Veri Koruma Görevlileri tarafından alınan önceden kontrol için bildirimler hakkında görüş: "İşyerinde sağlık verilerinin işlenmesi" konusunda belirli AB kurumlarından gelen bildirimler hakkında görüş.

"Brüksel, 11 Şubat 2011 (Dava 2010-0071)"

1. Prosedür

2008'de Avrupa Veri Koruma Görevlisi (EDPS), kurumlar arasındaki ortak prosedürler hakkında ex post önceden kontrol analizi için yeni bir prosedür duyuran bir mektup gönderdi.

2009'da EDPS, "Topluluk kurumları ve organları tarafından işyerinde sağlık verilerinin işlenmesi ile ilgili Yönergeler"i (EDPS Yönergeleri) tüm AB kurumlarına gönderdi. Bu kurumlardan sağlık verileriyle ilgili bildirimlerini EDPS Yönergeleri çerçevesinde vurgulanan özel yönleri belirten bir DPO tarafından yazılmış bir kapak mektubu ile sunmaları istendi. Bildirimlerin sunulması için son tarih 16 Kasım 2009 idi, ancak çok az kurum bunu zamanında yaptı. EDPS daha sonra bildirim almaya devam etti, en sonuncusu 20 Eylül 2010 tarihindeydi.

EDPS, şu 18 kurumın DPO'larından (Veri Koruma Görevlisi) önceden kontrol için bildirimler (45/2001 Sayılı Yönetmeliğin 27(3) maddesi anlamında) ve bir kapak mektubu aldı:

- Avrupa Eğitim Vakfı (ETF),
- Avrupa Hastalık Önleme ve Kontrol Merkezi (ECDC),
- Avrupa Birliği Temel Haklar kurumı (FRA),
- Araştırma Yürütme kurumı (REA),
- Avrupa Mesleki Eğitim Geliştirme Merkezi (CEDEFOP),
- Transe Avrupa Taşıma Ağı Yürütme kurumı (TEN-T EA),
- Avrupa Demiryolu kurumı (ERA),
- Sağlık ve Tüketiciler İçin Yürütme kurumı (EAHC),
- Topluluk Balıkçılık Kontrol kurumı (CFCA),
- Avrupa Araştırma Konseyi Yürütme kurumı (ERCEA),

- Rekabet ve İnovasyon İçin Yürütme kurumı (EACI),
- Avrupa İş Sağlığı ve Güvenliği kurumı (EU-OSHA),
- Avrupa Kimyasallar kurumı (ECHA),
- Avrupa Yaşam ve Çalışma Koşullarının İyileştirilmesi Vakfı (EUROFOUND),
- Avrupa Çevre kurumı (EEA),
- Avrupa Havacılık Güvenliği kurumı (EASA),
- Avrupa Denizcilik Güvenliği kurumı (EMSA).

Taslak görüş, ilgili kurumların 18 DPO'suna 10 Ocak 2011'de yorumlar için gönderildi. Bazı DPO'ların yorumları, bir kurumın DPO'sundan uzatma talebinin ardından, 11 Şubat 2011'de alındı.

2. Hukuki Yönler

2.1. Önceden kontrol

İncelenen işlemler ön alım tıbbi muayeneler, yıllık sağlık kontrolü ve hastalık izinleri gibi çeşitli prosedürleri kapsar ve farklı veri konularını içerir (daimi personel üyeleri, geçici görevliler, sözleşmeli görevliler, ulusal uzmanlar, stajyerler, bu pozisyonlardan herhangi birine adaylar ve AB kurumlarına ziyaretçiler). Bu işlemler, Tüzük 45/2001'in 27(2)(a) maddesine göre önceden kontrol gerektiren işlemlerdir ("Tüzük"), çünkü bunlar sağlıkla ilgili tıbbi verilerin yanı sıra sağlıkla ilgili olarak ya da bununla bağlantılı olarak idari ve mali verilerin işlenmesini içerir.

EDPS, her kurumın uygulamasını Tüzüğün veri koruma prensipleri doğrultusunda inceledi ve her kurumın EDPS Yönergelerini takip edip etmediğini değerlendirdi. Prosedürlerin benzerlikleri ve bazı kurumların veri koruma uygulamaları açısından sunduğu benzerlikler dikkate alındığında, EDPS tüm bildirimleri aynı bağlamda incelemeye ve tek bir ortak görüş yayınlamaya karar verdi. Bu ortak görüşte, EDPS, Tüzüğün prensiplerine veya EDPS Yönergelerine uygun olmayan herhangi bir kurum uygulamasını vurgular ve ilgili kurum(lar)a ilgili önerilerde bulunur. Ayrıca, bazı iyi uygulama örnekleri de belirtilir. Örneğin, EDPS, CEDEFOP'un EDPS Yönergeleri ışığında yapılan veri işleme işlemleri ve uygulamaları üzerine detaylı bir analizini not eder. Ayrıca, ETF kişisel ve tıbbi dosyaların yönetimi ile ilgili prosedürleri içeren kapsamlı bir kitapçık hazırlamıştır.

Alınan tüm bildirimlerdeki önemli bir unsur, FRA dışında tüm kurumların tıbbi ve laboratuvar testlerini dış bir tıbbi danışman veya taşeronlara ihraç etmeleridir. kurumların çoğu Brüksel ve Lüksemburg'daki Komisyon'un tıbbi hizmetlerini kullanır ve bu doğrultuda SLA'lar (Servis Seviyesi Anlaşmaları) yapmışlardır, hatta diğer dış tıbbi sağlayıcıları kullananlar da bunu yapmıştır. Ek olarak, tüm kurumlar (FRA hariç) Temmuz 2008'de EDPS tarafından onaylanan tıbbi anketi ön alım muayeneleri bağlamında İnter-enstitü Medikal Koleji ile iş birliği içinde kullanmaktadır. Güvenlik önlemleri açısından, EDPS, hiçbir kurumın sağlık verileriyle ilgili özel bir güvenlik politikası benimsemediğini not eder (güvenlikle ilgili 2.9 maddeye daha fazla bakınız).

EDPS, analiz edilen işlemlere dahil olan farklı tarafları belirtmenin faydalı olacağını düşünmektedir. Böylece ilgili kurumlar, denetleyici ve işleyici arasındaki ilişkinin ve personelin tıbbi dosyalarının hangi tarafça tutulduğunun net bir resmini elde edebilir.

i) Komisyon'un tıbbi hizmetleri tarafından tutulan tıbbi dosyalar

REA, TEN-T, ERA, CFCA, ERCEA, FRONTEX ve EACI, Brüksel'deki Komisyon'un tıbbi hizmeti ile bir SLA yapmıştır; EAHC ise Lüksemburg'daki Komisyon hizmeti ile bir SLA'ya sahiptir. Tıbbi dosyalar, Komisyon'un tıbbi hizmetlerinde tutulmaktadır.

ii) Dış bir tıbbi merkez tarafından tutulan tıbbi dosyalar

ECHA, EASA, CEDEFOP, EUROFOUND, EEA, EU-OSHA ve EMSA da Komisyon'un tıbbi hizmetleri ile bir SLA yapmıştır. Bunlardan bazıları, özellikle **EUROFOUND, EEA, EU-OSHA ve ECDC**, kurumların personelinin tıbbi dosyalarını tutan dış tıbbi merkezlerle de sözleşme yapmıştır.

iii) Dış bir tıbbi danışman tarafından tutulan tıbbi dosyalar

ECHA ve EASA ayrıca dış tıbbi merkezlerle sözleşmeye sahiptir, ancak personelin tıbbi dosyaları, faaliyetlerini kurumların tesislerinde gerçekleştiren dış tıbbi danışmanlar tarafından tutulmaktadır. CEDEFOP ve ETF, personelin dosyalarını tutan dış danışmanlarla sözleşme yapmıştır.

FRA'nın tıbbi memuru veya servisi yoktur. Personel, tıbbi verilerini kendileri saklar.

ECDC, EASA ve **EAHC**, ön alım tıbbi muayeneler ve yıllık kontrol etmelerle ilgili işlemlerde, sadece sağlıkla ilgili verilerle değil, aynı zamanda personelin hizmete uygun olup olmadığını belirlemeye yönelik verilerle de ilgili olduğunu bildirdi (Madde 27(2)(b)). EDPS, Avrupa Toplulukları Memurları İçin Personel Yönetmeliği'nin 28(e) maddesinde belirtildiği gibi, bir kişinin uygun olup olmadığının belirlenmesinin, kişinin görevlerini fiziksel olarak yerine getirip getiremeyeceğinin değerlendirilmesini içerdiğini açıklar, bireyin yeteneği, verimliliği veya iş performansı açısından bir değerlendirme değildir. Bu bağlamda Madde 27(2)(b) ilgili değildir.

Ön alım tıbbi muayenelerle ilgili olarak, **ECDC**, **EASA** ve **EEA**, aynı zamanda, sözleşmeden bireyleri hariç tutmayı amaçladığı için Yönetmelik'in 27(2)(d) maddesi kapsamına giren işlemlerin de olduğunu belirtmiştir. EDPS, başarılı bir adayın işe alınmasının, Topluluk Memurları İçin Personel Yönetmeliği'nin 28. maddesinde belirtilen bir dizi koşula dayandığını vurgular. Özellikle, Personel Yönetmeliği'nin 33. maddesi, "atanmadan önce, başarılı bir adayın, kurumun tıbbi memurlarından biri tarafından tıbben muayene edilmesi gerekmekte olup, kurumun 28(e) maddesinin gerekliliklerini yerine getirip getirmediği konusunda kurumun memnun olması gerekmektedir" der. Bu nedenle, bir ön alım tıbbi muayenesi, işe alımın altı gerekliliğinden birini yerine getirmeyi amaçlar, ki bu da Personel Yönetmeliği'nin 28(e) maddesinde belirtilen "bir memur sadece görevlerini fiziksel olarak yerine getirebilecek

durumdaysa atanabilir" şartını yerine getirmeyi amaçlar ve bir bireyi sözleşmeden hariç tutmayı değil. Bu nedenle, ön alım tıbbi muayene işlemi, Yönetmelik'in 27(2)(d) maddesi değil, özel olarak belirtilen riskler nedeniyle 27(2)(a) maddesi kapsamında önceden kontrol edilebilir niteliktedir.

Tüzük'ün 27(4) maddesine göre, EDPS, bildirimin alınmasını takiben iki ay içinde görüşünü bildirecektir. Son bildirimin 20 Eylül 2010'da EDPS'ye sunulduğu gerçeği göz önüne alındığında, EDPS, bu tarihi tüm bildirimlerin alındığı tarih olarak kabul eder. Son tarihin geçmesinin ardından, EDPS, DPO'ların sorulara ve daha fazla bilgiye cevap vermesini araştırmıştır. 6 Aralık 2010'da EDPS, ilgili tüm DPO'lara bir e-posta göndererek, Tüzük'ün 27(4) maddesi doğrultusunda, EDPS'nin bir aylık askı süresini 9 Ocak 2010'a kadar uzattığını bildirdi (bu bir Pazar günü olduğundan, görüş için taslak yorumlar 10 Ocak 2011'de DPO'lara gönderildi). Bu nedenle, önceden kontrol süresi 18 gün askıya alındı (yalnızca alınan son bildirimin askıya alınma süresini dikkate alarak), karmaşıklık nedeniyle bir ay ve DPO'lardan yorum almak için 15 gün. Bu nedenle, mevcut görüş en geç 11 Şubat 2011 tarihine kadar yayınlanmalıdır. EDPS ayrıca her kuruma, bu görüşün önerilerine yanıt olarak alınan önlemleri EDPS'ye 3 ay içinde bildirme zorunluluğunu vurgulayan bireysel bir mektup gönderecektir.

2.2. İşlemenin yasallığı

Kişisel veriler, Tüzük'ün 5. maddesinde bulunan yasal dayanaklara dayanılarak işlenebilir. İncelenen işlemler, 5/a madde kapsamına girer, bu maddeye göre veriler, "Avrupa Toplulukları'nı kuran Antlaşmalar temelinde veya bu Antlaşmalar temelinde kabul edilen diğer yasal araçlarla veya topluluğa ait kurum veya organa veya verilerin açıklandığı üçüncü bir tarafa atfedilen resmi otoriteyi kullanma yetkisinin meşru bir şekilde kullanılmasıyla kamusal çıkarlar doğrultusunda gerçekleştirilen görevin yerine getirilmesi için gereklidir" şeklinde işlenebilir.

Buna göre, 5(a) maddeye göre ilk konu, işlemenin belirli bir yasal dayanağının olup olmadığını belirlemektir ve ikinci konu, işlemin kamusal çıkarlar doğrultusunda gerçekleştirilen bir görevin yerine getirilmesi için gerekli olup olmadığını doğrulamaktır.

Antlaşma veya diğer yasal belgelerdeki ilgili yasal gerekçeler

Ön alım muayenelerinin gerçekleştirilmesine ilişkin yasal dayanak, Memurların Statüsü'nün 28 ve 33. maddelerinde ve Avrupa Toplulukları Diğer Memurlarının Çalışma Koşulları'nın 12(d), 13(2) ve 83(2) maddelerinde bulunabilir.

Yıllık sağlık kontrolü için yasal dayanak, Memurların Statüsü'nün 59(6) maddesi ve Diğer Memurların Çalışma Koşulları'nın 16(1), 59 ve 91. maddeleridir.

Memurların Statüsü'nün 59(1) maddesi, hastalık veya kaza nedeniyle bir izin sırasında herhangi bir tıbbi kontrolde sağlık verilerinin işlenmesinin yasal dayanağını oluşturur.

TEN-T EA ve **EEA**, ön alım tıbbi muayeneleri, yıllık kontroller veya hastalık izni ile ilgili kişisel verilerin işlenmesinin özel yasal dayanaklarını bildirmediği görünmemektedir. EDPS, bu hususun, Yönergelerinde açıkça belirtildiği gibi, özel hükümlerin ilgili personel tarafından gizlilik beyanları aracılığıyla görünür hale getirilmesini, tüm ilgili personel için önermektedir (aşağıdaki "Veri Konusu Kişiye Verilecek Bilgiler" bölümüne bakınız, madde 2.8).

EUROFOUND, yıllık sağlık ziyaretlerinin yasal dayanağı olarak Memurların Statüsü'nün 59(6) maddesini belirtmiştir. **EUROFOUND** ayrıca, CEOS'un hükümlerine göre geçici ve sözleşmeli görevlilerin yıllık kontrol zorunluluğunun yasal dayanağını da eklemelidir. Ayrıca, potansiyel personel için geçerli olan ön alım muayenesinin kesin yasal dayanağının da bildirilmesini (gizlilik beyanıyla ilgili daha fazla bilgi için, madde 2.8'e bakınız) önerir.

Yönergelerde vurgulandığı gibi, Memur Statüsü hükümlerine dayalı olarak toplanan tıbbi verilerin daha fazla işlenmesi, veri konusunun bilgilendirilmiş ve özgürce verdiği onay veya veri konusunun yaşamsal çıkarlarını korumak için işlemenin gerekli olması durumunda yasal olarak kabul edilebilir. Veri konusu kişiye, tıbbi takip amaçları için tıbbi verilerinin daha fazla işlenmesine ilişkin olarak onayını reddetme ve/veya geri çekme olanağı tanınmalıdır. Şu anki durumda, onay, her kurumın personeline vermesi gereken bilgilere dayandığı sürece geçerlidir ve bu da Tüzük'ün 11 ve 12. maddeleri ile uyum içinde olmalıdır ("Veri Konusu Kişiye Verilecek Bilgiler" bölümüne bakınız, madde 2.8).

Kamu yararına yürütülen bir görevi yerine getirmek için gereklilikler

Tüzük 45/2001'in 5. maddesinin ikinci koşulunu yerine getirip getirmediğini değerlendirirken, EDPS, ön alım tıbbi muayenelerin ve belirli tıbbi kontrol muayenelerinin kurumların personelinin uygunluğunu ve hastalık iznini yönetme ve izleme amacıyla gerekli olduğunu belirtmektedir. Ayrıca, yıllık sağlık kontrol muayenelerinin, özellikle bir ortak hastalık sigortası düzenlemenin oluşturulması amacıyla (Memurların Statüsü'nün 72 ve 73. maddeleri) gerekli ve bu nedenle yasal olduğu düşünülebilir. Bu tür işlemler, Tüzük'ün 5(a) maddesi uyarınca kurumların kamu yararı doğrultusunda misyonlarının icrası içinde yer almaktadır.

Her durumda, tüm kurumlar ilgili personelin:

- Muayene doktorundan yıllık muayene sonucu hakkında bilgilendirilmelidir,
- İsteği halinde doktordan ek bilgi/aydınlatma alması için davet edilmelidir,
- Yıllık muayenesini kendi tercih ettiği bir sağlık profesyoneliyle gerçekleştirebilir ve muayene kurumın tıbbi merkezinde gerçekleştirilmiş gibi geri ödeme alabilir.

2.3. Özel veri kategorilerinin işlenmesi

Seçim ve işe alım prosedürleri çerçevesinde, Tüzük 45/2001'in 10. maddesine dahil "özel veri kategorileri"nin işlenmesi, aynı 10. madde, alt maddeleri (2) ile (5) içerisinde bir istisna bulunmadıkça yasaktır.

Bazı kurumlar, kesin anlamda herhangi bir tıbbi veri almadıklarını ve bu nedenle işlemlerin önceden kontrol analizine tabi olmaması gerektiğini iddia etmektedir. Özellikle, EU-OSHA, REA, TEN-T ve EAHC, sadece iş gücü belgesi, hastalık izni ile ilgili idari veriler, tıbbi belgeler, yıllık kontroller ve bazı personelin günlük mesleki faaliyetleri için tıbbi ekipman satın alımı gibi konularda işlem yaptıklarını savunmaktadır.

EDPS, Yönergelerinde açıkladığı gibi, sağlık verisi kavramının başlıca olarak iki farklı veri formuna, tıbbi verilere ve bir kişinin sağlık durumuyla ilgili kişisel verileri içeren idari belgelere dayandığını belirtir. Birçok kurum, örneğin işe uygunluk için tıbbi notlar, bir kişinin yıllık bir tıbbi ziyareti veya aşılama yaptığına dair faturalar, olası bir takip tıbbi muayenesi talepleri için notlar veya sadece bir kişinin tıbbi izinde olduğunu belirten idari amaçlar için İK departmanına gönderilen bilgiler gibi, idari belgeleri toplar ve işler. Bu veriler bir kişinin sağlık durumuyla ilişkilidir ve belirli bir veri konusunun hastalığı veya engelliği ile ilişkilendirilebilir. Tam olarak hangi tür hastalığın belirtilmediği bir tıbbi belgede, veri konusu kişi, kısa veya uzun süreli bir hastalık nedeniyle, tedavi gören veya tıbbi nitelikte özel bir hastalık izni nedeniyle bulunmuş olarak tanımlanabilir.

Dolayısıyla, kesin anlamda tıbbi veri işlenmiş olmasa da, incelenen işlemler sağlıkla ilgilidir, bu nedenle Tüzük'ün 27(2)(a) maddesi kapsamında önceden kontrol edilebilir ve önceden kontrol edilmelidir.

Bu nedenle**, EDPS, ETF, ECDC, FRA, REA, CEDEFOP, TEN-T, EAHC, ECHA, EU-OSHA, EACI, EUROFOUND, EEA, EASA** ve **EMSA**'nın insan kaynakları personelinin uygunluk belgelerini toplama ve personellerinin sağlık durumlarıyla ilgili diğer tüm bilgileri işleme sorumluluğundaki personelin, bu bilgileri tıbbi gizlilik ilkelerine uygun olarak işlemelerini hatırlatır. EDPS, bu kurumları, sağlık verilerinin işlenmesine ilişkin olarak, 45/2001 Tüzüğü'nün 10(3) maddesi uyarınca sağlık profesyonelinin mesleki gizlilikle eşdeğer bir gizlilik yükümlülüğüne tabi olduklarına dair imzalanacak gizlilik beyannameleri hazırlamaya davet eder. (Bu konu, Tüzük'ün 7(3) maddesi ile bağlantılı olmalıdır, bu konuda daha fazla bilgi için görüşün 2.6 noktasına bakınız).

EDPS, CEDEFOP tarafından hazırlanan gizlilik beyannamesini dikkate alır ve beyannamede şu cümlelerden birinin eklenmesini önerir: "45/2001 Tüzüğü'nün 10(3) maddesi uyarınca sağlık verilerinin işlenmesine ilişkin olarak, ben, sağlık verilerine özgü bir mesleki gizlilik yükümlülüğüne tabi olduğumu beyan ederim." Bu ek cümle, özellikle işlenen sağlık verilerine atıfta bulunarak hassasiyetlerini vurgular.

2.4. Veri Kalitesi

Uygunluk, ilgili olma ve orantılılık: Regülasyon 45/2001'in 4(1)(c) maddesine göre "kişisel veriler, toplama ve/veya daha fazla işleme amacıyla toplanan veya işlenen amaçlarla orantılı olmalıdır, uygun ve gereğinden fazla olmamalıdır."

İncelenen kurumlar tarafından toplanan sağlıkla ilgili veriler ve aynı kurumların bazılarının dış sağlayıcıları tarafından toplanan ve işlenen tıbbi verilerin genel olarak, Regülasyonun 4(1)(c) maddesine uygun olarak, ilgili olması, uygun olması ve gereğinden fazla olmaması gereken amaç için uygun olduğu görünmektedir.

Bununla birlikte, EDPS, özellikle ECHA, EASA, CEDEFOP, EUROFOUND, EEA, EU-OSHA, EMSA, ECDC ve ETF'ye özellikle orantılılık ilkesine dikkat çeker. Bu kurumlar, sadece Komisyon'un tıbbi hizmetlerine bağlı değillerdir ve dış sağlayıcıları aracılığıyla ön alım muayenesi ve yıllık kontrol muayetleri çerçevesinde tıbbi verileri işlerler. Bu nedenle, bunlar personelinin fiziksel uygunluğunu belirleme, işgücü ile ilgili garantili hakları belirleme veya personelin sağlığını koruma amaçları dışında herhangi bir amaçla veri toplamanın yasaklanmasını sağlamalıdır. EDPS bu kurumlara "Hizmet için uygunluk değerlendirmesi yapmak amacıyla ön alım tıbbi muayene ve yıllık tıbbi kontrol muayenesi için sorulan soruların uygunluk, ilgi ve orantılılık ilkeleri ışığında genel bir değerlendirmesini yapmaları gerektiğini" önermektedir.

1) Ön alım tıbbi muayenesi

EDPS, ECHA'nın kullandığı tıbbi anketin, ön alım tıbbi muayeneye girecek veri konularının fotoğrafını gerektirdiğini belirtiyor. EDPS, bu tür bilginin, başarılı adayın iş pozisyonuna uygun olup olmadığına dair amaçla uygun olmadığını görüyor.

2) Genel bir hekim tarafından yapılan tıbbi kontrol muayenesi

Personelin kendi seçtikleri bir tıp uzmanında yıllık kontrol muayenesi yapmak istediği durumlarda, ETF, FRONTEX, EACI, EU-OSHA, ECHA, EUROFOUND, EEA, EASA ve EMSA, veri konusunun kendi rızasıyla bilgilendirilmeksizin sonuçlarını kurumın doktoruna veya Komisyon'un tıbbi hizmetine ulaştırmaması için bir politika oluşturmalıdır. Uzman, sadece muayenelerin yapıldığını onaylayan bir beyannameyi kurumın İK birimine göndermeli ve gerektiğinde ilgili veri konusunun özel düzenlemelere ihtiyacı olduğunu belirtmelidir.

CEDEFOP, yıllık tıbbi muayenelerin öncelikli olarak önleyici olmadığını, ancak personelin görevine uygun olup olmadığını veya çalışma ortamında ayarlamalar yapılması gerekip gerekmediğini belirtmiştir. kurum, bu nedenle tüm tıbbi sonuçların sadece onların işyerinde iş sağlığı açısından uygunluğu sertifikalandırabilecekleri dış tıbbi görevliye iletilmesi gerektiğini düşünmektedir. EDPS, veri koruma açısından, veri konusunun kendi tıbbi sonuçlarının özel bir tıbbi muayene aracılığıyla kurumın doktoruna iletilip iletilmeyeceğine serbestçe karar verebilmesi gerektiğini belirtir. kurum için, personelin uygun olduğunu teyit eden bir beyanname yeterli olmalıdır. Bununla birlikte, EDPS, bazı sorunlu durumlarda, bir personelin sağlık durumunun meslektaşlarına veya kendi iş performansına bir risk oluşturabileceği durumlarda, bu belirli sonuçların veri konusuna bilgi verilerek tıbbi verilerin aktarılmasından önce bilgilendirilmesi koşuluyla kurumın doktoruna gönderilebileceğini düşünmektedir.

Doğruluk: Regülasyonun 4(1)(d) maddesi, kişisel verilerin "doğru ve gerekli olduğunda güncel tutulması gerektiğini" belirtir. Ayrıca, "amaçlarına uygun olarak toplandıkları veya daha fazla işlem için oldukları göz önünde bulundurularak, yanlış veya eksik olan verilerin silinmesi veya düzeltilmesi için her makul adımın atılması gerekmektedir".

Bu ilke, hem tıbbi dosyalar hem de kişisel dosyalar için geçerlidir. **ETF, ECDC, REA, CEDEFOP, ERA, EAHC, CFCA, ERCEA, FRONTEX, EACI, EU-OSHA, ECHA, EUROFOUND, EEA, EASA ve EMSA,** ön alım uygunluk sertifikalarının ve yıllık kontrol beyanlarının kişisel dosyalarda tutulması gerektiğini sağlamalıdır. Dosyalar, gerektiğinde sağlık durumu belgeleriyle güncellenmeli, özellikle yıllık kontrol muayenesi durumunda. İç notlar, sorumlu İK personeline göre düzenlenmelidir.

ETF, ECHA ve **EASA**, kalite ilkesinin saygı gösterildiğinden emin olmak için dış tıbbi danışmanları ve tıbbi merkezlerle yapılan sözleşmelere örneğin bir madde ekleyerek bunu sağlamalıdır. **ECDC, EU-OSHA, EUROFOUND, EEA** ve **EMSA** da ilgili dış tıbbi hizmetlerle aynı şekilde hareket etmelidir. Bu madde, veri konularının tıbbi raporda bulunan tıbbi verilerin eksiksiz olduğundan emin olmak için kendi doktorları veya uzmanlarıyla temasları hakkında bilgi içeren veri konularının onayı ve imzası gibi belirli yöntemleri listeleyebilir:

- the consent and signature of the data subjects as regards information concerning contacts with their attending physician or specialist may help to ensure that the medical data contained in the medical report are complete;
- the data subjects can sign their medical examination reports so that the accuracy of their administrative data can be verified;
- the data subjects may submit other medical opinions to the medical advisors and medical services of the above agencies in order to ensure the completeness of their medical file;

- the medical advisor should ensure that no comment or annotation should be added to any medical form by any third party.

Komisyon'un tıbbi hizmetlerinin bazı veya tüm tıbbi muayeneleri bazı kurum personeli için gerçekleştirdiği ve tıbbi dosyalarının Komisyon'un tıbbi hizmetlerinde tutulduğu durumlarda, özellikle REA, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, EACI ve EMSA gibi kurumlar, veri konularının tıbbi dosyalarının doğruluğu ile ilgili olarak yukarıdaki uygulamalardan haberdar olduğundan emin olmalıdır.

FRA, tüm tıbbi muayeneleri gerçekleştirmek için bir işlemci ile sözleşme imzalarsa yukarıdaki önerileri dikkate almalıdır.

Çalışanların hastalık izni aldığı durumlarda sağlıkla ilgili idari verilerin elektronik olarak toplandığı durumlarda, ETF, ECDC, FRA, REA, ERA, EAHC, CFCA, FRONTEX, EU-OSHA, EACI, EEA, EUROFOUND ve EMSA, kullanıcı işlemlerinin izlenebilirliğini sağlamak için bir denetim izi olup olmadığından emin olmalıdır (güvenlikle ilgili sorun, 2.10. maddeye bakınız).

2.5. Verilerin Saklanması

Regülasyon 45/2001'in 4(1)(e) maddesi, *"kişisel verilerin, verilerin toplandığı veya daha fazla işlendiği amaçlar için gerekli olmadıkça veri konularının kimliğini belirlemenizi sağlayan bir şekilde saklanması gerektiğini belirtir*".

EDPS, genel olarak, dosyaya yerleştirilen son tıbbi belge tarihinden itibaren 30 yılın, bu bağlamda tıbbi verilerin saklanması için mutlak maksimum süre olarak kabul edilmesi gerektiğini belirtmek istemektedir, bu süre her saklama süresinin Regülasyonun 4(1)(e) maddesi ışığında değerlendirilmesi ve belirlenmesi gerekmektedir. EDPS, 26 Şubat 2007 tarihli mektubunda Başkanlar Kurulu'na önerdiği gibi, tıbbi belgelerin doğası, uygulanabilir kurallar ışığında incelenerek her belge türü için hangi saklama sürelerinin uygun olacağını belirlemek önemlidir. Bu nedenle, bir personelin istihdam dönemi sırasında ve sonrasında çeşitli tıbbi belgelerin ne ölçüde ve hangi amaçlarla saklanması gerektiği incelenmelidir. Önemli bir not olarak, Başkanlar Kurulu 11 Ekim 2010 tarihinde EDPS'ye, belirli tıbbi belgeler için özel saklama süreleri hakkında bir danışma göndermiş olup, EDPS ve Başkanlar Kurulu'nun ilgili alt komitesi arasında yapılan görüşmelerin ardından, EDPS yakında 26 Şubat 2007 tarihli mektubu ve önceden kontrol edilen görüşlerini dikkate alarak danışmasını yayımlayacaktır.

Bu konuda yanlış anlamaları önlemek ve herhangi bir belirsizliği ortadan kaldırmak adına, EACI'nin gizlilik bildirisine eklemesi gereken bir madde olduğunu belirtmek istiyorum: "Tıbbi veriler, "Regülasyonun 4(1)(e) maddesi ışığında son tıbbi belgenin dosyaya yerleştirilmesinden itibaren maksimum 30 yıl saklanır." EACI, hastalık izni ve işe alınmayan kişilerle ilgili özel veri saklama sürelerini EDPS'nin Rehberlerine uygun olarak belirlemelidir.

EDPS, ECDC'nin işe alınmış ve alınmamış kişilerin uygunluk sertifikalarını ("sağlık sertifikaları") maksimum otuz yıl süreyle sakladığını belirtiyor.

Ayrıca, EUROFOUND "ön alım sertifikasının bir kopyasını kişisel dosyada kalıcı olarak saklar. Orijinal belge ise tıbbi dosyada tutulur. Tıbbi dosya, bir personelin kişisel dosyasının bir parçası olarak kalıcı olarak saklanır."

ECHA, bildiriminde "personelin tıbbi dosyalarının, istihdam sözleşmesinin sona ermesinden itibaren 10 yıl boyunca saklandığını" belirtmiştir.

EASA da bildiriminde, "sona eren istihdam sözleşmesinin tarihinden itibaren 10 yıl boyunca saklanan sonuçların tıbbi dosyada tutulduğunu" belirtmiştir.

EDPS, kurumların işlemcilerinin tıbbi dosyalarda saklanması gereken verilerin, önceden kontrol edilen görüşlerine dayanarak personelin işyerinden ayrılmasından sonraki maksimum 30 yıl süreyle saklanması gerektiğini belirtmektedir. Veri konularının uygunluklarını belirten uygunluk sertifikalarının kişisel dosyada saklanması gerektiğini öneriyor. EDPS'nin personel alımı üzerine Rehberlerinde belirtildiği gibi, kişisel dosyaların, bir personelin aktif istihdam süresinin veya son emekli maaşı ödemesinin sona ermesinden sonra 10 yıl boyunca saklanması önerilir.

Sonuç olarak, ECDC ve EUROFOUND tarafından benimsenen veri saklama süreleri, verilerin toplandığı amaç için aşırı uzun olup ECHA ve EASA tarafından belirtilen saklama süresi yukarıda belirtilen politikalara uygun değildir. EDPS dört ajansı da tıbbi dosyalarda ve kişisel dosyalarda tutulan verileri yeniden değerlendirmeye ve yukarıda açıklandığı gibi uygun veri saklama süreleri belirlemeye davet eder.

Ayrıca, EDPS Kılavuzları doğrultusunda ECDC ve ECHA'nın, kişisel dosyalarda tutulan verilere ilişkin, veri saklama süresi belirlemesi gerektiğini önerir; bu süre zarfında verilere itiraz edilmesi veya olumsuz karar verilmesi mümkün olmalıdır. Bunun yanı sıra, EDPS ECDC ve ECHA'nın hastalık izni verileri ile ilgili belirli bir veri saklama süresi benimsemesini tavsiye eder.

FRA'nın bildirisine göre, ajans, kişisel dosyalarda yer alan kabiliyet sertifikalarını kişisel dosyanın var olduğu sürece belirsiz bir süreyle saklar. EDPS bu süreyi, Tüzük'ün 4(1)(e) maddesi gereğince aşırı ve gereksiz bulur. EDPS, FRA'nın kişisel dosyaları bir personel üyesinin aktif istihdam süresi sona erdikten veya son emeklilik ödemesinden sonraki en fazla 10 yıl süreyle tutmasını önerir.

EAHC'nin, ön alım muayeneleri ile ilgili kabiliyet sertifikalarının kişisel dosyada tutulma süresi ve EDPS Kılavuzları'nda önerilen şekilde ön alım muayeneleri için belirli bir veri saklama süresi benimsemesi gerektiği aynı tavsiyeleri takip etmesi gerektiğini önerir.

ETF'nün, hastalık izni verileri, belirli tıbbi muayene verileri ve ön alım muayeneleri için belirli bir veri saklama süresi ve EDPS Kılavuzları'na uygun olarak ön alım muayenesi olmayan kişiler için belirli bir saklama süresi benimsemesi önerilir.

REA'nın kendi özel saklama listesini oluştururken, sadece "Ortak Komisyon seviyesi saklama listesi"ni değil, aynı zamanda EDPS'nin Kılavuzlarında yaptığı önerileri de dikkate alması gerektiği, özellikle sağlıkla ilgili veriler (kabiliyet sertifikaları ve tıbbi sertifikalar), hastalık izni ve gerekirse belirli tıbbi muayeneler için hem alınmış hem alınmamış kişiler için saklama süreleri belirlemesi önerilir. Liste benimsendiğinde EDPS bilgilendirilmelidir.

TEN-T, hastalık izni ve alınmamış kişilerle ilgili verilere ilişkin saklama sürelerini bildirdi ve makul olduğu görünmektedir. EDPS bu saklama sürelerinin hem bildirimde hem de gizlilik bildiriminde belirtilmesini önerir.

FRONTEX'in EDPS Kılavuzları ışığında alınmamış kişilerle ilgili sağlıkla ilgili verilere yönelik bir saklama süresi belirlemesi gerekmektedir.

ERA ve EU-OSHA'nın, Staff Regulations'ın 59(4) maddesi ve EDPS Kılavuzları doğrultusunda hastalık izni ile ilgili verilere özel bir saklama süresi belirlemesi gerekmektedir.

Regülasyon'a göre, EEA, aşağıdaki veriler için saklama sürelerini belirtmemiştir:

- Kişisel dosyalardaki uygunluk sertifikaları,
- Hastalık izni ile ilgili veriler,
- Özel tıbbi muayeneler ve
- İşe alınmayan kişilerin verileri.

EDPS, EEA'nın bu veriler için belirli saklama süreleri benimsemesini önerir ve kurumun dış tıbbi sağlayıcısının, personelin dosyasındaki son tıbbi belgeden itibaren en fazla 30 yıl süreyle personelin tıbbi verilerini saklamasını sağlamasını önerir.

ERA, "tıbbi nedenlerle izin verilerinin istatistiksel amaçlarla anonim olarak işlendiğini" belirtti. Ancak, EDPS, Regülasyon 45/2001'in 4(1)(e) maddesine dikkat çekerek, bu verilerin istatistiksel amaçlarla kullanılması durumunda sadece anonim hale getirildiğinde Regülasyon'un geçerli olmayacağını belirtir. Bu durumda ERA'nın, verilerin istatistiksel amaçlarla kullanılması halinde anonim hale getirilmesini sağlaması gerektiğini belirtir ve ERA'dan bu verilerin anonim hale getirilmesine dair yöntemi gösteren kanıt sunmasını talep eder.

2.6. Veri Transferi

Maddenin kapsadığı işlem, kişisel verilerin diğer Topluluk kurumlarına veya organlarına iç veya dış transferidir. Bu transfer, alıcının yetki kapsamındaki görevlerin meşru yürütümü için verilerin gerekliliği durumunda yapılır.

Kurum içindeki veri iletişimi:

i) Tıbbi faturalar

EDPS, ECDC'nin benimsediği belirli politikayı memnuniyetle karşılıyor. ECDC, denetleyici, kurumın Finans/Muhasebe Bölümüne ödenecek toplam maliyeti iletiliyor. Ayrıca, kurumın bölümünün muhasebe memuru tarafından bir gizlilik beyannamesi imzalanıyor.

FRA, veri konusunun tıbbi uygulayıcısı tarafından doldurulan geri ödeme belgesinin (bildirimin Ek 2'si) kurumın ortak sigorta talepleri ofisine iletilmesini sağlamalıdır.

ETF, FRONTEX, EU-OSHA, EEA ve EASA'dan sağlık verilerinin muhasebe bölümüne geri ödeme bağlamında herhangi bir özel prosedür olup olmadığına dair bilgi sağlanmamıştır. EDPS, yukarıdaki kurumların tüm tıbbi faturaların önce kurumın tıbbi servisine gönderilmesi ve bunların onaylanması, ardından geri ödenecek toplam tutarın bütçe bölümüne iletilmesi için bir prosedür oluşturmalarını ısrarla talep eder.

REA, ERA ve FRONTEX, Komisyon'un tıbbi hizmetinin tüm tıbbi faturaları onaylamasını ve ardından geri ödenecek toplam tutarı gösterecek bir belge doldurmasını sağlayacak bir prosedür oluşturmalıdır. Bu belge, sadece Komisyon'un tıbbi hizmeti tarafından kurumın sorumlu finans departmanına iletilmelidir.

"CEDEFOP'un pozisyonuna ilişkin olarak, Rehberliğin amacının iyi uygulamaları uyumlu hale getirmek ve tüm kurumlar arasında tutarlılık sağlamak olduğunu EDPS hatırlatmaktadır. Bu

nedenle, EDPS, tıbbi faturalara ilişkin politikalarını yeniden gözden geçirmesi ve Rehberlerdeki önerileri benimsemesi için CEDEFOP'u davet etmektedir.

ii) Diğer kurumlara transferler

Ayrıca, diğer kurumlara transferler bağlamında, kurumlar tıbbi dosyaların alıcılarının sadece sağlık verilerine erişimi yetkili ve mesleki gizlilik kurallarına tabi kişiler olmasını sağlamalıdır. Bu, FRA, REA, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, EACI, AB-OSHA, ECHA, EEA ve EASA gibi kurumların, personel üyelerine ait uygunluk belgelerini veya sağlıkla ilgili diğer belgeleri başka bir kuruluşa aktarmaları gerektiğinde yapılmalıdır."

"iii) Yönetmeliğin 7(3) maddesine Uyum

Ayrıca, Yönetmeliğin 7(3) maddesi, 'alıcı, kişisel verileri sadece aktarıldıkları amaçlar için işleyecektir' hükmünü içermektedir. Bildirimlere göre, ETF, ECDC6, FRA, REA, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EEA, EASA ve EMSA, 7(3) maddesinin ilkesine uyulduğunu gösteren herhangi bir belge veya referans sağlamamıştır. EDPS, örneğin her kurum tarafından bir iç not hazırlanması veya potansiyel alıcılar tarafından imzalanacak bir beyanname gibi, alıcıların aldıkları verileri aktarıldıkları amaç dışında herhangi bir amaçla kullanmama yükümlülüğünü açıkça hatırlatan bir yöntemin benimsenmesini önermektedir.

EDPS, yukarıdaki ii ve iii maddelerinin, 2.3 maddesindeki öneriyle birlikte uygulanmasını önermektedir. Bu, ilgili kurumların hem 45/2001 Sayılı Yönetmeliğin 10(3) maddesi hem de 7(3) maddesi ile ilgili olarak personel tarafından imzalanacak iç notlar veya beyannameler hazırlaması gerektiği anlamına gelir."

Dış Transfer

i) Yönetmeliğin 8. Maddesi Işığında Yapılan Transfer

Yönetmeliğin 8. maddesi, 95/46/EC Direktifi'nin uygulanması için alınan ulusal yasaya tabi alıcılara kişisel verilerin nasıl aktarılabileceğini belirtir.

ETF, ECDC, FRA, REA, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, EACI, EU-OSHA, ECHA, EUROFOUND, EEA ve EMSA'nın bildirimleri, Direktif kapsamındaki herhangi bir alıcıya olası bir aktarım hakkında herhangi bir bilgi vermemektedir. Nadiren de olsa bu tür transferler dışlanamaz. Örneğin, kurumların milli bir makam tarafından yürütülen bir soruşturma bağlamında sağlık verilerini ulusal makamlara aktarmaları gerektiği durumlarda, bu aktarımın gerekliliği Yönetmeliğin 8(a) maddesi kapsamında gösterilmelidir. Ayrıca, EDPS, ulusal düzenlemeler tarafından belirlenen tıbbi gizlilikle ilgili gereksinimlerin ve mekanizmaların da ulusal makamlarla işbirliğinde saygı gösterilmesi gerektiğini vurgulamaktadır. Her durumda, yalnızca uygun, ilgili ve gereğinden fazla olmayan verilerin aktarılması temel önem taşır.

ii) Yönetmeliğin 9. Maddesi Işığında Yapılan Transfer

Yönetmeliğin 9. maddesi, 95/46/EC Direktifi'ne göre kabul edilen ulusal yasaya tabi olmayan alıcılara kişisel verilerin aktarılmasına izin verir; ancak bu durumda, üçüncü ülkenin veya kuruluşun yeterli bir koruma düzeyi sağlaması gerekmektedir. Korumanın yeterliliği, 9(2) maddesinde belirtilen kriterler göz önünde bulundurularak değerlendirilmelidir. Özel durumlar 9(6) maddesinde belirtilmiştir.

6 EDPS'nin bildirime göre, ECDC personeline veri işleme konusundaki gizlilik konusunda bilgi verilmiştir. Veri Koruma Sorumlusu tarafından talimat alınmış ve kurum şu anda eğitim/bilgilendirme oturumları düzenleme sürecindedir. Bu gibi uygulamalar teşvik edilir ve tüm kurumlar tarafından benimsenmelidir.

Direktif kapsamı dışında yapılan tüm aktarımlarda, kurumlar 9. Maddeye saygı göstermelidir.

Bu tür bir aktarım durumunda, kurumlar 9. Maddeye uygunluğu sağlamalıdır.

Regülasyonun 13. maddesi, ilgili personelin talebi üzerine izin hakkını belirler ve izlenecek prosedürleri açıklar. Regülasyonun 14. maddesi ise veri konusu olan kişiye hatalı veya eksik kişisel verilerin derhal düzeltilmesi hakkını verir.

2.7. Veri Erişim Hakkı

İşe Alınmış Personel İçin

i) Mantıklı Süre İçinde ve Engelsiz Erişim

Çoğu kurum personelinin tıbbi verilerinin işlenmesini dış kurumlara devreder, bu yüzden kendileri tıbbi dosyaları saklamazlar. Personelin tıbbi dosyasına ve kişisel dosyasına erişim arasında net bir ayrım yapılması önemlidir.

- Personelin Tıbbi Dosyasına Erişim

EDPS, ECHA, EU-OSHA, EEA, EASA ve EMSA'nın dış tıbbi sağlayıcı/advisörleri ile yaptıkları sözleşmelerle erişim taleplerinin, 95/46/EC Direktifi'ne uygun olarak engelsiz bir şekilde ele alınacağı makul bir süreyi sağlamalarını önerir. Bu, veri konularına haklarını bildiren gizlilik beyanlarında açıkça belirtilmelidir (bkz. 2.8. madde).

- Personelin Kişisel Dosyasına Erişim

ETF, ECDC, CEDEFOP, TEN-T, ERA, EAHC, ECHA, EEA ve EMSA, gizlilik beyanlarında veya diğer bildirimlerde, hem ön işe alım muayenelerinden hem de yıllık kontrol muayenelerinden alınan uygunluk belgelerinin makul bir süre içinde ve engelsiz bir şekilde erişilebilir olduğunu açıklamalıdır, bu da 45/2001 Sayılı Yönetmelik'in 13. maddesine uygun olmalıdır.

ii) Anlaşılabilir Biçimde Erişilebilir Veriler

Dış tıbbi sağlayıcılarla çalışan kurumlar - özellikle ECHA, EASA, CEDEFOP, EUROFOUND, EEA, EU-OSHA, EMSA, ECDC ve ETF - tıbbi muayeneleri gerçekleştiren doktorların, veri konularına anlaşılabilir tıbbi sonuçlar sağlamasını sağlamalıdır. Bu, verileri yorumlamayı (tıbbi kodlar veya kan analizi sonuçları gibi) ve veri konuları için anlaşılır hale getirmeyi içerir.

iii) Tıbbi Dosyaların Kopyaları

Tıbbi dosyalarının kopyalarını isteyen veri konuları için, ECHA, EU-OSHA, EASA ve EMSA personelinin tıbbi sağlayıcıları bu talepleri yerine getirmelidir.

ii) Anlaşılabilir Biçimde Erişilebilir Veriler

Dış tıbbi sağlayıcılarla çalışan kurumlar - özellikle ECHA, EASA, CEDEFOP, EUROFOUND, EEA, EU-OSHA, EMSA, ECDC ve ETF - tıbbi muayeneleri gerçekleştiren doktorların, veri konularına anlaşılabilir tıbbi sonuçlar sağlamasını sağlamalıdır. Bu, verileri yorumlamayı (tıbbi kodlar veya kan analizi sonuçları gibi) ve veri konuları için anlaşılır hale getirmeyi içerir.

iii) Tıbbi dosyalarının kopyalarıyla ilgili talepler için, ECHA, EU-OSHA, EASA ve EMSA, personellerinin tıbbi uzmanlarının bu talepleri karşıladığından emin olmalıdır.

iv) Psikolojik veya Psikiyatrik Verilere Erişim

Psikolojik veya psikiyatrik nitelikteki verilerle ilgilenirken, ETF, ECDC, REA, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EASA ve EMSA, veri konusu kişinin korunması için duruma göre belirlenen hallerde (Yönetmeliğin 20.1.c maddesi), veri konusu kişinin korunması için dolaylı erişimin gerekli olduğu belirlenirse, dolaylı erişim imkanını sağlamalıdır. Dolaylı erişim imkanları, 19 Şubat 2004 tarihli 221/04 sayılı Kararlar ışığında değerlendirilmeli ve bu ajanslar, veri konusu kişilere bu olanaklar hakkında bilgi vermeleri gerekmektedir (2.8 numaralı bölüme bakınız).

Eğitilmemiş Personel, Ziyaretçiler, Stajyerler

ECDC, REA, TEN-T, ERA, EAHC, CFCA, FRONTEX, ECHA, EU-OSHA, EACI, EASA ve EMSA, sağlıkla ilgili işlenmiş verilerine dair bu kategorideki veri konularına talep üzerine erişim hakları sunmalıdır. Bu bilgi, gizlilik bildiriminde detaylı bir şekilde yer almalıdır.

Doğrulama Hakkı

ETF, FRA, REA, CEDEFOP, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, ECHA, EU-OSHA, EUROFOUND, EEA, EASA ve EMSA, veri konularının, muhtemelen gizlilik bildiriminde bilgi vererek, verilerini düzeltme hakkının farkında olmalarını sağlamalıdır. Bu hak, tıbbi dosyalarındaki idari hataları düzeltmeyi ve diğer doktorlardan ikinci görüşleri eklemeyi içerir.

2.8. Veri Konusu Kişiye Verilecek Bilgiler

Regülasyon 45/2001'in 11. ve 12. maddeleri, ilgili verilerin işlenmesine ilişkin veri konusu kişilerin bilgilendirilmesini öngörür ve genel ve ek bilgi maddelerini listeler. Ek maddeler, işleme operasyonunun özel koşullarını göz önünde bulundurarak, veri konusu kişinin adil işlenmesini garanti etmek için gerekli olduğu ölçüde geçerlidir. Bu durumda, tıbbi veriler kısmen veri konusu kişi tarafından ve kısmen de Komisyon'un tıbbi hizmetleri veya dış doktorlar ve tıbbi sağlayıcılar tarafından sağlanır.

Gizlilik Bildirimi

ETF'nin EDPS'ye gönderdiği mektubun 1.7 noktası, bilgi hakkına ilişkin değildir. Ayrıca, ETF, bildirimde 11. ve 12. maddeler altındaki tüm bilgi unsurlarını listelediği halde, ilgili kişilere bu hükümler altındaki ilgili bilgiyi açıklayan bir gizlilik bildirimi hazırlamamıştır. Bu nedenle EDPS Kılavuzları doğrultusunda, ETF'yi, veri konusu kişilere kolayca erişilebilir bir gizlilik bildirimi sağlamaya ve 11. ve 12. maddeler altındaki tüm bilgiyi açıklamaya davet eder.

ECDC, veri konusu kişilere ait ön işe alım ve yıllık tıbbi muayene ile ilgili veri saklama sürelerini (yukarıda 2.5 noktasına bakınız) düzeltmeli ve ilgili veri konusu kişilere dış tıbbi servisin tıbbi dosyalarını, kişisel dosyaların ise kurumın insan kaynakları tarafından saklandığını netleştirmelidir.

FRA, REA, TEN-T, FRONTEX, EU-OSHA, EUROFOUND, EEA ve EASA, 11. ve 12. maddeler altında sağlanan veri konusu kişi haklarını listeleyen bir gizlilik bildirimi hazırlamalıdır ve bu işlemi en kısa sürede gerçekleştirmelidir.

CEDEFOP, 11 ve 12. maddeler uyarınca dahil etmeyi düşündüğü bilgiyi gizlilik bildirisine dahil etmektedir. Uygun tüm bilgilere kapsamlı bir şekilde atıfta bulunan bir gizlilik bildirisinin kopyası hazırlandığında, bunun EDPS'ye gönderilmesi tavsiye edilir.

EDPS, ERA tarafından sunulan "özel gizlilik beyanı e-HR"nin kurum tarafından gerçekleştirilen sağlıkla ilgili veri işlemeyle ilgili olmadığını buldu. Bu nedenle, kurum tarafından gerçekleştirilen özel işlemlerle ilgili uygun bir gizlilik beyanı hazırlanmasını önerilir. Bu, 11 ve 12. maddeler altında veri konusu kişilere tüm ilgili bilgileri açıkça açıklamalıdır.

EAHC, bildirimde ilgili bilginin intranetlerinde bulunabileceğini belirtti. EMSA, EDPS'ye, 11 ve 12. maddelerle ilgili olmayan bazı belgelerin intranet bağlantılarını sağladı. Bu nedenle, hem EAHC hem de EMSA'nın ön işe alım, yıllık kontrol ve hastalık izni işlemleriyle ilgili bir gizlilik beyannamesi hazırlaması için davet edilir. Bu gizlilik beyannamesi, 11 ve 12. maddeler altında belirtilen veri konusu kişi bilgi haklarına ilişkin net ve detaylı bilgi sağlamalıdır.

CFCA tarafından işlemin amacı, "CFCA personeli ve SNE'lerin hak ve yükümlülüklerini yönetmek" olarak tanımlanmıştır. Bu tanım belirsiz ve yanıltıcı olabilir. EDPS, kurumın verileriyle ilgili işleme bağlı olarak kurum personelinin hak ve yükümlülüklerini içeren bir cümle/klazül eklemesini önerir.

EDPS, ERCEA'nın gizlilik beyanının, kurum tarafından işlenen sağlıkla ilgili verileri içermemesi nedeniyle yetersiz olduğunu buldu. Sonuç olarak, EDPS, analiz edilen özel işlemlerle ilgili 11 ve 12. maddelerde listelenen tüm hakları içeren uygun bir gizlilik beyannamesinin hazırlanmasını önerir.

ECHA, ön işe alım muayenelerine ilişkin olarak veri konusu kişilere yapılan davetiyelerde veri koruma bildirimine yer verdi. Aynı veri koruma hükümleri, yıllık kontrol, tıbbi tedavi için özel izin ve işyerinden uzakta hastalık izniyle ilgili davetiyelerde de belirtilmiştir.

ECHA, dış tıbbi danışman tarafından gerçekleştirilen tıbbi muayenelere ilişkin bir veri koruma bildirimi hazırlamalıdır.

ECHA, EDPS'nin erişim ve düzeltme hakkına ilişkin önerilerini (yukarıdaki 2.7. noktaya bakınız) tüm veri koruma bildirimlerine eklemelidir. Ayrıca, EDPS Sağlık Verileri ile İlgili Kılavuzlar ışığında aşağıdaki bilgileri de eklemelidir:

- Sağlık verileri işlemine ilişkin yasal dayanak;
- Dış tıbbi danışman tarafından tutulan sağlık verilerinin, işe alınan ve alınmayan kişiler için saklama süresi;
- Hastalık izniyle ilgili verilerin saklama süresi ve
- Veri konusu kişilerin her zaman EDPS'ye başvurma hakkı.

EDPS, tüm kurumlara gizlilik beyanının yalnızca yeni işe alınan tüm personele (REA bildiriminde belirtildiği gibi) değil, kurumların tüm personeline hitap etmesi gerektiğini belirtmektedir. Örneğin, kurumun web sitesinde kolayca erişilebilir olmalıdır.

"Verilmesi Gereken Ek Bilgiler:"

Makale 11 ve 12'de listelenen haklarının yanı sıra, gizlilik beyannamesi, analiz edilen işlemlerle ilgili bazı ek bilgileri sağlamalıdır. EDPS, sağlık verileri üzerine olan kılavuzlarında vurguladığı önerileri yeniden belirtir.

REA, TEN-T, ERA, ERCEA, FRONTEX, EAHC, EU-OSHA, EUROFOUND, EEA, CEDEFOP, EASA ve EMSA, ön işe alım muayenelerini, yıllık ve diğer kontrolleri kimin (Komisyonun tıbbi hizmeti, harici sağlayıcı, kurumın doktoru) gerçekleştirdiği ve personelin tıbbi dosyalarının nerede tutulduğu konusunda gizlilik beyannamesinde açıklama yapmalıdır.

REA, CEDEFOP, TEN-T, ERA, EAHC, ERCEA, FRONTEX, EU-OSHA, EUROFOUND ve EEA, kurumların İK birimleri tarafından saklanan ve hangi amaçlarla sağlıkla ilgili hangi verilerin toplandığını ve saklandığını daha da belirtmelidir.

Tıbbi anketler

ETF, "sorveglianza sanitaria" ve "visite periodiche" adlı iki anketinde (kurumın tıbbi danışmanı tarafından yıllık kontrol sırasında kullanılan) sorulara verilen cevapların gönüllü mü yoksa zorunlu mu olduğunu ve cevap verilmemesinin olası sonuçlarını belirtmelidir.

Tıbbi kontroller

i) Özel bir tıbbi uygulayıcı seçimi

Tıbbi kontrollerde, ETF, REA, TEN-T, ERA, EAHC, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EEA, EASA ve EMSA, veri konusu kişilerin kendi özel uygulayıcılarını seçme hakkını ve tercih ettikleri uygulayıcıyla kontrolleri gerçekleştirmek için almaları gereken pratik adımları açıklamalıdır.

ii) Tıbbi muayene sonuçlarının aktarımı

Ayrıca, ETF, REA, CEDEFOP, TEN-T, ERA, EAHC, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EEA, EASA ve EMSA, gizlilik beyannamesinde, veri konusu kişinin özel tıbbi uygulayıcısının, tıbbi muayene sonuçlarını kurumın doktoruna, Komisyonun tıbbi hizmetine veya başka bir harici tıbbi sağlayıcıya iletip iletmemesi gerekip gerekmediğini ve eğer öyleyse hangi amaçla ileteceğini belirtmelidir. Kılavuzlarda açıklandığı gibi, EDPS yıllık bir kontrolün tıbbi sonuçlarının, veri konusu kişinin özgür iradesi ve bilgi sahibi rızası olmadan kurumın doktoruna veya Komisyonun tıbbi hizmetine iletilmemesi gerektiğinde ısrar etmelidir.

iii) Dolaylı olarak psikolojik veya psikiyatrik verilere erişim

Son olarak, EDPS, ETF, ECDC, FRA, REA, CEDEFOP, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EEA, EASA ve EMSA'nın, 19 Şubat 2004 tarihli 221/04 Sayılı Sonuçlar doğrultusunda, veri konusu kişilere psikolojik veya psikiyatrik verilere dolaylı erişim olasılıkları hakkında gizlilik beyannamesi veya iç not ile bilgi vermesini önermektedir.

2.9. Güvenlik

45/2001 Sayılı Yönetmeliğin 22. maddesine göre, "veri sorumlusu, işlenen verilerin temsil ettiği risklere ve korunması gereken kişisel verilerin doğasına uygun bir güvenlik seviyesini sağlamak için uygun teknik ve organizasyonel önlemleri uygulamalıdır".

EDPS, Komisyon'un, EACI, EAHC, ERCEA, REA ve ERA gibi bir dizi kurumla Avrupa Komisyonu Bilgi Sistemleri Güvenlik Politikası'nın uygulanmasına ilişkin bir "Bilgi Alışverişi Anlaşması" (MoU) imzaladığını belirtmektedir. Ayrıca, ERCEA, Yerel Bilgi Güvenliği Görevlisi tarafından Bilgi

Teknolojisi Güvenlik Politikası hazırlığına ilişkin kısa bir "durum tespiti" sağlamıştır. Ancak bu MoU, kurumun kendi IT güvenlik politikasını veya Yönetmelik kapsamında benimsemeleri gereken herhangi bir güvenlik önlemini sağlamak amacıyla oluşturulmamıştır veya yerine geçmemektedir.

2.4'te belirtildiği gibi, ETF, ECDC, FRA, REA, ERA, EAHC, CFCA, FRONTEX, EU-OSHA, EACI, EUROFOUND, EEA ve EMSA, özellikle sağlıkla ilgili yönetimsel verilerin elektronik olarak toplandığı hastalık izni durumlarında kullanıcı hareketlerini izlemek için bir denetim izi benimsemediği görünmektedir. Bu güvenlik önlemi, Yönetmeliğin 22. maddesinde belirtilen teknik ve organizasyonel önlemlere uygun olarak uygulanmalıdır.

Ayrıca, EDPS birkaç kurumun bilgi ve iletişim BT politikalarıyla ilgili belgeler sunduğunu belirtmektedir. Ancak bu belgeler, Yönetmeliğin özel gereksinimlerine uygun değildir. Sonuç olarak, EDPS tüm kurumların, Yönetmeliğin 22(2)(a - j) maddesinde belirtilen unsurlar listesini dikkate alarak kendi özel güvenlik politikalarını benimsemelerini önermektedir. Bu özel güvenlik politikası, her kurum tarafından yürütülecek bir risk değerlendirme çalışmasına dayandırılmalı ve kurumun mekânlarında gerçekleştirilen tıbbi ve/veya sağlıkla ilgili veri işleme faaliyetlerinin bir çerçevesinde uygulanmalıdır. Her kurum, özel güvenlik önlemlerinin bir kopyasını EDPS'ye göndermelidir.

2.10. Taşeronluk

Yönetmeliğin 23. maddesi doğrultusunda, kurumlar, tıbbi verilerin işlenmesi çerçevesinde yeterli teknik ve organizasyonel güvenlik önlemlerini sağlayabilecek bir işlemci seçmelidir.

EDPS üç alt taşeronluk kategorisi belirlemiştir:

i) Komisyon'un tıbbi servisi kuruma işlemci olarak hareket eder ve işlem SLA ile düzenlenir,

ii) Harici bir tıbbi merkez, kurum adına bazı veya çoğu tıbbi muayeneleri gerçekleştirir ve

iii) Tıbbi danışman, kurum adına tıbbi verileri kurumun mekânlarında işler.

EDPS, güvenlik önlemlerinin uygulanma şeklinin, yukarıdaki taşeronluk kategorilerinin her birinde farklı olduğunu vurgulamaktadır:

- SLA durumunda, güvenlik önlemleri zaten Komisyon'da mevcuttur. Bununla birlikte, kurumların kendi mekânlarında da bir güvenlik sistemi sağlaması gerektiği anlamına gelmez (bkz. yukarıdaki 2.9 madde);
- kurumların harici tıbbi merkezlerle sözleşme imzaladığı durumlarda, harici yüklenici tarafından uygun bir güvenlik seviyesinin Yönetmeliğin 23(2)(b) ve 23(3) maddeleri uyarınca benimsenip uygulandığından emin olmaları gerekir; ve
- Tıbbi danışmanların kurumların mekânlarında görevlerini yerine getirdiği durumlarda, kurumlar, sözleşme ile tıbbi danışmanın, kurumun iç güvenlik önlemlerine saygı göstermesini

sağlamalıdır. Bu önlemler, Yönetmeliğin 22. maddesine uygun olmalıdır, zira 23(1) maddesi bunu sağlar.

Özellikle, EU-OSHA, harici tıbbi servisle kurum arasında Yönetmeliğin 23. maddesine uygun olarak bir sözleşme veya diğer yasal olarak bağlayıcı bir belge oluşturmalıdır. Bu yasal belge, işlemcinin yalnızca kurumın talimatlarına göre hareket etmesi gerektiğini sağlamalıdır. Ayrıca, sağlayıcı, 95/46/EC Sayılı Direktif'in 16. veya 17(3), ikinci sıra kapsamındaki ulusal hukuka tabi olacak ve güvenlik ve gizlilikle ilgili ulusal hukuk hükümlerine uyulmasını sağlamak zorunda kalacaktır. EU-OSHA, bu unsurları içeren sözleşmenin bir kopyasını oluşturulduğunda derhal EDPS'ye göndermelidir.

EAHC ve EASA, 2006'da Komisyon'un Lüksemburg'daki tıbbi servisi ile bir SLA imzaladılar. Ancak bu SLA, Yönetmeliğin uygulanabilirliğine atıfta bulunmamaktadır. EDPS, ilgili kurumların 2008'de Brüksel'deki Komisyon tıbbi servisiyle imzaladıkları SLA'ların Yönetmelik 45/2001'e atıfta bulunduğunu vurgulamaktadır. Bu nedenle, EAHC ve EASA'nın Lüksemburg'daki Komisyon tıbbi servisi ile SLA'larını güncellemeleri ve tıbbi servisin Yönetmeliğin hükümlerini uyguladığını belirtmeleri önerilmektedir.

"ETF, ECHA, CEDEFOP, EUROFOUND ve EASA'nın dış tıbbi hizmet sağlayıcıları ve danışmanları ile olan sözleşmeleri, işleyici konumunda benzerlikler taşımaktadır. EDPS, bu sözleşmelere aşağıdaki hususların eklenmesini önermektedir:"

- Harici tıbbi merkezlerle yapılan sözleşmeler için, ECHA, EASA ve EMSA'nın ajansın gerektirdiği güvenlik önlemlerini net olarak belirten bir ek bulunmalıdır. Bu önlemler, Yönetmelik'in 23(2)(b) ve 23(3) maddelerine uygun olmalıdır.

- ETF, ECHA ve EASA'nın medikal danışmanlarla yaptığı sözleşmeler, ajansın kendi tesislerinde uyguladığı güvenlik önlemlerini içermelidir. Her iki ajans da medikal danışmanın, Yönetmelik'in 23(1) maddesi gereğince belirlenen güvenlik seviyesine uymasını sağlamalıdır.

- Veri koruma ile ilgili sözleşmelerin I.9. maddesine ilişkin olarak, yalnızca yüklenicinin kişisel verilerine ve erişim haklarına atıfta bulunmak yeterli değildir. Sözleşme yürütmesinde yer alan veri konuları açıkça belirtilmelidir. Bu nedenle, ETF, ECHA, EASA ve EMSA tarafından "Yüklenici" ifadesine atıfta bulunulan herhangi bir yerde, "Yüklenici tarafından işlenen verileri içeren veri konuları" ifadesi eklenmelidir.

Ek olarak, EUROFOUND'un sözleşmesindeki Madde I.8'i "Yüklenici tarafından işlenen verileri içeren veri konuları" ifadesini içerecek şekilde değiştirmesi gerekmektedir.

ECDC ve CEDEFOP'un harici tıbbi sağlayıcılarla yaptıkları sözleşmelere bir veri koruma maddesi eklemesi ve 23(2)(b) ve 23(3) maddelerine uygun güvenlik önlemlerini belirten bir ek eklemesi gerekmektedir.

EEA (Avrupa Çevre Ajansı) için harici tıbbi sağlayıcı ile yapılan sözleşme sunulmadığından, Yönetmelik'in 23. maddesi gerekliliklerine uygunluğun sağlanması ve sözleşmenin incelenmesi için bir kopyasının iletilmesi önerilmektedir.

"Sonuç olarak, EDPS Rehberleri, kurumların ön eleme muayeneleri, yıllık sağlık kontrolleri ve hastalık izinleriyle ilgili veri koruma prensiplerinin 45/2001 Sayılı Yönetmelik kapsamındaki etkilerini düşünmeleri için yararlı bir araç oldu. 2.1 maddesinde belirtildiği gibi, "sağlık verileri" kapsamının geniş anlamını EDPS Rehberleri'nde net bir şekilde açıklanmasına rağmen, bazı kurumlar işledikleri verilerin Yönetmelik'in 27(2)(a) maddesi altında belirli riskler taşımadığını iddia etti.

EDPS, mevcut analizden türetilen iki diğer konuya özellikle dikkat çekmektedir: dış kaynak kullanımının yasal dayanağı ve gizlilik bildirimi. EDPS, bazı kurumların dış sağlayıcılarla yaptıkları sözleşmelerden ortak unsurları atladıklarını, özellikle güvenlik önlemleri ve veri koruma maddelerini. Bu, işlemcinin bulunduğu sözleşmelere dahil edilmesi gereken temel unsurlardır.

Ayrıca, kurumların gizlilik bildiriminin önemini kavrayamadığını gözlemliyoruz. EACI dışında, neredeyse tam bir gizlilik bildirimi oluşturan kurum yoktur. EDPS, veri konusunun yasallığı için veri konusunun tamamen bilgilendirilmesi gerektiğini vurgular ve bu nedenle bunun, Yönetmelik'in 11 ve 12. maddelerine uygun olarak sağlanan bilgilere dayandığını belirtir. Bundan dolayı, işlemcinin başlamadan önce veri konularına, işleme ve bunlarla ilgili haklarına dair gerekli tüm bilgileri sağlaması gerektiği açıktır. Bu özellikle işlemin veri konusunun onayına dayandığı durumlarda geçerlidir.

DPO'ların başvuru mektuplarını, bildirimlerde belirtilen bilgileri ve yorumlarını göz önünde bulundurarak, EDPS, belirli bir veri koruma uygulamasının EDPS Rehberleri ve önerilerine uygun olarak uygulanacağını belirtmek yeterli olmadığını vurgulamak gerektiğini düşünmektedir. Bunun yerine, somut önlemler gereklidir. EDPS'nin görüşünün yayınlanmasından ve kontrolörün bunu tamamen dikkate almasından sonra, kontrolörün derhal uygulamak üzere somut önlemler alması ve bu önlemleri EDPS'ye bildirmesi gerekmektedir. Bu prosedürün bir parçası,

önceden kontrol gerektiren bir işlemin EDPS önerilerinin izlenmesidir. İzleme işlemi, görüşün yayınlanmasından itibaren 3 ay içinde gerçekleşmelidir.

Bu nedenle, 45/2001 Sayılı Yönetmelik kapsamındaki her kurumun denetleyicisi, sağlık verilerinin işlenmesine ilişkin EDPS önerilerini uygulamak için özel ve somut önlemler almak üzere davet edilmektedir. Bunun anlamı, izlemenin bağlamında, her kurumun EDPS önerilerinin gerçekten uygulandığını gösteren belgeleri EDPS'ye sunması gerektiğidir."

"Brüksel'de Yapıldı,

Giovanni BUTTARELLI

Avrupa Veri Koruma Görevlisi Yardımcısı

8 45/2001 Sayılı Yönetmeliğe Uyumun İzlenmesi ve Sağlanması Politika Belgesi, Brüksel, 13 Aralık 2010, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_EN.pdf."