TİCARET	AB VE JAPONYA' DAN DÜNYANIN EN BÜYÜK GÜVENLİ VERİ AKIŞI		
Yayın Adı	İstanbul Ticaret	**Referans No**	81360588
Newslighter	http://gold.ajanspress.com.tr/linkpress/BpVhcijuYerXBz3-XFjXDQ2/?v=2&s=38801&b=896728&isH=1		
	İlk Sayfa|Liste		

Samuray makûs talihi yenebilir mi?

AB-ABD Gizlilik Kalkanı uygulamasının etkinliğinin sorgulandığı şu zamanlarda Genel Veri Koruma Tüzüğü'nün (GDPR) temel maddelerinden bazılarının Japon Kişisel Veri Koruma Yasası'ndan (APPI) farklılık göstermesi, akıllarda soru işaretleri doğurdu. Komisyon, ekim ayında AB-ABD Gizlilik Kalkanı ilkelerinin etkinliğini gözden geçirmeyi planlıyor. ABD'nin anlaşmanın gerekliliklerine uymadığı kanısına varıldığı takdirde AB, ABD şartları tam anlamıyla yerine getirene kadar ABD ile veri alışverişini askıya almayı planlıyor. Henüz bu sorun çözülmemişken, Japonya ile AB'nin benzer sorunları yaşayıp yaşamayacağı akıllarda soru işareti uyandırıyor. Ancak komisyona göre, üçüncü ülkelere veri aktarımı yapılabilmesi için, iki sistemin eşdeğerliğe sahip olması yeterli. Ayrıca, Japonya'nın AB vatandaşlarından gelecek şikâyetlerin ele alınması için sistem kuracak olması taraflar arasında büyük çaplı bir veri ihlali oluşması olasılığını düşürüyor. İki taraf da gerekli iç prosedürlerini tamamladığı takdirde, karşılıklı ve akıcı bir kişisel veri aktarımının 2018 sonbaharında faaliyete geçmesi bekleniyor.

AB ve Japonya'dan dünyanın en büyük güvenli veri akışı

Avrupa Birliği'nin son dönemdeki ticaret anlaşmalarının en önemlisi, AB-Japonya Ekonomik Anlaşması. Bu kapsamda dünyanın en büyük güvenli veri akış sistemi ve yönetimi çok konuşulacak. Konu, kişisel verilerin güvenliği bakımından büyük önem taşıyor.

Melis Bostanoğlu
İktisadi Kalkınma Vakfı

TÜRKİYE, AB ile 1996 yılından bu yana yürürlükte olan Gümrük Birliği'nin uzun bir süredir güncellenmesini beklerken; AB, her geçen gün yeni ticaret anlaşmalarına imza atarak, dünya ticaretinde öne çıkan ve özellikle ABD'nin başını çektiği korumacı politikalara meydan okumaya devam ediyor. Son dönemde bu ticaret anlaşmalarının en önemlisi, Birliğin tarihindeki en kapsamlı ticaret anlaşması olma niteliğini taşıyan AB-Japonya Ekonomik Anlaşması (EOA). Dünyanın en büyük ikinci ve dördüncü ekonomisi arasındaki bu anlaşma yürürlüğe girdiğinde küresel hasılanın yüzde 28.5'ini kapsayacak ve 600 milyon nüfuslu bir serbest ticaret alanı oluşacak.

TEMEL HAKLAR

Anlaşmanın AB için sadece ticari açıdan değil, temel haklar açısından da bir o kadar önemli olduğu aşikâr. Bu kapsamda verilerin korunması, son yıllarda AB'nin en çok üzerinde durduğu konulardan biri. 25 Mayıs 2018 tarihinde yürürlüğe giren Genel Veri Koruma Tüzüğü (*General Data Protection Regulation* – GDPR) ile AB, kişisel verilerin korunmasında yepyeni bir çağa geçiş yapmıştı. Hizmet sektöründe kişisel veriler sıkça işlendiğinden ve diğer sektörler için de dikkate değer çıktılar yarattığından, verilerin korunması AB için en az anlaşmanın ticari maddeleri kadar önem taşıyor.

3. ÜLKELERE AKTARMA

AB hukuku kapsamında, vatandaşların kişisel verilerinin üçüncü ülkelere aktarılabilmesi için iki yol bulunuyor. Bunlardan ilki, AB üyesi olmayan bir ülkenin "esasen eşdeğer" düzeyde veri koruması sağladığını belirten Komisyon "yeterlilik kararı". Yeterlilik kararının yokluğunda uluslararası transferler, uygun veri koruma önlemleri sağlayan bir dizi alternatif aktarım aracı vasıtasıyla gerçekleştirilebiliyor. AB, bu zamana kadar yalnızca Andorra, Arjantin, Kanada, Faroe Adaları, Guernsey, İsrail, Man Adası, Jersey, Yeni Zelanda, İsviçre, Uruguay ve ABD gibi üçüncü ülkelerin yeterli koruma sağladığını tanıdı. Japonya ile yapılan bu anlaşmayı diğer ülkelerinkinden ayıran en önemli özellik, bahsi geçen ülkelerle olan yeterlilik kararları tek taraflı tanınıyorken, bu sefer AB ilk kez üçüncü bir ülkenin veri koruma sisteminin yeterli düzeyde olduğunu "karşılıklı" tanıyacak olması. Bu anlaşma ile dünyanın en büyük güvenli veri akışının tesis edilmesi bekleniyor.

JAPONYA ÖRNEĞİ

Kişisel bilgilerin doğru işlenmesi için gereken önemin gösterilmesini temel ilkeler aracılığıyla sağlayarak, bireylerin hak ve çıkarlarını korumak amacıyla tasarlanan Japon Kişisel Veri Koruma Yasası (*The Act on the Protection of Personal Information* - APPI), en eski gizlilik yasalarından biri.

Hem GDPR hem de APPI, verilerin yalnızca kendi yasalarına eşdeğer kabul edilen yasal sistemlere veya yeterli ihtiyati tedbirlere sahip üçüncü taraflara aktarılabileceği konusunda mutabık olsa da, bazı noktalarda farklılıklar gösteriyor. Öncelikle, APPI kişisel veriyi, birden fazla kişisel bilginin veri tabanında kümelenmiş hali olarak tanımlarken, GDPR'ın tanımlanmış veya tanımlanabilir kişilere ait herhangi bir bilgiyi kişisel veri olarak kabul ediyor. 2017'de getirilen ek düzenlemelerle birlikte Japonya, kurallarını AB'ye uyumlaştırmaya yönelik bir adım atarak, parmak izi ve yüz tanıma gibi biyometrik verileri ile ehliyet ve pasaport numarası gibi kişilere özgü tahsis edilen harfler veya rakamlardan oluşan Kişisel Tanımlayıcı Kodları da kişisel veri olarak kabul etti.

Japonya'nın kişisel veri yasası yeterli mi?

GDPR kişisel bilginin herhangi bir amaçla işlenmesinde uygulanırken, APPI sadece bilgilerin ticari amaçla işlenmesinde kullanılıyor. Ayrıca GDPR, yasanın gözetilmesinden hem veri kontrolörlerini hem de veri işlemcilerini sorumlu tutarken, APPI sadece ticari operatörü gerçekleşebilecek bir hatadan sorumlu tutuyor.

GDPR, her veri işleme eyleminde veri sahibinin rızasının açıkça alınmasını ve verinin işlenme amacının ve metotlarının detaylandırılmasını gerektirirken, APPI *opt-out* (kişinin verilerinin varsayılan olarak kaydolduğu listeden cayma isteği) rıza yöntemini uygulamakta. APPI'ye göre şirketler, *opt-out* yöntemini kullanmadan önce Kişisel Bilgi Koruma Komitesi'nden onay alarak, aktarım öncesi verileri anonimleştirme zorunluluğuna sahip. Tüm bunların yanı sıra iki yasa da veri ihlalleri durumunda farklı cezalar uyguluyor. GDPR, ceza koşullarını ihlal bildiriminde bulunulmaması, şartların yerine getirilmemesi ve tasarımdan itibaren veri gizliliği (*privacy by design*) konseptinin ihlal edilmesi olarak belirlerken, APPI cezai koşulunu sadece kişisel bilgilerin yasa dışı kazanç amacıyla kullanılması olarak belirtiyor. GDPR, veri ihlali halinde şirketlere 20 milyon avro veya hizmet sağlayıcısının küresel gelirinin yüzde 4'ü oranında bir ceza keserken, APPI kuralları altında en az bir yıl hapis cezası ya da 500 bin yenden başlayan para cezası öngörülüyor.