

Kamu idarelerinde ve kurumsal şirketlerde sosyal medya yönetimi, sadece fotoğraf paylaşmak veya duyuru yapmaktan ibaret basit bir iş değildir; kurumun dijital cephesidir. Resmi hesaplardan yapılan amatörce bir paylaşım, telif hakkı ihlali veya yönetilemeyen bir kriz, yıllarca inşa edilen kurumsal itibarı saniyeler içinde yerle bir edebilir. Bu tür iletişim kazaları sadece prestij kaybı yaratmakla kalmaz, idareyi ağır KVKK cezalarıyla ve yöneticileri hukuki soruşturmalarla baş başa bırakır.

Kurumunuzun dijital iletişim süreçleri aşağıdaki idari ve hukuki standartlara ne ölçüde uyum sağlıyor?

1. KVKK İHLALLERİ VE TELİF HAKKI (COPYRIGHT) TUZAKLARI

- Kontrol Sorusu:** Kurumunuzun sosyal medya hesaplarında paylaştığınız etkinlik fotoğraflarında yer alan vatandaşlardan, çocuklardan veya personelden "Açık Rıza Beyanı" alıyor musunuz? Kullandığınız müzik ve görsellerin telif haklarını yasal olarak kontrol ediyor musunuz?
- Gizli Risk:** Sosyal medya paylaşımlarında yapılan en yaygın ve en tehlikeli hata KVKK ihlalleridir. Bir çocuğun veya vatandaşın fotoğrafının izinsiz paylaşılması, Kişisel Verileri Koruma Kurulu tarafından kuruma milyonlarca liralık idari para cezası kesilmesine neden olur. Aynı şekilde, lisanssız kullanılan bir müzik veya görsel yüzünden açılacak telif davaları, kurum bütçesini sarsar. Bu cezalar, paylaşımı yapan personele ve Basın Yayın Müdürlüğüne rücu edilebilir. Kurumunuzun dijital paylaşımlarını bu yasal risklerden nasıl arındıracaksınız?

2. KRİZ ANLARINDA DEZENFORMASYON VE LİNÇ YÖNETİMİ

- Kontrol Sorusu:** Kurumunuz hakkında sosyal medyada viral olan yalan bir haber (dezenformasyon) veya organize bir linç kampanyası başladığında; ilk 60 dakika içinde devreye girecek, kimin ne açıklama yapacağını belirleyen yazılı bir "Kriz İletişimi Protokolünüz" var mı?
- Gizli Risk:** Kriz anlarında idarenin sessiz kalması veya panikle yanlış bir açıklama yapması, krizi derinleştirir ve haklıyken haksız duruma düşmenize yol açar. Sosyal medyadaki linç kültürü, kurumun hizmetlerini gölgeler ve üst yönetimin istifasına kadar gidebilecek geri dönüşüme bir güven kaybı yaratır. Dezenformasyon saldırılarına karşı proaktif bir savunma hattını ve doğru "Tone of Voice" (ses tonunu) nasıl kurgulamalısınız?

3. KURUMSAL HESAP GÜVENLİĞİ VE YETKİ DEVRİ ZAFİYETLERİ

- Kontrol Sorusu:** Kurumunuzun resmi sosyal medya hesaplarının şifreleri kimlerde bulunuyor? Hesabı yöneten personel işten ayrıldığında veya kurumla husumet yaşadığında, hesapların güvenliğini anında sağlayacak bir "Yetki Devri ve Güvenlik Prosedürünüz" mevcut mu?
- Gizli Risk:** Resmi hesapların şifrelerinin tek bir personelin inisiyatifinde olması, kurumsal güvenliğin en zayıf halkasıdır. İşten öfkeyle ayrılan bir personelin resmi hesaptan yapacağı uygunsuz bir paylaşım veya hesabın siber saldırganlarca (hacker) ele geçirilmesi, kurumsal bir sabotaja dönüşür. Bu tür güvenlik zafiyetleri, idarenin dijital varlıklarını koruyamadığı gerekçesiyle yöneticiler hakkında idari soruşturma açılmasına neden olur.

DİJİTAL İTİBARI VE KURUMSAL GÜVENLİĞİ ULUSLARARASI STANDARTLARA TAŞIMAK

Eğer yukarıdaki kritik sorulara tereddütsüz ve mevzuata uygun net cevaplar veremiyorsanız, kurumunuzun dijital itibarı ve şahsi kariyeriniz devasa bir risk altındadır. Bu krizleri sosyal medyada linç edilirken veya KVKK cezalarıyla yüzleşirken değil, uzmanlardan proaktif olarak öğrenmek zorundasınız. Yasal risklerinizi sıfırlamak ve kurumunuza özel eğitim planlaması yapmak için Vizyonder Kurumsal Sosyal Medya Yönetimi ve Kriz İletişimi Eğitimi programına hemen başvurun.

VIZYONDER EĞİTİM DANIŞMANLIK VE TEKNOLOJİ A.Ş.

İSTANBUL	:	Meşrutiyet Mahallesi, Kodaman Sokak, Bahar Apartmanı No:6 Daire:7 Nişantaşı - Şişli / İSTANBUL
ANTALYA	:	Etiler Mah. Evliya Çelebi Cad. No:23 /106 Muratpaşa / Antalya
MERSİS NO	:	0925131571200001
İLETİŞİM	:	0.212 232 2016
GSM	:	0.545 335 2016
Eposta	:	bilgi@vizyonder.org.tr
TİCARET SİCİL NO	:	142629
KURUMLAR V.D.:	:	9251315712
Faks:	:	0.850 811 2016
	:	0.545 332 2016