Düşünce · 16 Mayıs 2026

← Önceki·Sonraki →

Dijital çağda mesleki sır saklama yükümlülüğü

Profesyonel ile müşterisi arasındaki iletişim teknik olarak yetersiz bir kanal üzerinden yapıldığında, sır sızıntı gününde bozulmaz. Çok daha önce, araç seçildiği anda bozulmuştur.

Neredeyse kimsenin görmediği bir sorun

Bir avukat, müşterisinden gelen gizli bir belgeyi telefonuna alır. Bir doktor, bir meslektaşıyla hassas bir teşhisi tartışır. Bir psikolog, bir psikiyatristle bir hastanın tedavisini koordine eder. Bir mali müşavir, incelenmeyi bekleyen bir beyannamenin verilerini gönderir. Hepsi bunu anlık mesajlaşma yoluyla yapar. Ve neredeyse hiç kimse bu mesajların gerçekte nerede bittiğini düşünmek için durmaz.

Cevap çoğu durumda aynıdır: profesyonelin kontrol etmediği bir sunucuda, mevzuatını mutlaka bilmediği bir ülkede, iş modeli –doğrudan ekonomik terimlerle– veri biriktirmek olan bir şirket tarafından yönetiliyor. Mesaj iletim sırasında şifrelenmiş olabilir. Ancak sunucuya ulaştığı anda, üçüncü bir tarafın altyapısında saklanan ve o üçüncü tarafın operatif, yasal ve ticari kararlarına tabi olan bir kopyadır. Profesyonelin kararlarına değil.

Mevzuat ne diyor?

Avrupa Genel Veri Koruma Yönetmeliği 32. maddesinde açıktır: kişisel verileri işleyen herkes, riske uygun bir güvenlik düzeyi garanti etmek için "uygun" teknik ve organizasyonel önlemleri uygulamalıdır. Önlemlerin uygunluğu "uygulamanın ne yaptığını iddia ettiğine" göre değil, gerçek riske göre ölçülür. Müşteri verileri, yargı yetkisi Avrupa Ekonomik Alanı'na eşdeğer bir koruma düzeyi garanti etmeyen bir sunucuda biterse, veri sorumlusu –yani profesyonel– muhtemelen tam olarak farkında olmadığı bir risk üstlenir.

Ve bu sadece GDPR değildir. Avukatlar, doktorlar, psikologlar, denetçiler, gazeteciler ve diğerleri için özel olarak düzenlenen mesleki sır saklama yükümlülüğü, müşteriyle iletişimin gizli olmasını gerektirir. "Mümkün olduğunca gizli" değil. Kayıtsız şartsız gizli. Kullanılan teknik kanal bunu garanti edemiyorsa, profesyonel, mesleğinin deontolojisinin izin vermediği bir risk üstleniyor demektir.

Paradoks, riskin görünmez olmasıdır. Ofis mesajlaşmasını kimse denetlemez. Sohbet sağlayıcısından veri işleme sözleşmesini kimse istemez. Risk ancak iş işten geçtikten sonra ortaya çıkar: bir sızıntı, yayınlanmış bir güvenlik açığı, kullanıcıya bildirilmeden başka bir kıtada icra edilen bir mahkeme kararı.

Bir profesyonelin teknik olarak neye ihtiyacı var?

Sır saklama yükümlülüğü olan bir kişinin ihtiyacı olan şey, gereksinimler açısından bakıldığında aslında şaşırtıcı derecede basittir:

- Mesajların, kopya saklayan bir ara sunucudan geçmeden doğrudan göndericinin cihazından alıcının cihazına gittiği bir kanal.
- Yargı yetkisi ve politikaları beyanla değil, tasarımla GDPR ile uyumlu olan bir altyapı.

- Profesyonel kişileri (müşteri isimleri, telefon numaraları, rehber) üçüncü bir tarafa teslim etmek zorunda kalmadan muhatapla kimlik doğrulama yolu.
- Mesajın doğru kişiye ulaştığını teyit etmek için sağlayıcının sözüne dayanmayan, doğrulanabilir bir sistem.

Bu zorlu bir liste değil. Aslında dijital öncesi profesyonel iletişimde doğal kabul edilen şeydir. İadeli taahhütlü bir mektup tüm bu kriterleri karşılıyordu. Ofis santralinden müşterininkine yapılan bir telefon görüşmesi de öyle. Garip olan bu garantilerin bugün istenmesi değil: garip olan, dijital kanala geçişte kimse fark etmeden bunların kaybedilmiş olmasıdır.

Şifrelemek ile depolamamak arasındaki fark

Yararlı bir metafor var. Bir mesajı şifreleyip bir sunucuda depolamak, bir belgeyi kasaya koyup kasayı bir yabancının evinde bırakmaya eşdeğerdir. Kasa iyidir. Belge prensip olarak okunamaz. Ancak belge *hala başkasının evindedir*. Ve o birisi bir mahkeme kararı alabilir, bir siber saldırıya uğrayabilir, hizmet şartlarını değiştirebilir, başka bir etik anlayışına sahip başka bir şirket tarafından satın alınabilir veya yarın yok olabilir.

Yapısal alternatif –prosedürel değil, güvene dayalı değil– belgenin ofisten hiç çıkmamasıdır. Herhangi bir aracı olmadan doğrudan profesyonelin masasından müşterinin masasına seyahat etmesidir. Cihazlar arasındaki noktadan noktaya iletişimin teknik olarak yaptığı şey budur: aracıyı ortadan kaldırır. Aracının kötü olması meselesi değildir. Sadece mesleki sır durumunda aracının *gereksiz* olmasıdır. Ve güvenli olmak isteyen her sistemde gereksiz olan, ilke olarak ortadan kaldırılmalıdır.

Sorumluluk meselesi

Nihayetinde, sır saklama yükümlülüğü olan her profesyonelin kesin bir evet ile cevaplayabilmesi gereken soru şudur:

> Eğer yarın müşterilerimden biriyle olan bir görüşme sızarsa ve bir mahkeme veya meslek odası bana gizliliği nasıl yönettiğimi sorarsa, kullandığım kanalın üçüncü taraf altyapısında kopya saklamadığını teknik olarak kanıtlayabilir miyim? Verilerin konuşmaya dahil olan iki kişinin cihazlarından hiç çıkmadığını kanıtlayabilir miyim? Başka bir kıtadan bir şirketin sözüne güvenmeden, gizliliğin bir vaatle değil mimariyle garanti edildiğini kanıtlayabilir miyim?

Eğer cevap hayırsa, sorun somut olarak araç değildir. Sorun, bir araca, aracın desteklemek üzere tasarlanmadığı bir sorumluluğun devredilmiş olmasıdır. Gizli dosyaları şeffaf bir zarfa koyup postacının içine bakmayacağına güvenmek gibidir.

Bir profesyonelin müşterileriyle iletişim kurmak için seçtiği araç, onların güvenine ne kadar değer verdiği hakkında çok şey söyler. Bu güvenin vaatlere değil mimariye bağlı olması için tasarlanmış araçlar vardır. Ve öyle olmayan araçlar vardır. Aradaki farkı bilmek işin bir parçasıdır.

Alıntılanan yasal çerçeve

- Yönetmelik (AB) 2016/679 (GDPR), özellikle madde 5, 25 (tasarımdan itibaren veri koruma) ve 32 (işleme güvenliği).
- Türkiye'de 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve mesleki sır saklama yükümlülüğüne ilişkin mevzuat (Avukatlık Kanunu m. 36, Tıbbi Deontoloji Nizamnamesi m. 4).
- Türk Ceza Kanunu (TCK) m. 239 (Ticari sır, bankacılık sırrı veya müşteri sırrı niteliği taşıyacak bilgi veya belgelerin açıklanması).
- Avukatlık Meslek Kuralları (gizlilik ve mesleki sır).

← ÖncekiŞifrelemek gizli olmak demek değildir: meta veriler hakkınızda ne söyler?Sonraki →GDPR ve profesyonel mesajlaşma: çoğu kişi neden bilmeden kuralları ihlal ediyor?

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 ae9a9f1c1c04a75dc5cde1cf602c5884b5e003a0fb627a73ba43b9d38796b757

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