Analiz · 16 Mayıs 2026

← Önceki·Sonraki →

GDPR ve profesyonel mesajlaşma: çoğu kişi neden bilmeden kuralları ihlal ediyor?

Hemen hemen her ofis, muayenehane veya danışmanlık firması, sunucusu Avrupa Ekonomik Alanı dışında bulunan uygulamalar aracılığıyla müşteri belgeleri gönderiyor. Kötü niyet olmadan, ancak birçok durumda yönetmeliği ihlal ederek ve kimse onları uyarmadan.

Düşündüğünüzden daha uzağa seyahat eden belge

Gündelik bir durum: bir mali müşavir mesajlaşma yoluyla müşteri verilerini içeren bir belge alıyor. Bir satış temsilcisi sohbet üzerinden bir meslektaşına bir teklif iletiyor. Bir doktor aynı yolla bir meslektaşıyla bir klinik rapor paylaşıyor. Kimse üzerinde iki kez düşünmüyor. Normaldir. Uygundur. Avrupa'nın her şehrindeki her ofiste her gün yapılan şeydir.

Ancak bu belge, birçok durumda az önce Amerika Birleşik Devletleri'ndeki bir sunucuya seyahat etti. Geçici de olsa, "bekleme halindeyken şifrelenmiş" de olsa, ne profesyonelin ne de müşterisinin kontrol etmediği bir bulutta depolandı. İçerikle bağlantılı meta verileri teknik olarak dizine ekleyebilen sistemlerden geçti. Ve Avrupa Genel Veri Koruma Yönetmeliği'nin bu konuda söyleyecek oldukça net bir şeyi var.

Normun gerektirdikleri

GDPR –ve dolayısıyla Avrupa Birliği Adalet Divanı'nın içtihatları (özellikle 2020 tarihli Schrems II kararı, C-311/18)– Avrupalı vatandaşların kişisel verilerinin uygun şekilde korunması gerektiğini belirler. Bu veriler Avrupa Ekonomik Alanı dışına çıkarsa, veri sorumlusu alıcının Avrupa'dakine "esasen eşdeğer" bir koruma düzeyi sunduğunu garanti etmelidir. Uygulamada bu, müşteri verilerinin sunucuları ABD yargı yetkisine tabi olan servisler aracılığıyla gönderilmesinin, bir etki değerlendirmesi yapılmadan ve ek güvenceler –standart sözleşme maddeleri, doğrulanabilir şifreleme gibi ek teknik önlemler vb.– uygulanmadan yönetmeliğin ihlali anlamına gelebileceği anlamına gelir. Şimdiye kadar kimse bir şey dememiş olsa bile.

Ve mesele sadece mesajların içeriği değildir. Meta veriler –kim kime neyi gönderiyor, ne zaman, ne sıklıkta, nereden– de düzenlemelere göre ve Avrupa Veri Koruma Kurulu'nun mükerrer yorumuna göre kişisel veridir. Bir kullanıcının profesyonel iletişiminden meta veri toplayan bir servis, bu kullanıcının müşterilerinin kişisel verilerini, onların haberi olmadan veya bu tür bir işlemeye herhangi bir onay vermeden işler.

Yaygın düşünce şeması –"uygulamayı sadece yazmak için kullanıyorum; uygulama müşterimin veri sağlayıcısı değil"– hukuken yanlıştır. Eğer müşterinin verileri üçüncü bir tarafın altyapısından geçiyorsa, o üçüncü taraf bu verileri işliyor demektir. Ve eğer bunları işliyorsa, yasal bir dayanak, bir veri işleme sözleşmesi ve uygun güvenceler olmalıdır.

Kim sorumlu?

Hukuki sorumluluğu kimin taşıdığı sorusu akademik değildir. GDPR, *veri sorumlusu* (hangi verilerin hangi amaçla işleneceğine karar veren) ile *veri işleyen* (bunu maddi olarak sorumlunun adına yapan) arasında ayrım yapar. Müşteri belgelerini gönderen profesyonel veri sorumlusudur. Mesajlaşma uygulaması sağlayıcısı birçok durumda fiili veri işleyendir. Bir veri işleme sözleşmesi olmadan –ve böyle bir sözleşmenin içermesi gereken maddelerin çoğu olmadan– sorumlu yükümlülüğünü yerine getirmemiştir.

İyi niyetli yorum: "çoğu profesyonel bunu bilmiyor" der. Sert yorum: "kanunu bilmemek mazeret sayılmaz" der. Ve bu konuda görüşüne başvurulan herhangi bir uzman veri koruma avukatının yorumu genellikle sert olandır.

Bunun somut olarak kimin için önemli olduğu

Üçüncü şahısların kişisel bilgileriyle ara sıra bile olsa işlem yapan her profesyonel veya şirket için:

- Müşteri belgeleri alan avukatlar (sözleşmeler, davalar, beyanlar, varlık raporları).
- Sağlık verilerini paylaşan doktorlar ve diğer sağlık profesyonelleri –ki bunlar GDPR 9. maddeye göre güçlendirilmiş bir koruma rejimine sahip *özel nitelikli veriler* olarak kabul edilir–.
- Kimlik, vergi ve banka verileriyle işlem yapan mali müşavirler ve idari yöneticiler.
- Çalışanların iş ve kişisel belgelerini yöneten İnsan Kaynakları departmanları.
- Potansiyel ve mevcut müşterilerden iletişim bilgilerini ve genellikle hassas ticari bilgileri alan ticari temsilciler.

Her durumda bilgiler GDPR ile korunmaktadır. Her durumda, alışılagelmiş uygulamada bu bilgiler, yargı yetkisi ek güvenceler olmadan Avrupa çerçevesine "esas itibarıyla eşdeğer" beyan edilmesine izin vermeyen kanallar üzerinden akmaktadır. Kötü niyetten değil. Alışkanlıktan. Ve on beş yıl boyunca kolaylığı uyumluluğun önüne koyan teknolojik bir altyapı nedeniyle.

"Herkes yapıyor" argümanı

En yaygın itirazı öngörmek akıllıca olacaktır: "eğer herkes yapıyorsa, bu gerçek bir sorun olamaz". Bu tamamen anlaşılabilir bir argümandır ve hukuken hiçbir gücü yoktur. Bir uygulamanın yaygın olması, onu yönetmeliğe uygun kılmaz. Veri koruma yetkilileri son yıllarda, denetim anına kadar zararsız görünen mesajlaşma kullanım biçimleri nedeniyle birkaç şirketi tam olarak cezalandırmıştır.

Mevcut operatif gerçeklik, riskin olasılık açısından düşük olması –bir Kurul denetiminin orta ölçekli bir ofisin spesifik mesajlaşma araçlarını denetlemesi çok nadirdir– ancak gerçekleşirse etki açısından yüksek olmasıdır. Çoğu kişinin aldığını bilmeden aldığı bir risktir. Yani, kullanılan aracın veri sorumlusunun yasal sorumluluğuyla uyumlu olup olmadığını değerlendirmeden.

Dijital izler geriye dönüktür

Öngörülmesi gereken, öncekine neredeyse simetrik ikinci bir argüman daha vardır: *"eğer bu ciddi bir sorun olsaydı, idare bunu zaten denetlemeye başlardı"*. Mevcut gözlemlenen gerçeklik ona yüzeysel olarak hak veriyor. Küçük şirketlerde ve özellikle kendi hesabına çalışanlarda hatalı mesajlaşma kullanımı nedeniyle yapılan denetimler bugün neredeyse yok denecek kadar azdır –bu davranışa izin verildiği için değil, Türkiye ve AB'nin büyük bölümündeki idarenin milyonlarca yükümlüyü denetlemek için gereken insan kaynağından yoksun olması nedeniyle.

Bugünün gözlemlenen pratiği bunu düşündürüyor. Ancak gelecek on yılın düşündürdüğü şey bu değil. İki vektör, nispeten kısa süreler içinde dengeyi değiştirmek için birleşiyor.

Birincisi: dijital izler geriye dönüktür. Merkezi bir sunucuya sahip bir uygulama üzerinden gönderilen her mesaj, en azından meta verilerde, kalıcı bir altyapıda kayıtlı kalır. Altı ay önce gönderilen şey bugün teknik olarak hala denetlenebilir durumdadır. Bugün gönderilen şey beş yıl sonra da denetlenebilir olacaktır. Mevcut bir

denetimin olmaması, gelecekte bir denetim olmayacağının garantisi değildir. Bu, değerlendirmenin ertelenmesidir, muafiyet değil.

İkincisi: idari denetim kapasitesi hızlanarak artacaktır. Yapay zeka araçlarının denetim süreçlerine dahil edilmesi, şimdiye kadar –hukuken değil fiilen– küçük şirketleri ve serbest meslek sahiplerini koruyan insani darboğazı ortadan kaldırıyor. Devasa meta veri yığınlarını, vergi beyannamelerini, ticaret sicillerini ve güvenlik ihlali bildirim yükümlülüklerini çapraz kontrol edebilen bir sistemin müfettişlere ihtiyacı yoktur: erişime ihtiyacı vardır. Ve mevcut normatif çerçeve altında AB'de yasal varlığı olan sağlayıcılara yönelik talepler yoluyla erişim tamamen mümkündür.

Buna daha az teknik ama bir o kadar belirleyici bir faktör daha ekleniyor: Avrupa devletleri sürekli artan bir borçlanma sürecindedir ve neredeyse istisnasız olarak vergi tabanlarını genişletmeleri gerekmektedir. GDPR'a uyulmamasından kaynaklanan idari yaptırım, saf mali terimlerle büyüyen ve siyasi olarak elverişli bir gelir kaynağıdır. Bu bir varsayım değil: Avrupa veri koruma yetkililerinin yıllık raporlarında gözlemlenebilir bir eğilimdir ve burada toplam ceza hacmi birkaç mali yıldır üst üste artmaktadır.

Veri sorumlusu için operatif sonuç alarmist değil, ayık bir sonuçtur: **bugün müşteriyle iletişimin nasıl yönetildiğine dair karar, bugünkü değil, denetimin geldiği yılın denetim kapasitesine göre değerlendirilir.** Ve bu kapasite, makul bir süre içinde bugünkünden önemli ölçüde farklı olacaktır. Bugün işleri doğru yapmaya başlayan kişi sadece bugünden itibaren düzgün olmayacak: bu andan itibaren oluşturulan iz norma uygun olacak ve bu, gelecek süreci geriye dönük olarak koruyacaktır. Şimdiye kadar olduğu gibi devam eden kişi, uyumluluğu gelecek yılların standartlarına –ve kaynaklarına– göre değerlendirilecek olan denetlenebilir bir iz biriktirecektir.

Farklı bir mimariyle ne değişir?

Verilerin üçüncü şahıs altyapısında depolanmadığı, bunun yerine doğrudan göndericinin cihazından alıcının cihazına seyahat ettiği teknik alternatifler mevcuttur. Bu mimaride, uluslararası aktarımlar açısından GDPR'a uyum; standart sözleşme maddelerine, sağlayıcının iyi niyetine veya gelecekteki denetimlere bağlı değildir. *Aktarımın olmamasına* bağlıdır. Ve var olmayanı ihlal edemezsiniz.

Bu tek çözüm değildir ve mümkün olan tek çözüm de değildir. Ancak yapısal olarak farklıdır ve normatif uyum bir prosedürel ek olmaktan çıkıp tasarımın doğrudan bir sonucu haline gelir. Sorumluluğunu ciddiye alan bir profesyonel için bu fark bir fark yaratır.

Cuadernos'un bir sonraki sayısı, Schrems II kararını ve ABD bulut servislerine bağımlı küçük ve orta ölçekli şirketler için yayınlanmasından beş yıl sonraki pratik etkilerini ayrıntılı olarak analiz edecektir.

Kaynaklar ve yasal çerçeve

- Yönetmelik (AB) 2016/679 (GDPR), özellikle uluslararası aktarımlara ilişkin Bölüm V.
- ABAD C-311/18 ("Schrems II"), 16 Temmuz 2020.
- EDPB – Aktarım araçlarını tamamlayan önlemlere ilişkin 01/2020 sayılı Tavsiyeler.
- Veri Koruma Yetkilileri – Profesyonel ortamlarda anlık mesajlaşmanın uygunsuz kullanımı nedeniyle verilen ceza örneklerini içeren yıllık raporlar.

← ÖncekiDijital çağda mesleki sır saklama yükümlülüğüSonraki →Arada kimse olmadığında

Son okumalar

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Bu makaleyi ihtiyacınız olan her yere yanınızda götürün.

↓ Markdown ↓ Düz metin ↓ PDF

Dosya cihazınıza indirilecektir. Oradan kaydedebilir, Solo2'ye aktarabilir veya istediğiniz yerde paylaşabilirsiniz. Cuadernos hedef noktaya sizin yerinize karar vermez.

Mühür mumu · SHA-256 0cc911ae7eeb78f4278383095448e76967951869e213d64dba30090e6235a72f

Cuadernos Lacre · Menzuri Gestión S.L. yayını ·
R.Eugenio tarafından yazıldı · Solo2 ekibi tarafından düzenlendi.