

KİŞİSEL VERİLERİN COVID-19 SALGINI KAPSAMINDA İŞLENMESİ HAKKINDA AÇIKLAMA

19 Mart 2020 tarihinde Avrupa Veri Koruma Kurulu aşağıdaki açıklamayı kabul etmiştir:

Avrupa'daki hükümetler, kamu ve özel kuruluşlar COVID-19'u kontrol altına almak için önlemler almaktadırlar. Bu önlemler kapsamında da farklı türdeki kişisel veriler işlenebilmektedir.

Veri koruma düzenlemeleri (GDPR gibi) koronavirüs pandemisine karşı mücadelede alınan önlemleri engellememektedir. Bulaşıcı hastalıklarla mücadele tüm uluslar tarafından paylaşılan değerli bir hedeftir ve bu nedenle mümkün olan en iyi şekilde desteklenmelidir. Dünyanın büyük bölgelerini etkileyen belalarla mücadelede hastalıkların yayılmasını engellemek ve modern teknikleri kullanmak insanlığın yararınadır. Buna rağmen Avrupa Veri Koruma Kurulu, bu istisnai zamanlarda bile, veri sorumlusunun ve veri işleyenin, veri ilgililerinin kişisel verilerinin korunmasını sağlamaları gerektiğini vurgulamak istemektedir.

Bu nedenle, kişisel verilerin hukuki olarak işlenmesini garanti altına almak için bir dizi husus dikkate alınmalı ve her durumda alınan herhangi bir önlemin genel hukuk ilkelerine uyması ve geri döndürülemez olmaması gerektiği unutulmamalıdır. Acil durum, bu kısıtlamaların acil durumla orantılı ve sınırlı olması koşuluyla, özgürlük kısıtlamalarını meşrulaştırabilecek yasal bir durumdur.

1. Veri İşlemenin Hukukiliği

GDPR geniş kapsamlı bir düzenlemelidir ve aynı zamanda kişisel verilerin COVID-19 gibi durumlarda işlenmesi bakımından geçerli olan kuralları öngörmektedir. GDPR, halk sağlığı otoriteleri ve işverenlerinin kişisel verileri ulusal yasalara uygun olarak ve burada belirtilen koşullar çerçevesinde bir salgın bağlamında işlemesine izin verir. Örneğin, halk sağlığı alanında önemli bir kamu yararı nedeniyle veri işlemenin gerekli olması gibi. Bu koşullar altında, veri ilgililerinin açık rızasına dayanmaya gerek yoktur.

1.1 Avrupa Veri Koruma Kurulu, kamu otoriteleri (örneğin halk sağlığı otoriteleri) tarafından özel veri kategorileri de dahil olmak üzere kişisel verilerin işlenmesine ilişkin olarak, kamu otoritesinin (özellikle de ulusal mevzuat ve GDPR'da öngörülen şartlar tarafından sağlanan) yasal yetkisi kapsamına girdiğinde, GDPR'ın 6. ve 9. maddelerinin kişisel verilerin işlenmesini sağladığını düşünmektedir.

1.2.İstihdam bağlamında, kişisel verilerin işlenmesi, işverenin tabi olduğu (sağlık ve güvenlikle ilgili yükümlülükler gibi) yasal bir zorunluluğa uymak için ya da kamu yararı için (hastalıkların ve sağlığa yönelik diğer tehditlerin kontrolü) gerekli olabilir.

GDPR ayrıca, Birlik hukuku veya ulusal hukuk kapsamında, (Madde 9/2/c) halk sağlığı alanında önemli olduğu ölçüde kamu yararı nedeniyle (Madde 9/2/i) veya veri ilgilisinin hayati

çıkarlarının korunması gerektiğinde (Gerekçe 46 açıkça bir salgının kontrolünü ifade etmektedir.) sağlık verileri gibi özel nitelikli kişisel verilerin işlenmesini yasaklayan kuralların derogasyonunu öngörür.

1.3 Yer verileri gibi telekomünikasyon verilerinin işlenmesiyle ilgili olarak, e-Gizlilik Direktifini uygulayan ulusal yasalara da uyulmalıdır. Prensip olarak, konum verileri yalnızca anonim hale getirildiğinde veya kişilerin rızasıyla operatör tarafından kullanılabilir. Ancak, e-Gizlilik Direktifinin 15. maddesi, Üye Devletlerin kamu güvenliğini korumak için yasal önlemler almalarını sağlamaktadır.

Bu tür istisnai mevzuat ancak demokratik bir toplumda gerekli, uygun ve orantılı bir önlem teşkil ediyorsa mümkündür. Bu önlemlerin Avrupa Temel İnsan Hakları Bildirgesi'ne ve Avrupa İnsan Hakları Sözleşmesi'ne uygun olması gerekmekte olup, alınan önlemler Avrupa İnsan Hakları Mahkemesi'nin denetimine de tabidir. Acil durumda alınan bu önlemlerin, acil durumun süresiyle sınırlı kalması gereklidir.

2. Kişisel verilerin işlenmesine ilişkin temel ilkeler

İzlenen hedeflere ulaşmak için gerekli olan kişisel veriler, belirtilen ve açık amaçlar için işlenmelidir.

Buna ek olarak, veri ilgilileri, toplanan verilerin saklanma süresi ve işlemenin amaçları da dahil olmak üzere yürütülen işleme faaliyetleri ve ana özellikleri hakkında şeffaf bilgiler almalıdır ve bu bilgiler kolayca erişilebilir, açık ve anlaşılır bir dilde sunulmalıdır.

Kişisel verilerin yetkisi olmayan kişilere açıklanmasını engelleyen yeterli güvenlik önlemleri alınmalı ve gizlilik politikaları benimsenmelidir. Mevcut acil durum ve karar alma sürecini yönetmek için alınan önlemler uygun bir şekilde belgelenmelidir.

3. Mobil konum verilerinin kullanımı

- Üye Devlet hükümetleri, COVID-19'un yayılmasını izlemek, kontrol altına almak veya hafifletmek için bireylerin cep telefonlarıyla ilgili kişisel verileri kullanabilir mi?

Bazı Üye Devletlerde, hükümetler COVID-19'un yayılmasını izlemek, kontrol altına almak veya hafifletmek için mobil konum verilerini olası bir yol olarak kullanmayı öngörmektedir. Bu, örneğin, bireyleri coğrafi olarak konumlandırma veya belirli bir alandaki kişilere telefon veya kısa mesaj yoluyla halk sağlığı mesajları göndermek anlamına gelmektedir. Kamu otoriteleri önce konum verilerini, belirli bir konumdaki mobil cihazların toplanması/konsantrasyonu hakkında raporların oluşturulmasını sağlayabilecek ("haritacılık") şekilde, anonim bir şekilde işlemeye çalışmalıdır (yani, bireylerin yeniden tanımlanamayacak şekilde toplanan verileri işlemelidir).

Kişisel veri koruma kuralları, uygun şekilde anonimleştirilmiş veriler için geçerli değildir.

Yalnızca anonim verilerin işlenmesi mümkün olmadığında, e-Gizlilik Direktifi Üye Devletlerin kamu güvenliğini korumak için yasal tedbirler almalarını sağlar (Madde 15).

Anonimleştirilmemiş konum verilerinin işlenmesine izin veren tedbirler getirilirse, bir Üye Devlet, elektronik iletişim hizmetleri sağlanan bireylere yargıya başvurma hakkı gibi yeterli önlemleri almakla yükümlüdür.

Orantılılık ilkesi de aynı zamanda geçerlidir. Ulaşılabilecek özel amaç dikkate alınarak daima en az müdahaleci çözümler tercih edilmelidir. Bireylerin “izlenmesi” (ör. Anonimleştirilmemiş konum verilerinin işlenmesi) gibi invaziv/müdahaleci önlemler, ancak istisnai koşullar altında ve işlemenin somut yöntemlerine bağlı olarak orantılı olarak değerlendirilebilir.

Bununla birlikte, veri koruma ilkelerine (tedbirin süre ve kapsam açısından orantılılığı, sınırlı veri saklama ve amaç sınırlaması) uyulmasını sağlamak için tüm bunlar incelemelere ve güvencelere tabi olmalıdır.

4. İstihdam

- Bir işveren ziyaretçilerin veya çalışanların COVID-19 bağlamında belirli sağlık bilgileri vermelerini isteyebilir mi?

Orantılılık ve veri minimizasyonu ilkesinin uygulanması burada özellikle önemlidir. İşveren yalnızca ulusal yasaların izin verdiği ölçüde sağlık bilgisine ihtiyaç duymalıdır.

- Bir işverenin çalışanlar üzerinde tıbbi kontroller yapmasına izin var mıdır?

Cevap, istihdam veya sağlık ve güvenlikle ilgili ulusal yasalara dayanmaktadır. İşverenler sağlık verilerine yalnızca kendi yasal yükümlülükleri gerektiriyorsa erişmeli ve işlemelidir.

- Bir işveren, bir çalışanın meslektaşlarına veya bunlar dışındaki kişilere COVID-19 bulaştığını açıklayabilir mi?

İşverenler personeli COVID-19 vakaları hakkında bilgilendirmeli ve koruyucu önlemler almalı, ancak gereğinden fazla bilgi iletmemelidir. Ulusal yasaları izin verdiği ve açıklamanın gerekli olduğu hallerde ilgili çalışanlara önceden bilgi verilirse onurları ve dürüstlükleri korunmuş olacaktır.

- COVID-19 bağlamında işlenen hangi bilgiler işverenler tarafından elde edilebilir?

İşverenler görevlerini yerine getirmek ve işi ulusal mevzuata uygun olarak organize etmek için kişisel bilgiler alabilirler.

Avrupa Veri Koruma Kurulu adına

Üye

Andrea Jelinek

Bu açıklamanın özgün metni için bkz:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldatatandcovid-19_en.pdf