KİŞİSEL VERİLERİN KORUNMASI KANUNU DERNEKLER

Kanunun Amacı ve Kapsamı

Bu Kanunun amacı; kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.

Kanunun 2. maddesinde kapsamı belirtilmiştir; Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacaktır.

GAP Analizimizin Amacı ve Kapsamı

- Dernek iş süreçlerinin veya onun parçalarının tetkik kriterlerine uygunluğunu belirlemek ve onun;
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu gerekliliklerine uygunluğunun kontrolü,
- Kişisel Verilerin Korunmasına ilişkin Yönetmelik, Tebliğ ve Kurul kararlarına uygunluğun kontrolü,
- İş/Görev tanımları ve Dernek süreç tanımlarına uygunluğun kontrolü,
- KVKK Kapsamında teknik ve idari tedbirlerin uygunluğu, yeterliliği ve etkinliğinin kontrolü,
- Potansiyel iyileştirmeler için ilgili alanları tanımlayabilecek kabiliyette olduğunu tespit etmek.

TEMEL KAVRAMLAR

- Açık Rıza;
    a. Belirli Bir Konuya İlişkin Olması
    b. Rızanın Bilgilendirmeye Dayanması
    c. Özgür İradeyle Açıklanması
- Anonim Hale Getirme (Anonimleştirme)
- İlgili Kişi
- Kişisel Veri
- Kişisel Verilerin İşlenmesi
    a. Otomatik İşleme
    b. Otomatik Olmayan İşleme
- Veri Sorumlusu ve Veri İşleyen
- Mahremiyet Risk Etkisi

Kişisel Veri Kavramı

Kişisel Veriler

- Adı Soyadı
- Doğum Yeri
- Doğum Tarihi
- Taşıt Plakası
- TC Kimlik No
- Pasaport Numarası
- E-Mail Adresi / IP Adresi
- Özgeçmiş
- Kişiyi belirlenebilir kılan benzer tüm veriler

Özel Nitelikli Kişisel Veriler

- Din/Mezhep
- Siyasi Düşünce
- Felsefi İnanç
- Dernek/Vakıf/Sendika Üyeliği
- Irk / Etnik Köken
- Sağlık
- Ceza Mahkumiyeti ve Güvenlik Tedbirleri Verileri
- Kılık kıyafeti
- Cinsel Hayatı
- Biyometrik ve Genetik Veriler

Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler

KVKK Ortak Sorunlar

- KVKK süreçleri için bir ekip yazılı olarak belirlenmemiştir. İçeride bilgilendirme yapıldığına dair kanıt bulunamamaktadır. Tüm departmanları ve süreçleri kapsayacak bir komitenin görev ve sorumluluklarıyla beraber atama **yazısının resmi olarak paylaşılması önerilir.**
- Gönüllü dahil işe giriş sürecinde standart işe giriş başvuru belgeleri isteniyor. Bu süreçte kişi ile sözleşme imzalanıyor internet üzerinden de başvuru alınıyor. Kvkk metni olmadığı paylaşıldı.
- Gönüllü dahil çalışan özlük ve sağlık verileri ayrı ortamda tutulmakta. Dernekte henüz bir imha işlemi yapılmamıştır.
- Bilgi ve veri güvenliği ile ilgili farkındalık ve/veya bilinçlendirme eğitimler verilmelidir. **Farkındalık eğitim içeriğine KVKK gereksinimlerinin de dahil edilmesi önerilir.**
- Dernek ve Web sayfası üzerinden başvurular alınabilir. Telefon ve e-posta ile iletişime geçiliyor. İşe alımlarda gönüllü kişiler ile çalışabiliniyor. Bu gönüllü kişiler ile **gizlilik sözleşmesi imzalandığına dair objektif delile ulaşılamamıştır.**
- Disiplin talimatının olmadığı ve KVKK nezdinde gözden geçirilip **elde edilmesi** önerilmektedir.

KVKK Ortak Sorunlar

- Mailler Hotmail, Gmail ve Webmail üzerinde tutulduğu gözlemlenmiştir.
- Email yazışmalarında KVKK imza aydınlatma metni olmadığı bildirilmiştir.
- Meta şirketinin sosyal medya araçlarından Facebook dernek grubu kurulmuş ve KVK aydınlatma metninin güncel olmadığına karar verilmiştir.
- Meta şirketinin sosyal medya araçlarından Instagram üzerinden genel ya da gelen kişisel veri içeren mesajlara nasıl aydınlatma yapılması gerektiği ile ilgili **objektif delile ulaşılamamıştır. (iab.europe transparency and consent framework)**
- Proje yapıldığında proje bilgileri ve içerik açısından gizlilik sözleşmesi incelenmesi talep edilmiştir.
- Çalışılan ajanslar ve gönüllü web yazılım/tasarım mevcut. Bunlarla ilgili hizmet veri gizliliği sözleşmesi **imzalandığına dair objektif delile ulaşılamamıştır.**
- Web sitesi tamamlanmadığından kamuoyuna duyurularında ve üye formunda revizeler gerekecektir.

KVKK Ortak Sorunlar

- Derbis hasta yakınları bilgileri girilmektedir. Hasta yakın bilgileri başka yerde tutuluyor mu?
- Formlarda zorunlu olan veri girişlerinin gözden geçirilmesi gerekmektedir.
- Saklama süreleri belirlenmemiştir.
- Dernekler KVKK Politikası oluşturmalıdır.
- Web sitesi, sosyal medyada fotoğraf ve videolarda yer alan kişilerden açık rıza alınması gerektiğiyle ilgili çalışmalar yapılacaktır.
- Sosyal medyalara uygun şekilde Aydınlatma metinleri hazırlanması ve KVKK politikamız diye atıfta bulunmasına karar alınmıştır.
- Ajans, gazeteciler, tedarikçiler, IT hizmeti alınan firmalarla gizlilik sözleşmesi yapılması önerilir.
- Mali müşavir gibi veri transferi yapılan kişi ya da kurumlarla veri transfer sözleşmesi imzalanması önerilir.
- GDPR uyumlu Kvkk çalışmaları yürütülmesi gerekmektedir.
- Maillerde Kvkk imza aydınlatma metni olmadığı ve gereksinimin karşılanacağına karar verilmiştir.
- Log kayıtlarıyla ilgili firmadan bilgi alınacak ve gereklilikler sağlanması önerilir.
- Veri envanterlerinin tamamen boş olduğu, doldurulmadığı (dernek gerekçeleri) paylaşılmıştır.
- Kişisel veri mahremiyet etki risk analizi yapılmadığı tespit edilmiştir.
- KVKK politikası olmadığı ve gizlilik politikasında revizeler gerektiğine karar verilmiştir.
- Verbis bildirimi zorunlu olmadığından yapılmamış olup envanter, risk yönetimi tamamlandıktan sonra hazırlanacak olan dokümantasyon bilgilerde göz önünde bulundurularak ön hazırlıkla ilerlenmesi ve gereğinin yapılmasına karar verilmiştir.

KVKK Ortak Bulgular

- (Gönüllü dahil) İşe alım süreçlerinde **gizlilik sözleşmesi imzalanmalıdır.**
- Çalışan sözleşmelerinde KVKK gereksinimleri doğrultusunda **kısmi eksiklikler** tespit edilmiştir.
- Çalışan adaylarına ait bilgilerin **süresiz saklanması** risk oluşturmaktadır. Çalışan adaylarına ait veriler belirlenecek bir süre boyunca yeniden değerlendirme amacıyla saklanabilir ve sonrasında **imha edilmelidir**.
- Farkındalık eğitimi içeriklerine KVKK Konuları da **dahil edilmelidir**.
- Mailleri 4.1.2 Saklamayı Gerektiren İşleme Amaçları kapsamında süre belirlenmesine karar verilmiştir.
- Meta uygulamaları hakkında facebook grup **aydınlatma metni dahil edilmelidir.**
- Bağış makbuzları için **aydınlatma metni dahil edilmelidir.**
- Gizlilik politikası en az yılda bir iş birliği dahilinde **incelenmelidir.**
- Ajanslarla ve IT hizmetleriyle ilgili **Veri Gizlilik sözleşmesi imzalanmalıdır.**
- Yönetim Kurulu dahil bütün tam zamanlı/yarı zamanlı/stajyer/gönüllü çalışanlar **gizlilik sözleşmesi imzalamalıdır.**
- GDPR Envanter Mahremiyet Olasılık Etki Risk Analiz yapılması **önerilir.**
- KVKK Envanter oluşturulması **önerilir.**
- Dernek defteri resmi yazışma defteri olduğundan kanuni sebeplerle saklanma süresi 1 yıl olarak belirtilmiştir. 1 yıldan sonra arşivde saklanması **yasal olarak gerekliliktir.**
- Web sitesinde üye formu KVKK bildirimi kısmına ilgili metni yazmanız gerekmekte ve içerisinde bilgi paylaşımı varsa bu konuda **aydınlatma yapmanız gerekmektedir.**
- KVKK Politikası yılda 1 gözden geçirilmesi gerekmektedir.
- Web hosting zaman damgalı log kaydı alınıp alınmadığını kontrol ettirmeniz gerekmektedir.

KVKK Ortak Öneriler

- Veri envanterinin tamamlanması önerilir.
- Risk Yönetimi için analiz çalışması tamamlanması önerilir.
- Bu çalışmalar tamamlandıktan sonra ilgili sözleşmeler, aydınlatma metinleri, açık rıza metinleri, imza metni vb. dokümantasyon çalışmaları yapılması önerilir.
- KVKK Politikasının hazırlanması önerilir.
- Web sitesinde yayınlanacak olan aydınlatma metinleri ve politikanın tamamlanması önerilir.
- Log kayıtları ile ilgili kanuni çalışmaların tamamlanması önerilir.
- Çalışan/Gönüllü/Stajyer ile ilgili ayrı gizlilik sözleşmeleri ve aydınlatma metinleri çalışmalarının tamamlanması önerilir.
- Tedarikçi, Ajans, IT Hizmeti gizlilik sözleşmeleri yapılması önerilir.
- Mali Müşavir veri transfer gizlilik sözleşmesi yapılması önerilir.
- Sosyal medyalara ilgili aydınlatmaların şeffaf ve açık bir şekilde yapılması önerilir.
- KVKK Politikasında, kep adresi, mail adresi, telefon ve adres bilgisi alması gerektiği kararına varılmış olup tamamlanması ve web sitede yayınlanması önerilir.
- Hasta yakınları ile ilgili veri envanteri tamamlandıktan sonra ilgili doküman hazırlandığında bakım sözleşmesi revize edilmesi önerilir.
- Saklama ve imha prosedürü önerilir.
- Saklama ve imha tutanağı önerilir.
- GDPR uyumlu KVKK çalışmalarında danışmanlık alınması önerilir.

KVKK Ortak Öneriler

- KVKK politikası ile ilgili revizelerin yapılması gerekmekte ve yayınlanması uygun görülmüştür.
- KVKK süreçleri için bir ekip yazılı belirlenmesi önerilmiştir. Bütün departmanları temsil eden bir komitenin oluşturulup görev ve sorumluluklarıyla birlikte **atama yazısının resmi olarak paylaşılması önerilir.**
- Kişisel verilerin işlendiği tüm iş süreçlerinin kapsandığı Kişisel Veri Envanterlerinin mevzuat gerekliliklerini karşılayacak şekilde **hazırlanması ve güncelliğinin sağlanması** gereklidir.
- Hizmet tedarikçileri ile **eksik gizlilik sözleşmelerinin** tamamlanması gerekmektedir.
- Dernek iş süreçlerinin yurt dışı üzerinden federasyon, ilaç firmaları ve mail alt yapısı ile yürütülmesi nedeniyle birçok noktada yurt dışı veri aktarımı söz konusu. Kurul onayı alınması için gerekli süreçler tespit edilecek ve detaylı bir veri envanteri çalışması yapılarak ve aktarımda izin alınması gereken hususlar belirlenecektir.
- Bilgi güvenliği farkındalık eğitimlerinin en az yılda bir kez olacak şekilde planlanıyor ve sağlanıyor olması gerekmektedir. Bu periyodik olarak gerçekleştirilecek olan **bilgi güvenliği farkındalığı** eğitim içeriğine KVKK konularının da dahil edilmesi gerekir.
- Metinlerde aydınlatma ve açık rıza metinlerinin olmadığı, aydınlatma ve açık rıza metinlerinde ilgili güncel kurul kararlarından doğan güncellemelerin (26.06.2020 tarihli Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu) revizeleri gerektiği söylenebilir. Yasal metinlerin (Sözleşmeler, Aydınlatma, Açık Rıza vb.) değişen mevzuat şartlarına uygun halde hazırlanması üzere **gözden geçirilip revize edilmesi** gerekmektedir.
- 6698 Sayılı kişisel verilerin korunması kanunu kapsamında belirsiz süreli veri saklama kabul edilebilir bir durum değildir. Kişisel veri envanteri çalışmalarıyla birlikte detaylı **veri saklama süreleri belirlenecek** ve sürelerini tamamlamış saklanan verilerin imhası için gerekli aksiyonlar planlanacaktır.
- İş süreçlerinde işlenen kişisel verilere yönelik riskler değerlendirilmeli ve gerekli aksiyonlar belirlenmelidir. **Risk değerlendirme** faaliyetleri kişisel veri envanteri çalışmalarıyla beraber gerçekleştirilecektir.
- WhatsApp üzerinden yapılabilen derneğe yönelik paylaşımlar risk oluşturmaktadır. Veriyi paylaşan taraf ilgili aktarım karşı tarafın sorumluluğunda olup ancak güvenlik ihlalinden dolayı gerçekleşebilecek bir ihlal durumunda dernek tarafında da **risk oluşturmaktadır**. Mümkünse daha kurumsal bir iletişim kanalı tercih edilmesinde fayda vardır.
- İnternet erişim loglarının 5651 sayılı kanun gereksinimleri doğrultusunda **saklandığı tespit edilememiştir.**
- Veri **silme, anonimleştirme politikalarının** hukuk departmanı ve mevzuatlar ile planlanarak uygulamaya konulması gerekmektedir.
- KVKK uyumunun gözden geçirilmesini sağlamak üzere periyodik olarak iç denetim faaliyetlerinin uygulanması önerilir. 2023 yılı için bir iç denetim planlanmalıdır, sonraki yıllar için de periyodik olarak planlanması önerilir.

Suçlar (KVKK m.17):

TCK m.135: Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.

TCK m.136: Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

TCK m.137: Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, verilecek ceza yarı oranında artırılır.

TCK m.138: Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

Kabahatler (KVKK m.18)

- Aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk Lirasından 100.000 Türk Lirasına kadar idari para cezası
- Veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk Lirasından 1.000.000 Türk Lirasına kadar idari para cezası (KVKK m.12 ye aykırılık)
- Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk Lirasından 1.000.000 Türk Lirasına kadar idari para cezası
- Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk Lirasından 1.000.000 Türk Lirasına kadar idari para cezası

Örnek İhlal Bildirimi

Anasayfa | Kurumsal | Mevzuat | Veri Sorumlusu | İlgili Kişi | Yayınlarımız | İletişim

Yayınlanma Tarihi: 04 Mayıs 2018

Kamuoyu Duyurusu (İhlal Bildirimi)

Kamuoyu Duyurusu (İhlal Bildirimi)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

Araç çağırma hizmeti sunmak üzere Türkiye'deki faaliyetlerini Careem Networks Teknoloji A.Ş. aracılığıyla yürüten Dubai merkezli Careem Inc. (Şirket) unvanlı şirketten alınan 18.04.2018 tarihli yazıda;

- Müşteri ve sürücü bilgilerinin tutulduğu bilgisayar sistemlerine 14.01.2018 tarihinde yetkisiz üçüncü kişilerce erişim sağlandığı, (yapılan inceleme sonucunda konuya ilişkin tespitlerin 21.03.2018 tarihinde ortaya çıktığı,)
- Şirket tarafından adli bilişim incelemesi başlatıldığı ve önde gelen bir siber güvenlik şirketinin konu ile ilgili görevlendirildiği,
- Söz konusu yetkisiz erişimden Türkiye'de mukim 103.337 müşteri ile 900 araç sürücüsünün etkilendiği,
- Yetkisiz erişim sağlanmış olan kişisel veriler arasında müşterilerin isim, telefon numarası, kredi kartı bilgisi, e-posta adresi, kayıtlı konum bilgisi ve yolculuk özeti bilgisi ile araç sürücülerine ait isim telefon numarası, araç modeli, plaka numarası, yolculuk özeti, uluslararası banka hesap numarası, T.C. kimlik numarası ve ehliyet numarası bilgilerinin olabileceği

bilgisine yer verilmiştir.

Yapılan değerlendirmeler neticesinde, Kişisel Verileri Koruma Kurulunun 02.05.2018 tarih ve 2018/45 sayılı Kararı ile Careem Inc. nezdinde gerçekleşen söz konusu yetkisiz erişimin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Öte yandan, konuya ilişkin sorular için https://blog.careem.com/security internet sitesinin ziyaret edilmesi veya infosupport@careem.com e-posta adresi üzerinden destek alınması mümkün bulunmaktadır.

Kamuoyuna saygıyla duyurulur.

TEŞEKKÜR EDERİZ