012'de sunulan teklif metninde Avrupa Komisyonu, 2016/680 sayılı Direktif'in konusunu oluşturan kolluk ve adli yargılama alanlarında yeknesaklığı sağlayacak bir düzenleme yapılması ihtiyacını; (i) kişisel verilerin tüm taraflarca aynı seviyede korunması, (ii) ilgili kurumlar arasındaki iş birliğinin ancak açık ve tutarlı kurallar ile sağlanabileceği, (iii) kişisel verilerin sorunsuz bir şekilde sınır ötesi aktarılabilmesi hususları ve gereklilikleri ile açıklamıştır[6]. Bu ihtiyaçlar doğrultusunda yasama politikasının belirlenmesinde orantılılık ilkesinin temel alınması gerektiğinin özellikle altı çizilmiştir.

25 Ocak 2012 tarihinde Avrupa Komisyonu tarafından sunulan ilk teklif metni üzerine Avrupa Birliği Bölgeler Komitesi yayınladığı görüş metninde[7] sınır ötesi paylaşıma konu olan kişisel verilerin korunabilmesi için kolluk ve adli birimlere yönelik bağlayıcı nitelikte kurallar getirilmesinin bir ihtiyaç olduğunun altını çizmiştir. Görüşte aynı zamanda kişisel verilerin korunması mevzuatı çerçevesindeki genel düzenleme ile kolluk ve yargılama makamlarınca gerçekleştirilen işleme faaliyetlerine ilişkin bu düzenlemenin sınırlarının net olarak çizilmesi, kapsamlarının belirli olması ve bu düzenlemenin uluslararası veri akışı ilkelerine uyumlu olması önerilmiştir. Bölgeler Komitesi tarafından Avrupa Komisyonu tarafından göz önünde tutulması tavsiye edilen konular arasında kolluk ve adli birimlerce gerçekleştirilecek bu kapsamlı belgeleme ve raporlama süreçlerinin adaleti geciktirici etkisi yer almaktadır.

[5] http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm, http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=EN

[7] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:391:0127:0133:en:PDF

Avrupa Veri Koruma Gözetçisi'nin 7 Mart 2012 tarihli görüş yazısında[8] ise 2016/680 sayılı Direktif'e ilişkin teklif metninin "hayal kırıklığı" yarattığını, Avrupa Birliği Genel Veri Koruma Regülasyonu'na ilişkin teklif metni ile karşılaştırıldığında bundan ayrı düzenlenmesinin doğru olmadığını ve yeterli korumanın bu teklif metni ile sağlanmadığını belirtmiştir. Giriş bölümünde belirttiğimiz üzere 2016/680 sayılı Direktif tamamen ulusal seviyede kolluk ve adli birimlerce yapılan işlemeler için de uygulanacak şekilde kaleme alınmış ve bu kapsam değişikliği Avrupa Veri Koruma Gözetçisi tarafından da olumlu bir gelişme olarak nitelendirilmiştir. Görüş kapsamında somut durumlara (örneğin PNR veya telekomünikasyon verilerinin kullanımına) ilişkin düzenlemeler getirilmesi teklif edilmiş ancak metnin kabul edilen versiyonuna yansıtılmamıştır. Genel kapsamlı değerlendirmeler arasında ise teklif metninin yeterince açık olmaması, düzenlemeye uygunluğun ortaya konmasına ilişkin bir mekanizma getirilmemesi, üçüncü taraflara aktarımların ağır şartlara bağlanmaması ve yetkili kurumlarına sınırlı yetkiler tanınması eleştiriye konu olmuştur. Bu görüşler de dikkate alınarak, "2016/680 sayılı Direktif'in İçeriği" başlığı altında belirtildiği üzere, direktif düzenlemeleri netleştirilmiş, detaylandırılmış ve sınırlamalar daha açık bir şekilde ortaya konmuştur. Kabul edilen metinle; denetleyici otoritelerin görevlerinin artırıldığı, veri koruma etki değerlendirmesi uygulamasının zorunlu tutulduğu ve yurt dışına aktarımın daha detaylı düzenlendiği de söylenebilecektir.

Avrupa Parlamentosu ise ilk okuma sonucundaki görüşlerini[9], tüm teklif metnine ilgili değişikliklerin işlendiği bir versiyonu yayınlayarak iletmiştir. Avrupa Parlamentosu tarafından gündeme getirilen revizyon önerilerinin oldukça kabul gördüğü ve kabul edilen metne yansıtıldığını söylenebilecektir. Bu doğruluda, aşağıda da bir kısmına değinileceği üzere, 2016/680 sayılı Direktif kapsamına "maskeleme" ve "profilleme" terimleri ve veri korum etki değerlendirmesi uygulaması eklenmiş, profilleme sonucu ayrımcılığa ilişkin ekleme yapılmış, kişisel verilerin saklanma ve gözden geçirilme sürelerinin sınırlandırılmasına dair hüküm düzenlenmiştir. Avrupa Parlamentosu tarafından teklif edilmekle birlikte final metin kapsamında olmayan düzenlemelere örnek olarak, veri sorumlularının kişisel veri aktarmadan önce verinin doğruluğu, tamlığı ve güncelliği konusunda bir kontrol gerçekleştirmesi ve bu unsurları sakat kişisel verilerin aktarıma konu olmaması verilebilir. Bu hüküm 2016/680 sayılı Direktif'te bulunmamakla beraber kabul edilen metinde kişisel verilerin yanlış olduğu hallerde kişisel verinin kaynağı birime bilgilendirme yapılması öngörülmüştür. Bir başka revizyon teklifinde Parlamento (veri işlemenin kanuniliği ilkesi kapsamında) direktifin kapsamında düzenlenen/düzenlenecek ulusal mevzuatlarda asgari olarak veri işleme amaçlarının ve hedeflerinin, işlenecek kişisel verilerin, işleme araçlarının, veri

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012XX0630(01)&from=EN
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014AP0219&from=EN

sorumlusunun belirlenmesinin, veri işlemeye yetkili görevlilerin ve işleme sırasında takip edilecek prosedürün belirtilmesi gibi oldukça geniş çaplı ve detaylı bir düzenleme yapılması teklif edilmiştir. Aşağıda belirtildiği üzere bu tekliflerden sadece bir kısmına 2016/680 sayılı Direktif'te yer verilmekle beraber ulusal mevzuatlarda kişisel veri işleme faaliyetlerinin düzenlendiği hükümlerde belirlilik sağlanması (görüşe paralel olarak) hedeflenmiştir. Diğer taraftan Parlamento tarafından oldukça detaylı düzenlemeler talep edilmiş, yapılan revizyon teklifleri de bu doğrultuda sunulmuştur. Örneğin genetik verilerin işlenmesine ilişkin ayrı bir madde eklenmesi, otomatik yollarla veri işlenmesinin hangi durumlarda nasıl mümkün olabileceğinin daha kazuistik düzenlenmesi teklif edilmiştir. Bu hükümlerin final metine yansımaması, kabul edilmedikleri anlamına gelmemekle beraber (direktiflerin Üye Devletler'e alan tanıması da dikkate alındığında) daha genel düzenlemeler ile yetinilmesi ile açıklanabilecektir.

Avrupa Konseyi'nin ilettiği görüş[10] ise daha genel kapsamlıdır ve temel noktalara değinmektedir. Bu çerçevede Avrupa Konseyi, teklif metninde şeffaflık ilkesine yer verilmediğine değinmiş, kolluk ve adli birimlerce yürütülen faaliyetlerin zaman zaman şeffaflığa uygun olmamasına (devam eden soruşturmaların tehlikeye girmesi vs.) rağmen genel ilkeler kapsamında yer verilmesi gerektiğini belirtmiştir. Devam eden işleme faaliyetlerinin (aynı veya farklı veri sorumluları tarafından) uygunluğu değerlendirilmiş, gereklilik, orantılılık ve mevzuatın izin vermesi hallerinde direktif kapsamında işleme amaçları için bu işlemenin uygun olacağı kanaatine varmıştır. Avrupa Parlamentosu'nun da görüşünde belirttiğine paralel olarak saklama ve gözden geçirilme sürelerinin sınırlandırılması gerekliliğinin altı çizilmiştir. Yine benzer şekilde işlemenin kanuniliğinin sağlanması adına birtakım işleme unsurlarının (amaç ve hedefler gibi) belirtilmesi gerektiği ifade edilmiştir. Özel nitelikli kişisel verilerin teklif metni kapsamında işlenmesi özelinde ise biyometrik veri ve cinsel eğilime ilişkin verilerin de kapsam dahilinde olması önemli bulunmuştur. Profillemenin ayrımcılık sonucu doğurması halinde yasaklanması yine teklif kapsamında yer almaktadır.

Article 29 Working Party, yayınladığı görüş metninde[11] özellikle özel nitelikli kişisel verilerin işlenmesinde her zaman yerel hukukta spesifik bir hukuki zeminin olması ve bu verilerin işlenmesinde gereklilik ilkesine özellikle dikkat edilmesi gerektiğini belirtmiştir. Ayrıca veri işleme faaliyetinin ayrımcılığa yol açmasının, yeterli tedbirlerin alınmadığı anlamına geleceği ifade edilmiştir. Profilleme yoluyla ayrımcılığa izin verilmemesi de bu kapsamda değinilmiştir. Görüşlerde genelde dillendirildiği üzere saklama ve gözden geçirme sürelerinin sınırlandırılması

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5418_2016_REV_1_ADD_1&from=EN
[11] http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48804

Article 29 Working Party tarafından da teklif edilmiştir. Veri koruma etki analizinin gerekliliğine değinen Article 29 Working Party, otomatik karar mekanizmalarında mutlaka işleme öncesi gerçekleştirilmesi gerektiğini ifade etmiştir. Veri sahiplerinin düzeltme ve silme talep etme haklarına ilişkin ise birtakım hallerde veya birtakım veri kategorileri için bu hakların her zaman ileri sürülebileceği ve veri sorumluları tarafından her zaman yerine getirileceğinin düzenlenmesi gerektiği belirtilmiştir.

2016/680 sayılı Direktif ile Avrupa Birliği Genel Veri Koruma Regülasyonu Arasındaki Temel Farklar

2016/680 sayılı Direktif'in uygulama alanı ve kapsamındaki kişisel veri işleme faaliyetlerinin niteliği nedeniyle genel veri koruma düzenlemelerinden ayrıştığı noktalar bulunmaktadır. Bu çerçevede temel farklar şu şekilde özetlenebilir[12];

- Avrupa Birliği Genel Veri Koruma Regülasyonu uyarınca veri işleme faaliyetinin temeli ilgili kişinin rızası olmakla beraber açık rızanın kolluk ve adli birimlerce gerçekleştirilen işleme faaliyetleri için aranması makul değildir. Dolayısıyla genel düzenlemede temel işleme şartı açık rıza, 2016/680 sayılı Direktif temelinde esas veri işleme şartı kanunlarca düzenlenmedir[13].

- 2016/680 sayılı Direktif kapsamında şeffaflık ilkesinin sağlanmasına ilişkin düzenlemeler neredeyse bulunmamaktadır.

- 2016/680 sayılı Direktif düzenlemeleri veri sahiplerinin kategorilere ayrılmalarını gerektirir niteliktedir (örn. Suçlu, şüpheli, tanık…).

- 2016/680 sayılı Direktif kapsamında veri sahiplerine sunulması gereken bilgilere ilişkin yükümlülük, genel düzenlemeye oranla daha hafiftir.

- 2016/680 sayılı Direktif ile birtakım hallerde veri sahiplerinin haklarını kullanmalarının engellenmesi daha mümkündür.

[12] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711221/Law_Enforcement_Directive_Impact_Assessment.pdf
[13] https://link.springer.com/content/pdf/10.1007%2Fs12027-019-00549-x.pdf

- 2016/680 sayılı Direktif uyarınca veri sorumlularının mevzuata uygunluklarını ispat etmeleri adına daha sıkı şartlar getirilmiştir. Log kayıtlarına ilişkin yükümlülük bu anlamda genel düzenlemelerden ayrılmaktadır.

2016/680 sayılı Direktif'in İçeriği

2016/680 sayılı Direktif, on bölüm ve altmış beş madde olarak kabul edilmiştir. Aşağıda her bir bölüm altında getirilen düzenlemelere yer verilmiş, teklif metni ile farklarının altı çizilmiştir.

- **Bölüm 1 – Genel Hükümler**

Genel hükümler ile 2016/680 sayılı Direktif'in kapsamına, amaçlarına ve tanımlara yer verilmiştir. Teklif metnine ek olarak 2016/680 sayılı Direktif'in kapsamına "kamu güvenliğinin korunması ve bunlara karşı tehditlerin engellenmesi" eklenmiştir. Üye Devletlerin temel yükümlülükleri listelenirken, görüşler kapsamında da altı çizilmesi sonucunda, kişisel verinin paylaşılmasının ancak mevzuatın gerektirdiği hallerde söz konusu olacağı açıkça belirtilmiştir.

Tanımlar kapsamında ise; teklif metninde yer verilmiş olan "çocuk" tanımı çıkarılmış (ve iletilen görüşlerde çocukların kişisel verilerinin özellikle düzenlenmesi önerilmesine karşın genel olarak çocuklara ilişkin spesifik bir düzenleme yapılmamıştır), "alıcı" ve "genetik veri" tanımları revize edilerek (i) belirli bir soruşturma kapsamında kamu otoriteleri tarafından kişisel verilerin mevzuata uygun olarak alınması halinde bu kişilerin "alıcı" sayılmayacağı ve sadece genel veri koruma hükümlerine tabi olacakları düzenlenmiş ve (ii) "genetik veri"lerin kişinin psikolojisi veya sağlığı hakkında özgün (*unique*) bir bilgi sağlaması aranmıştır. Benzer bilgi sağlama kriteri sağlık verileri için de getirilmiştir. Teklif metnine ek olarak "uluslararası organizasyon", "işlemenin kısıtlanması", "profilleme" ve "maskeleme" tanımlarına yer verilmiştir.

Tanımlar dikkate alındığında, 2016/680 sayılı Direktif'in Avrupa Birliği Genel Veri Koruma Regülasyonu ile paralel konseptleri düzenlediği ve bu regülasyonla uyumlu düzenlemeler getirdiği görülmektedir.

- **Bölüm 2 – İlkeler**

Kişisel verilerin işlenmesine ilişkin ilkeler kapsamında eklemeler yapılmış, bu kapsamda; (i) kişisel verilerin güvenliğinin sağlandığı bir şekilde veri işlemenin yapılacağı, (ii) aynı veya başka bir veri sorumlusu tarafından işleme faaliyetinin direktifin birinci maddesinde sayılan amaçlarla ancak o kişisel verinin toplanması amacından farklı bir amaçla yürütülmesine ancak ilgili veri sorumlusunun

kanunen böyle bir yetkisi olması ve işlemenin gerekli ve orantılı olması halinde izin verileceği (Avrupa Konseyi'nin görüşünde de belirtildiği üzere) ve (iii) aynı veya başka bir veri sorumlusu tarafından ilgili kişisel verilerin kamu yararı, bilimsel, istatistiki vb. amaçlarla arşivlenmesinin veri sahiplerinin hak ve özgürlüklerinin korunması halinde mümkün olacağı açıkça düzenlenmiştir.

Teklif metninde yer verilmeyen "Saklama Ve İncelemeye İlişkin Süre Sınırları" başlıklı madde 2016/680 sayılı Direktif'e eklenmiş ve kişisel verilerin silinmesi ile saklamaya ilişkin gereklilik kapsamında periyodik olarak gözden geçirilmesi için süre sınırları getirilmesi gerektiğini ortaya konmuştur. Article 29 Working Party de yayınladığı görüşünde bu düzenleminin mutlaka yer alması gerektiğini belirtmiştir[14]. Kabul edilen metinle ayrıca "olgulara dayanan kişisel veriler" ile "kişisel değerlendirmeye dayanan kişisel veriler"in ayrıştırılmasına ilişkin düzenleme ortaya konmuştur.

Veri işlemenin kanuniliği ilkesi kapsamında 2016/680 sayılı Direktif, iletilen görüşlerdeki netleştirme talebiyle de paralel olarak, direktifin kapsamında düzenlenen/düzenlenecek ulusal mevzuatlarda asgari olarak veri işleme amaçlarının, işlenecek kişisel verilerin ve hedeflerinin belirtilmesini zorunlu tutmuştur.

Teklifte düzenlenmeyen ancak kabul edilen metinde yer verilen bir başka madde ise "Özel İşleme Şartları"dır.

Otomatik bireysel karar alma süreçlerini düzenleyen 2016/680 sayılı Direktif'in on birinci maddesine (teklif metninin dokuzuncu maddesine) yapılan eklemeler ile bu süreçlere kişilerin hak ve özgürlüklerinin korunması için alınacak tedbirler kapsamında en azından insan müdahalesinin sağlanmasına ilişkin hakkın tanınması zorunlu kılınmıştır. Bununla beraber getirilen sonuncu fıkra ile profillemenin ayrımcılığa yol açtığı hallerde mevzuatın bu işlemeye izin vermemesi gerektiği düzenlenmiştir.

- **Bölüm 3 – Veri Sahiplerinin Hakları**

Bu bölüm altında veri sahiplerinin haklarını nasıl kullanabilecekleri, veri sahiplerine sağlanacak bilgilerin kapsamı, kişisel verilere erişim hakkı, bu hakkın sınırları, düzeltme ve silme talep etme hakkı ile veri işlemenin kısıtlanması, denetleyici otoritelerin rolü ve cezai soruşturmalar ve kovuşturmalar kapsamında veri sahiplerinin hakları düzenlenmektedir.

Veri sahiplerinin haklarına ilişkin düzenlemeler teklif metni ile karşılaştırıldığında çoğunlukla korunmakla beraber birtakım detaylı prosedürel düzenlemeler çıkartılarak bu hususlar Üye

[14] http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48804

Devletler'in takdirine bırakılmış, bununla beraber kolluk ve adli birimlerin talepte bulunan kişilerin kimliğinden emin olamadıklarına ilişkin makul bir şüpheleri olması halinde ek bilgiler (kimliğin doğrulanması adına) talep edebileceği düzenlenmiştir.

Bu kapsamda bir başka ekleme ise kişisel verilerinin düzeltilmesi veya silinmesine ilişkin talepte bulunan kişilerin bu taleplerinin reddedilmesine ilişkindir. Buna göre, Avrupa Konseyi'nin görüşüne paralel olarak, ret sebebinin belirtilmesine ilişkin yükümlülüğün yanı sıra kanuni düzenlemeler ile bu yükümlülüğün tamamen veya kısmen kaldırılmasının mümkün olduğu hükme bağlanmıştır. Ret sebebinin belirtilmemesinin hukuki zeminin kamu güvenliği, ulusal güvenlik, yasal soruşturmanın engellenmemesi gibi bir dayanağının olması gerektiği ve gereklilik ile orantılılık ilkelerine uyulması gerektiği belirtilmiştir.

Son olarak kişisel verinin düzeltilmesi halinde yanlış kişisel verinin kaynağının da bu konuda bilgilendirilmesi öngörülmüş, bu şekilde yanlışlığın temelden düzeltilmesi amaçlanmıştır.

- **Bölüm 4 – Veri Sorumlusu ve Veri İşleyen**

Bu bölümde getirilen yükümlülükler, teklif sonrası yapılan revizyonlar aracılığı ile Avrupa Birliği Genel Veri Koruma Regülasyonu'na paralel hale getirilmiştir. Bu kapsamda dikkat çeken düzenlemeler; tasarımdan itibaren veri koruması (*privacy by design*) ve başlangıçtan itibaren veri koruması (*privacy by default*) müesseselerine ilişkin düzenlemelerin revize edilmesi[15], veri sorumlusunun kişisel verileri koruma sorumluluğu kapsamında risk temelli yaklaşımın eklenmesi, ve bu kapsamda işlemenin doğası, kapsamı, içeriği ve amaçlarının değerlendirilmesinin temel teşkil etmesi, ortak veri sorumluları için organizasyonel çerçevenin çizilmesi, alt veri işleyenlerin regüle edilmesi, (Avrupa Konseyi'nin görüşünde belirtildiği üzere) veri işleyenler özelinde gizliliğe ilişkin yükümlülüğünve diğer yükümlülüklerin direktif kapsamında düzenlenmesi ve veri koruma etki değerlendirmesinin direktif kapsamına alınmasıdır.

Raporlamalara ve log kayıtlarının tutulmasına ilişkin düzenlemelere yine bu başlık altında yer verilmiş, raporlama yükümlülüğünün içeriği yapılan revizyonlar ile artırılmış ve netleştirilmiştir. Kolluk ve adli birimlerin bu kapsamda veri işleme faaliyetlerine ilişkin detaylı bir raporlama prosedürü yürütmesi gerekmektedir. Teklif metnindeki düzenlemeye ek olarak log kayıtlarının aynı zamanda suç kovuşturmalarında da kullanılabileceği düzenlenmiştir.

[15] Article 29 Working Party'nin buna ilişkin görüşü için Bknz. http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48804

Kişisel verilerin güvenliğine ilişkin düzenlemeler ayrı bir başlık olmaktan çıkartılarak bu bölüm altında düzenlenmiş ve burada yine işlemenin doğası, kapsamı, içeriği, amaçları ve riskinin göz önünde bulundurulması gerektiği vurgulanmıştır. Bir veri ihlalinin gerçekleşmesi halinde bildirim süreleri teklif metninde 24 saat iken kabul edilen metinde bu süre 72 saate çıkarılmıştır. Sürenin dikkate alınmasında ihlalin ilgili kişilerin hak ve özgürlüklerine ilişkin risk teşkil edip etmediğine bakılması gerektiği de yapılan revizyon ile eklenmiştir. İhlalin ilgili kişilere bildirilmesi kapsamında "ihlalin yüksek risk teşkil edeceği"ne dair emarelerin olması halinde derhal bildirim yükümlülüğü getirilmiş ancak sayılan birtakım hallerde (teklif sonrası revizyon ile bu haller arasına "veri sorumlusu tarafından bu risklerin gerçekleşmesini engelleyici nitelikte tedbirler alınması" ve "bildirim yapılmasının orantısız bir efor gerektirmesi" eklenmiştir) bu yükümlülüğün söz konusu olmayacağı hükme bağlanmıştır.

Bu bölümde son olarak veri koruma görevlisinin belirlenmesi, rolü ve görevleri düzenlenmiştir. Teklifin aksine, veri işleyenlerin veri koruma görevlisi tayin etme yükümlülüğü kaldırılarak bu düzenleme sadece veri sorumlularına ilişkin olarak revize edilmiştir[16]. Veri koruma görevlisinin görevleri zenginleştirilmiş ve bu sayede daha etkili bir pozisyon haline getirilmiştir.

- **Bölüm 5 – Yurtdışına Aktarım**

Kişisel verilerin 2016/680 sayılı Direktif kapsamında üçüncü ülkelere ve uluslararası organizasyonlara aktarımı bu başlık altında düzenlenmektedir. Teklif metninde getirilen temel düzenlemeye ek olarak kişisel verilerin aktarımı için birtakım şartlar getirilmiştir. Bu çerçevede; (i) kişisel verilerin aktarıldığı veri sorumlusu, 2016/680 sayılı Direktif kapsamında "yetkili otorite" olmalı, (ii) başka bir Üye Devlet'ten aktarılan veya erişimine izin verilen kişisel veriler için bu Üye Devlet'in ön izni alınmalı ve (iii) aktarıma konu kişisel verilerin başka bir ülkeye/organizasyona aktarımı devam edecek ise, suç teşkil eden fiilin niteliği, kişisel verinin ilk aktarım amacı ve aktarıma konu ülkenin/organizasyonun veri koruma seviyesi gibi unsurlar göz önünde bulundurularak bu aktarıma izin verilmesi gerekmektedir. Yapılan eklemeler ile, yukarıda belirtilen (ii) numaralı iznin, kamu güvenliğine veya temel menfaatine acil ve ciddi tehdit teşkil eden durumlar halinde alınmayabileceği düzenlenmiştir.

[16] Çekya tarafından iletilen çekinceler kapsamında bu yükümlülüğün orantısız bir yük getirdiği belirtilmiştir. Bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7921_2016_INIT&from=EN

Her halükarda, üçüncü ülkelere ve uluslararası organizasyonlara aktarımlara ilişkin tüm düzenlemeler, Avrupa Konseyi'nin de görüşünde teklif ettiği üzere, kişisel verilerin korunması için sağlanacak güvenliğin olumsuz etkilenmemesi şartı ile uygulanabilecektir.

Yurtdışına aktarım kapsamında yeterli korumaya sahip ülkelere, bölgelere veya yeterli korumanın bulunduğu belirli sektörler kapsamında ilgili ülkelere aktarım düzenlenmektedir. Avrupa Komisyonu'nun bu listeleri belirlerken göz önüne alacağı kriterler arasında ilgili ülkenin/sektörün yasal düzenlemeleri bulunmakla beraber mahkemelerin içtihatlarına, kamu otoritelerinin kişisel veriye erişimine, insan hakları ve özgürlüklerine saygıya, icraya ilişkin uygun yetkilerin varlığına, bu konuda taraf olduğu uluslararası düzenlemelerin de değerlendirileceği açıkça düzenlenmiştir. Verilen yeterlilik kararları ise düzenli olarak gözden geçirilecek ve ilgili ülke/sektördeki yasal gelişmeler dikkate alınacaktır. Böyle bir yeterlilik kararının bulunmadığı hallerde ise gerekli güvenlik tedbirlerinin alınması aranmaktadır. Bu hallerin dışında 2016/680 sayılı Direktif üçüncü bir "istisnai" aktarım öngörmektedir ve acil durumların varlığında, veri sahibinin temel menfaatlerin korunması için vb. gereklilikler halinde aktarım mümkün olabilecektir. Bu durumda dahi veri sahibinin hak ve özgürlükleri ile kamu menfaati arasında bir denge testi yapılması ve her halükarda belgeleme prosedürüne uyulması gerekecektir.

Üçüncü ülkelerdeki alıcılara kişisel verilerin doğrudan aktarımına ilişkin düzenlemeler, teklif metninde yer almamakla beraber 2016/680 sayılı Direktif'te kabul edilmiştir. Buna göre, yurtdışındaki bir alıcıya doğrudan aktarımın söz konusu olabilmesi için; aktarımın kesinlikle gerekli olması, veri sahibinin hak ve özgürlüklerinin kamu menfaatine oranla baskın olmaması, ilgili otoriteye aktarımın etkisiz veya uygunsuz olması, alıcının aktarım amaçları konusunda bilgilendirilmesi gibi şartların beraber sağlanması gerekmektedir.

- **Bölüm 6 – Bağımsız Denetleyici Otoriteler**

Altıncı bölüm kapsamında bağımsız denetleyici otoritelerin kurulması, bunların dış etkilerden tamamen etkilenmeyecek şekilde yapılandırılmaları, üyelerin seçimi, otoritenin yetkisi ve görevleri ile otoritenin işlemlerine karşı yargı yolunun temin edilmesi düzenlenmektedir.

2016/680 sayılı Direktif'in 28inci maddesi uyarınca bağımsız denetleyici otoritelerin yasama süreçlerinde (veri işlemeye ilişkin olması halinde) görüşleri alınmalıdır. Aynı madde kapsamında veri sorumluları ve işleyenler, oluşturulacak yeni bir dosyalama sisteminin parçasını oluşturan veri işleme faaliyetlerini, kişilerin hak ve özgürlüklerinin korunmasında yüksek risk teşkil eden yeni teknolojilerin/prosedürlerin kullanıldığı ve veri koruma etki değerlendirmesi sonucunda yüksek

risk tespit edilen hallerde bağımsız denetleyici otoritelere önceden danışarak yürütmekle yükümlüdürler. Altıncı bölümde de bu görüşlerin verilmesi ve gerekmesi halinde resen veya talep üzerine görüşlerini yasama meclisine, hükümete, diğer kuruluşlara, organlara ve kamuya açıklaması/iletmesi düzenlenmektedir.

- **Bölüm 7 – İşbirliği**

Karşılıklı işbirliğine ilişkin bu bölümdeki düzenlemeler ile denetleyici otoriteler arasında gerekli bilgi paylaşımının ve işbirliğinin yürütüleceği düzenlenmektedir.

Teklif metninde yapılan değişiklik ile bilgi ve işbirliği taleplerinin en kısa zamanda ve en geç bir ay içerisinde karşılanması öngörülmüştür. Yapılan diğer eklemeler ile; (i) talebe konu bilgilerin sadece bu talep ve amaç kapsamında kullanılabileceği, (ii) talebin yerine getirilmesinin 2016/680 sayılı Direktif'in ihlali anlamında geldiği veya yetkisizlik hallerinde bu talebin karşılanmayabileceği, (iii) bilgi paylaşımlarının kural olarak elektronik yollarla ve standart bir format ile gerçekleştirileceği, (iv) kural olarak işbirliği faaliyetleri için ücretlendirme söz konusu olmayacağı ve (v) Avrupa Veri Koruma Kurulu'nun bu kapsamdaki yetki ve görevleri düzenlenmiştir.

- **Bölüm 8 – Kanun Yolları, Sorumluluk ve Yaptırımlar**

2016/680 sayılı Direktif , veri sahiplerinin 2016/680 sayılı Direktif'in ihlaline dair şikayetleri için tek bir otorite gösterileceğini ve bu otorite tarafından ilgili kuruma iletimin sağlanacağını öngörmektedir. İhlale ilişkin şikayetlerin ve diğer idari yollara ek olarak Üye Devletler, denetleyici otoritenin bağlayıcı kararlarına karşı etkin bir yargı yolu tesis etmekle yükümlüdürler. Bununla paralel olarak 2016/680 sayılı Direktif uyarınca getirilen ulusal düzenlemelerin ihlal edilmesi halinde uygulanacak yaptırımların da düzenlenmesi gerekmektedir.

- **Bölüm 9 – Uygulama Hükümleri & Bölüm 10 – Son Hükümler**

Uygulama hükümleri ile 2016/680 sayılı Direktif'in yürürlüğe girme tarihinden önce taraf olunan ve sınırötesi kişisel veri aktarımı düzenleyen uluslararası anlaşmaların, yürürlük tarihinden önce mevzuata uygun olmaları halinde (değiştirilmesine, yerine başka bir anlaşma yapılmasına veya kaldırılmasına kadar) yürürlükte kalacakları öngörülmüştür. Avrupa Konseyi de görüşünde bu hususun veri sorumluları nezdinde hukuki öngörülebilirliğin sağlanması adına önemli olacağını

belirtmiştir. Benzer şekilde yerel mevzuat hükümleri de 2016/680 sayılı Direktif'ten etkilenmeyecektir[17].

2016/680 sayılı Direktif'in Türkiye Perspektifinden Değerlendirilmesi

2016/680 sayılı Direktif'in düzenlediği alanlar dikkate alındığında Türk mevzuatında ilgili kişisel veri işleme faaliyetlerinin tek bir hukuki metin ile düzenlenmediği görülmektedir. Kişisel verilere ilişkin temel kaynak Anayasa'nın[18] yirminci maddesinin üçüncü olup buna göre herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı anayasal koruma altına alınmıştır. Bu kapsamda bilgilendirilme, erişme, düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığı öğrenme hakları tanınmaktadır.

Mevcut tek kanuni düzenleme olan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun[19] kapsamı oldukça geniş olmakla beraber "kişisel verilerin soruşturma, kovuşturma yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi" istisna tutulmaktadır. Dolayısıyla bu çerçevede veri işlenmesi hallerinde veri sorumluları ilgili kanuna tabi olmayacaktır. Buna ek olarak "kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması" halleri de kısmi istisna kapsamında olup, bu işleme faaliyetleri için kolluk ve adli birimlerin aydınlatma yükümlülüğü (ve Veri Sorumluları Siciline kayıt yükümlülüğü) bulunmamakta, veri sahibinin haklarına ilişkin madde uygulanmamaktadır. Suçların önlenmesi ve suç soruşturmaları için gerekli kişisel veri işleme faaliyetleri her halükarda kanunun amacına ve temel ilkelerine uygun ve orantılı olacak, veri sahiplerinin zararları veri sorumlularınca tazmin edilecektir. Ancak görüldüğü üzere bu yeterli bir düzenleme olmayıp veri işlemeye ilişkin net sınırlar çizmemektedir. Dolayısıyla veri sahiplerinin anayasal haklarının ihlal edilmemesine ilişkin bir düzenlemeye ihtiyaç doğmaktadır.

Kişisel verilerin kolluk ve adli birimlerce işlenmesine ilişkin diğer düzenlemeler ise 25673 sayılı Ceza Muhakemesi Kanunu[20] (Madde 38/A, 80, 134, 137, 209), 2559 sayılı Polis Vazife ve Salahiyet Kanunu[21] (Madde 5), Suç Eşyası Yönetmeliği[22] (Madde 8, 26), Adli Sicil Yönetmeliği[23] (Madde 13),

[17] Çekya tarafından iletilen çekinceler kapsamında bu hususun uygulamada karışıklığa yol açacağı belirtilmiştir. Bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7921_2016_INIT&from=EN
[18] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf
[19] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf
[20] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf
[21] http://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf
[22] https://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.21470&MevzuatIliski=0&sourceXmlSearch=su%C3%A7%20e%C5%9Fyas%C4%B1
[23] http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.9394&MevzuatIliski=0&sourceXmlSearch=a

Yargıtay'dan Verilen İcra Ve İflas İşlerine Ait Kararların Yayımlanmasına Dair Yönetmelik[24] (Madde 6), Bilirkişilik Yönetmeliği[25] (Madde 69), Bölge İdare Mahkemeleri, İdare Mahkemeleri Ve Vergi Mahkemelerinin İdari İşler İle Yazı İşleri Hizmetlerinin Yürütülmesi Usul Ve Esaslarına İlişkin Yönetmelik[26] (Madde 70) gibi kaynaklarda yer almaktadır ancak tek tip bir düzenleme söz konusu olmadığı gibi oldukça kısıtlı alanlarla kişisel verilere ilişkin hükümler söz konusudur. Ayrıca belirtmek gerekir ki MASAK (Mali Suçları Araştırma Kurulu) ve kolluk arasındaki bilgi paylaşımı ve benzeri ulusal işbirlikleri kapsamında hiçbir düzenleme bulunmamaktadır. Son olarak 5809 sayılı Elektronik Haberleşme Kanunu'nda[27] "(Bilgi Teknolojileri ve İletişim Kurumu) kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır." hükmü yer almakla beraber kişisel verilerin korunmasına ilişkin bir düzenleme niteliğinden bahsetmek oldukça zordur.

Türkiye'nin, ağır suçlar ve terörizm ile mücadele kapsamında Europol ile uluslararası işbirliği ve kişisel veri aktarımına ilişkin görüşmeleri Kasım 2018'de başlamış ve ikinci görüşme Nisan 2019'da tamamlanmıştır. Ancak (mevcut stratejik işbirliklerinin ve irtibat görevlilerinin olması ile birlikte) Türkiye ile Europol arasında henüz böyle bir sözleşme akdedilmemiştir.

Türkiye'nin suç ve terörizmle mücadele çerçevesinde toplam 103 ülke ile toplam 172 güvenlik işbirliği anlaşması bulunmaktadır[28]. Avrupa Birliği kapsamında ise 22 Üye Devlet ile toplam 47 işbirliği sözleşmesi mevcuttur. Dolayısıyla bütün bu faaliyetlerin kişisel verilerin korunması perspektifinden düzenlenmemesi, 2016/680 sayılı Direktif'e benzer bir düzenlemeye duyulan ihtiyacı da ortaya koymaktadır.

Kişisel verilerin kolluk ve adli birimlerce suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması veya cezaların infazı amacıyla işlenmesi, gerçek kişilerin korunması ve bu kapsamda kişisel veri aktarımına ilişkin mevcut bir düzenlemenin Türkiye'de bulunmaması Avrupa Komisyonu'nun 29 Mayıs 2019 tarihli Türkiye 2019 Raporu'nda[29] da değinilmiş bir eksikliktir. Türkiye'de kişisel verilerin korunmasına ilişkin değerlendirmelerinde Avrupa Komisyonu, Kişisel Verileri Koruma Kurumu'nun faaliyet gösterdiğini ancak özellikle 2016/680 sayılı Direktif'e (ve Avrupa Birliği Genel Veri Koruma Regülasyonu'na) uyumluluğun sağlanması adına herhangi bir kanuni değişikliğin yapılmadığını belirtmiştir. Bu durumun, kişisel verilerin kolluk ve adli yargılama

[24] https://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.19574&MevzuatIliski=0&sourceXmlSearch=icra%20ve%20iflas
[25] https://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.23818&MevzuatIliski=0&sourceXmlSearch=bilirki%C5%9Filik
[26] https://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.20899&MevzuatIliski=0&sourceXmlSearch=b%C3%B6lge%20idare%20mahkemeleri
[27] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf
[28] http://www.uhdigm.adalet.gov.tr/sozlesmeler/munhasir_adli_yardimlasma.html
[29] https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-turkey-report.pdf

kapsamında korunması ve Kişisel Verileri Koruma Kurumu'nun bu kapsamdaki yetkilerinin belirsizliğine ilişkin olduğu belirtilmiştir.

Avrupa Komisyonu'nun Türkiye 2019 Raporu aynı zamanda Türkiye ile Europol arasındaki işbirliği ve kişisel veri paylaşımı görüşmelerini değerlendirmiş, böyle bir uluslararası sözleşmenin akdedilmesi için temel şartlardan birinin Türkiye'deki kişisel veri koruma mevzuatının Avrupa Birliği düzenlemeleri ile (ve dolayısıyla 2016/680 sayılı Direktif ile) uyumluluğu olduğunun altı çizilmiştir. Rapor kapsamında sadece Europol ile işbirliğine değinilmemiş, aynı zamanda kolluk ve adli birimler arasında (özellikle polis ve jandarma arasındaki) işbirliğinin de artırılması gerektiği ortaya konmuştur.

Almanya

- Veri Koruma Kanununun 2016/679 Sayılı AB Regülasyonuna Ve 2016/680 Sayılı Avrupa Birliği Direktif'ine Uyarlanması (Avrupa Birliği Veri Koruma Uyarlama Ve Uygulama Kanunu - DAFUG-EU) Hakkında Kanun
- Genel Veri Koruma Kanunu'nun 2016/679 Sayılı Avrupa Birliği Regülasyonuna Uyumu ve 2016/680 Sayılı Direktifin İç Hukuka Aktarımı Hakkında Kanun
- Hessen'in Veri Koruma Yasasının 2016/679 Sayılı Avrupa Birliği Regülasyonuna ve 2016/680 Sayılı Direktife Ve Bilgi Alma Özgürlüğüne Uyarlanması Hakkında Hessen Kanunu
- Veri Koruma Kanununun 2016/679 Sayılı AB Regülasyonuna Uyarlanması ve 2016/680 Sayılı AB Direktifinin İç Hukukuna Aktarımı Hakkında Kanun
- Baverya Veri Koruma Yasası (Baydsg)
- Bavyera'nın Polis Yasasının Yeniden Düzenlenmesi Hakkında Kanun (Almanya - Neuordnungsgesetz)
- Hamburg Veri Koruma Yasası Ve Diğer Düzenlemelerin 2016/679 Sayılı Avrupa Birliği Regülasyonuna Uyarlanması Hakkında Kanun
- "Hamburg Kolluk Kuvvetleri"ne İlişkin 2016/680 Sayılı Avrupa Birliği Yasa Yönlendirme Direktifi
- 2016/680 Sayılı AB Direktifi'nin Hamburg'a Uygulanması Hakkında Kanun
- Güney Saksonya Veri Koruma Yasasının Yeniden Düzenlenmesi Hakkında Kanun
- Genel Veri Koruma Kanununun 2016/679 Sayılı AB Regülasyonuna Uyarlanması Ve 2016/680 Sayılı Avrupa Birliği Direktif'in İç Hukuka Aktarımı (Avrupa Birliği NRW Veri Koruma Uyum Ve Uygulama Kanunu) Hakkında Kanun
- Ulusal Veri Koruma Kanununu Ve Meclenburg-Batı Pomerania İçişleri Ve Avrupa Bakanlığının Sorumluluk Alanındaki Diğer Veri Koruma Kanunlarını, 2016/679 Sayılı Avrupa Birliği Regülasyon Ve 2016/680 Sayılı Avrupa Birliği Direktifinin İç Hukuka Aktarımına Uyacak Şekilde Değişikliği Hakkında Kanun
- Genel Veri Koruma Kanununun 2016/679 Sayılı Avrupa Birliği Regülasyonuna Uyarlanması Ve 2016/680 Sayılı AB Direktifinin İç Hukuka Aktarımı Hakkında Thuringia Kanunu

- Berlin Veri Koruma Yasası Ve Diğer Düzenlemelerin 2016/679 Sayılı Avrupa Birliği Regülasyonuna Ve 2016/680 Sayılı Direktife Uyarlanması Hakkında Kanun

Fransa

- 20 Haziran 2018 Tarih ve 2018-493 Sayılı Kişisel Verilerin Korunmasına Dair Kanun
- 2018-493 Sayılı 20 Haziran 2018 Tarihli Kişisel Verilerin Korunması Hakkında Kanun ile Tadil Edilen 78-17 Sayılı 6 Ocak 1978 Sayılı Bilgi, Veri ve Özgürlüklere İlişkin Kanunun Başvuru İçin Uygulanması Hakkında 2018-687 Sayılı 1 Ağustos 2018 Tarihli Kararname

Hollanda

- Avrupa Mevzuatının İç Hukukuna Uygulanması ve Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla Kolluk Veri Kanunu ile Adli ve Cezai Sicil Kanunu'nunda Değişiklik Yapılması Hakkında 17 Ekim 2018 Tarihli Kanun
- Soruşturma Ve Kovuşturmaya İlişkin Veri Koruma Direktifinin Uygulanmasına Dair 6 Aralık 2018 Tarihli Kararnamenin Yürürlüğe Giriş Anını Düzenleyen 6 Aralık 2018 Sayılı Kararname
- Avrupa Mevzuatının İç Hukukuna Uygulanması ve Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla Kolluk Veri Kanunu ile Adli ve Cezai Sicil Kanunu'nunda Değişiklik Yapılması Hakkında 17 Ekim 2018 Tarihli Kanunun Yürürlüğe Girmesine İlişkin 6 Aralık 2018 Tarihli Kararname
- Soruşturma Ve Kovuşturmaya İlişkin Veri Koruma Direktifinin Uygulanmasına Dair Kararname
- Kişisel Verilerin İşlenmesinde Olağanüstü Soruşturma Görevlisi Olarak Cezai Suçları Soruşturmakla Yetkili Kılınmış Kişiler Tarafından Kişisel Verilerin İşlenmesinde Kolluk Veri Kanununa Uygun Başvuruları İçeren Hükümler Hakkında 6 Şubat 2019 Sayılı Kararname

Birleşik Krallık

- 2018 Sayılı Veri Koruma Kanunu

İtalya

- Avrupa Parlamentosu ve Konseyi'nin 2016/680 Sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA Sayılı Konsey Çerçeve Kararı'nı Yürürlükten Kaldıran Direktifin İç Hukuka Aktarımı Hakkında Kanun