PERSONEL SERTİFİKASYON MEKANİZMASINA İLİŞKİN USUL VE ESASLAR HAKKINDA TEBLİĞ HAKKINDA DEĞERLENDİRMELER

Kişisel Verileri Koruma Kurumu (**"Kurum"**) tarafından sertifikasyon mekanizması getirilerek, Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ (**"Tebliğ"**) 06.12.2021 tarihli Resmî Gazete'de yayımlandı.

Tebliğ'e göre Kişisel Verileri Koruma Kurulu (**"Kurul"**) tarafından düzenlenen eğitim programını tamamlayanlara verilecek olan katılım belgesi sonrasında, 4 yıl içerisinde sertifika sınavına başvurup sınav sonucunda başarılı olan adaylar **"veri koruma görevlisi"** unvanını almaya hak kazanacaklardır.

Veri koruma görevlisi, Avrupa Birliği Genel Veri Koruma Tüzüğü (**"GDPR"**) kapsamında Data Protection Officer (**"DPO"**) olarak adlandırılan unvana benzetilmeye çalışılmakla birlikte veri sorumlusu bünyesindeki verileri korumak için çalışan kimseler anlamına gelmektedir. Bu noktada GDPR'ın DPO'su ile Kurum'un veri koruma görevlisi arasında benzerlikten çok farklılık bulunmaktadır.

Sertifikasyon programlarına dahil olup düzenlenecek sınavlarda başarılı olan herkes, veri koruma görevlisi unvanını kazanmış olacaktır. Aslında bazı özel şirketlerin verdikleri sertifikaların, Resmî Gazete'nin bu sayısı ile regüle edilmiş olduğunu söyleyebiliriz.

Veri koruma görevlisi olmak için harekete geçecek ilk kurum, Türk Akreditasyon Kurumu (**"TÜRKAK"**), eğitimlerin verilip sınavların gerçekleştirilmesine aracılık edecek eğitim kurumlarının belirlenmesini sağlayacaktır. Böylelikle bazı eğitim merkezleri, veri koruma görevlisi yetiştirme konusunda yetkili hale geleceklerdir. Sertifika sınavında başarılı olanları belgelendirmeye TÜRKAK tarafından **(TS) EN ISO/IEC 17024 standardına uygun** olarak akredite edilen personel belgelendirme kuruluşları yetkili olacaktır.

Kurum'un bu hamlesi ile **Türkiye'de ISO standartlarına sahip veri koruma görevlilerinin oluşturulması** amaçlanmaktadır.

Sertifikaların geçerlilik süresi **sınav sonuçlarının ilanını takiben 4 yıl** olacak ve veri koruma görevlileri, unvanlarını yalnızca **sertifikalarının geçerlilik süresi boyunca** kullanabilecektir. Getirilen 4 yıl şartı Kurum'un veri sorumlularına *tek seferde gerçekleştirilen kişisel verileri korumaya ilişkin bir projenin yeterli olmadığını ve güncelliğin uyumlulukta hayati önem arz ettiğini* zımni olarak dile getirmesi olarak görülebilecektir.

Veri koruma görevlisinin sertifikalandırıldığı program kapsamında kişisel verilerin korunması mevzuatı açısından **yeterli bilgiye sahip olduğu** kabul edilecektir. Bunun yanında *sertifikasyon faaliyetleri esnasında herhangi bir eksiklik ve aksaklık yaşanmaması adına* **personel belgelendirme kuruluşunun da** gerekli ve yeterli personele, kaynağa, fiziki, teknik ve idari altyapıya sahip olmasının gerekmekte olduğu şartı getirilmiştir.

Veri sorumlusunun ve/veya veri işleyenin bünyesinde veri koruma görevlisi istihdam etmesi, veri sorumlusunun ve veri işleyenin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na (**"Kanun"**) ve ilgili mevzuata uyma sorumluluğunu ortadan kaldırmayacaktır.

Sertifika Takip ve Doğrulama Bilgi Sistemi (**"SERTABİS"**) Kurum tarafından yönetilecek olan, sertifikasyonun şeffaf ve etkin sürdürülmesini sağlamak amacıyla kamuya açık oluşturulmuş bir sistemdir. SERTABİS'te *katılım belgesinde yer alan bilgiler, personel belgelendirme kuruluşunun bilgileri ve statülerinde gerçekleşen değişiklikler ile sertifika sahibi kişilerin bilgileri, program kapsamında yapılan sınavların tarihlerinin yanı sıra sınavda başarılı olan kişilerin; sertifika tarihleri, sertifika numaraları, sertifika geçerlilik süreleri ve sertifika statülerine dair bilgiler yer alır.*

Tebliğ'in Kurum'a bilgi ve belge gönderme başlıklı 16. Maddesi uyarınca Kurum, ilgili taraflardan **program kapsamında tüm bilgi ve belgeleri** isteyebilecektir. **Bu noktada akıllara gelen soru, veri sorumlularına veri minimizasyonunu öğütleyen ve aksi halde idari yaptırımlar uygulayan bir otoritenin kendi uygulamalarında böyle bir yola başvurmayışının ne kadar doğru olduğudur.** Taraflardan istenen belgeler için öngörülen süre on beş gün olarak belirlenmiştir ve **"tüm bilgi ve belgeler"** şeklindeki nitelendirmeler süre de göz önüne alındığında arka planda hazırlığının yapılmasını olanaksız kılmakta ve **gecikmelere daha Tebliğ'in doğuşunda sebebiyet vermektedir.**

Çelişki içeren ve açıkta bırakılan bir diğer durum da personel belgelendirme kuruluşunun yetkisinin iptal edildiği durumlarda o kuruluşun veri koruma görevlisi unvanını kazandırdığı kişiler açısından ne gibi bir yaptırımı olacağının belirtilmemesidir.

> *"Sınav tarihinden önceki son 4 yıl içinde katılım belgesi almış olanlar veya geçerli bir veri koruma görevlisi sertifikasına sahip olanlar arasından programda belirlenen şartları haiz olanlar veri koruma görevlisi sertifikası sınavına başvurmaya hak kazanırlar."*

Tebliğin m.11/1. fıkrası uyarınca sınava başvuruda bulunabilmek için *sınav tarihinden önceki 4 yıl içince katılım belgesi almış olanlar/geçerli sertifikaya sahip olanlar* şartı konulmuştur. Bu durumda **halihazırda bu hizmeti sunan kuruluşlardan bazılarının geçerli sertifikayı sağladığının varsayılacağı** anlaşılmaktadır. Yapılan değerlendirmeler neticesinde "geçerli sertifikayı" sağlayabilen kuruluşların daha sonradan yetkilendirilmesinin iptal edilmesi halinde sınava girip unvana hak kazanan veri koruma görevlilerinin unvanının geçerliliği hususunda bir açıklamada bulunulmamıştır.

İlgili hususlarda daha önce de görüldüğü gibi Kurul'un belli açıklamalarda ve netleştirmelerde bulunması beklenecek, de facto uygulamaların takip edilmesi gerekecektir.

Veri Koruma Görevlisi vs. Data Protection Officer

DPO, Avrupa Birliği'nde Mayıs 2018'de yürürlüğe giren GDPR kapsamında düzenlenen bir kavramdır. Bu düzenlemenin amacı, veri sorumlularının mevzuata uyması konusunda sorumlu olacak bir kişinin atanmasını sağlamaktır. GDPR, bir takım kriterleri karşılayan veri sorumlularına veri koruma görevlisi atama yükümlülüğü getirmekte ve söz konusu veri koruma görevlisinin görev ve yükümlülüklerini detaylı olarak ele almaktadır.

DPO'nun birincil rolü kuruluşunun *personelinin, müşterilerinin, sağlayıcılarının veya diğer kişilerin (veri öznesi-ilgili kişi)* kişisel verilerini veri kurallarına uygun olarak işlemesini sağlamaktır.

GDPR'ın 37. maddesi uyarınca Avrupa Birliği kurum ve kuruluşlarında DPO atanması zorunlu kılınmıştır. Yaygın inanışın aksine, bir DPO atanmasına ilişkin yasal zorunluluk için belirleyici olan, **şirketin büyüklüğü değil**, şirketin hedeflerine ulaşması için gerekli olanlar olarak tanımlanan **temel işleme faaliyetleridir**. Bu temel faaliyetler, **hassas nitelikli kişisel verilerin büyük ölçekte işlenmesini** veya özellikle **ilgili kişilerin haklarına yönelik geniş kapsamlı bir veri işleme biçimini** içeriyorsa, şirketin bir DPO ataması gerekmektedir. **Öte yandan, yargı yetkisine göre hareket eden mahkemeler dışında, kamu kurumları her zaman bir DPO atamak zorundadır.**

CNIL. Herhangi bir yasal zorunluluk yoksa, şirketler veri koruma uyumluluğuna yardımcı olmak için gönüllü olarak bir DPO atayabilir *(örneğin, Fransız veri koruma yetkilisi CNIL tarafından tavsiye edilir)*.

Şirketler, DPO atama yükümlülüklerini yerine getirmek için iki seçeneğe sahiptir. Bu kapsamda ya bir çalışan DPO olarak adlandırılır ya da harici, dışarıdan bir DPO atanır. **Dahili bir DPO'nun Bilgi Teknolojileri ya da İnsan Kaynakları departmanında veya üst yönetimdeki görevleri nedeniyle bir çıkar çatışmasına maruz kalmamasının ve kendini de denetlemesinin sağlanması önem arz etmektedir.**

Hangi seçeneğin seçildiğine bakılmaksızın, bir DPO, veri işlemenin karmaşıklığına ve şirketin büyüklüğüne bağlı olarak, veri koruma mevzuatı ve teknik tedbir güvenliği konusunda uzman profesyonel bilgi sağlamalıdır. DPO'nun görevleri ve nitelikleri GDPR m. 39 hükmünde detaylı olarak ele alınmıştır.

İngiltere, muhatap bir kamu kurumu veya kuruluşu ise veya belirli türde işleme faaliyetleri yürütüyorsa, bir DPO atanmasını öngörmekte; ilgili DPO Veri Koruma Etki Değerlendirmeleri (Data Protection Impact Assessments, DPIA) hakkında tavsiyelerde bulunmaya, veri sahipleri ve Bilgi Komiserliği Ofisi (Information Commissioner's Office, ICO) için bir iletişim noktası olarak hareket etmeye yardımcı olmaktadır.

ico. Information Commissioner's Office

2018 yılında yürürlüğe giren Kanun'da bir DPO öngörülmemekteydi, Türkiye'de yine Kanun'da bahsi geçirilmeyen, Veri Sorumluları Sicil Bilgi Sistemi (**"VERBİS"**) uygulamaları kapsamında Veri Sorumluları Sicili Hakkında Yönetmelik'te düzenlenen ve kullanımı yaygınlaşan **irtibat kişisi** unvanı, GDPR uygulamalarındaki DPO unvanını karşılar nitelikte kurgulanmaktaydı. İngiltere örneğinde bahsedildiği gibi irtibat kişileri hem ilgili kişilere hem de veri koruma otoritesine (Kurum) karşı sorumlu tutulan, ilk iletişimde muhatap alınacak kişi olarak gözükmekteydi.

Görüldüğü üzere İrtibat Kişisi unvanı GDPR'da öngörülen ilgili kişi ve veri koruma otorilerine karşı **ilk muhatap alınan ve irtibat sağlanan gerçek kişi** olma özelliğini taşımaktadır. Ancak DPO'dan **en önemli farkı** veri korumayla ilgili **uzman bilgi sahibi olma ve bu bilgileri sağlama şartının aranmıyor oluşudur**. Güncel düzenlemeyle birlikte Türkiye'deki DPO uygulamasının yalnızca uzmanlık gerektiren noktaya ilişkin eksikliği tamamlamaya yönelik olduğu ve iletişim noktasında herhangi bir sorumluluğunun bulunmayacağı zira bu sorumluluk için irtibat kişilerinin görevlendirilmekte olduğu söylenebilecektir.

GDPR'ın belirlemiş olduğu DPO atama zorunluluğunda; kamu kurum ve kuruluşlarının istisna olmaksızın DPO ataması şartına, Tebliğ'de yer verilmediği gözlemlenmektedir.

GDPR'ın 37. Madde gerekçesinde (recital) yalnızca kamu kurum ve kuruluşlarının değil, kamu görevi görülen özel sektör kişilerinin de (*örnek olarak toplu taşıma araçları, yol, su ve enerji tedariği sağlayan şirketler de gösterilmektedir)* bu zorunluluğa dahil olduğu belirtilmektedir.

İlgili Tebliğ düzenlemesinde veri koruma görevlisini atama zorunluluğuna yer verilmemiş ve belirsiz bırakılmıştır. Tebliğ'de yer verilen uygulamasının geliştirilmesiyle bu hususların zaman içinde açıklığa kavuşturulacağı kanaatindeyiz.

Veri Koruma Görevlisi Belgelendirme Programı

Kurum tarafından Tebliğ kapsamında yapılacak olan sertifikasyon faaliyetine ilişkin olarak **Veri Koruma Görevlisi Belgelendirme Programı** (**"Program"**) hazırlanıp 07.12.2021 tarihinde Kurumun internet sitesinde yayımlanmıştır.

İlgili programın amacı "Kurum tarafından yetkilendirilmiş Personel Belgelendirme Kuruluşuna müracaat eden *adayların başvurularının değerlendirilmesi, sınavların yapılması ve değerlendirilmesi, Veri Koruma Görevlisi veya Veri Koruma Görevlisi adayının belgelendirilmesi veya yeniden belgelendirilmesi ve belgelendirme yöntemi* ile ilgili bütün esasların belirlenmesi" olarak hükmedilmiştir.

Yukarıda izaha çalıştığımız sertifika sahibi olan veri koruma görevlerinin sertifikalarının askıya alınması ve/veya iptal edilmesi hususu bu Programda düzenlenmektedir.

Buna göre; *(i) veri koruma görevlisinin kendi talebiyle, (ii) gerekli koşullardan herhangi birini taşımadığı halde, gerçeğe aykırı beyanda bulunduğunun tespit edilmesi halinde, (iii) belgeyi kötü amaçla veya yanıltıcı bir biçimde kullandığının tespiti halinde, (iv) veri koruma görevlisi hakkında bildirilen şikâyetin değerlendirilmesi sonrasında Kurum veya ilgili mahkemelerce aleyhinde bir karar alındığında, (v) belge üzerinde oynandığının tespiti durumunda,* şartları **sınırlı sayı prensibiyle (numerus clausus)** öngörülmüştür.

Veri koruma görevlisi sertifika sınavına başvuru şartı olarak, *yurt içindeki üniversitelerin veya diploma denkliği Yükseköğretim Kurulu tarafından onaylanmış olmak kaydıyla yabancı üniversitelerin,* ***en az dört yıllık lisans eğitimi veren fakültelerinden mezun olanlardan*** *sınav tarihinden önceki son 4 yıl içerisinde Katılım Belgesi almış olan veya geçerli bir Veri Koruma Görevlisi Sertifikasına sahip olanlar* gösterilmektedir.

Sınav konuları incelendiğinde Kişisel Verilerin Korunması alanında uluslararası mevzuatın da yer aldığı, bu kapsamda sertifika sahibi olabilmek için GDPR, 108 sayılı sözleşme ve 95/46/EC Direktifi hakkında bilgi sahibi olunmasının da arandığı gözlemlenmektedir.

SONUÇ

Yukarıdaki izahlarda açıklanmaya çalışan veri koruma görevlisiyle ilgili düzenlemelerde Tebliğ'in konunun sertifikasyon sürecine odaklandığı ve unvanın ne anlama geldiğiyle ilgili açıklamalarda eksiklikler bulunduğu tespit edilmiştir.

Öncelikli hedef veri koruma görevlisinin mevzuatın sistematiğinde yer aldığı konumu belirlemekten çok kişisel verilerin korunmasıyla ilgili halihazırda verilen danışmanlıklardaki bilgi kirliliği ve yanlış uygulamaların giderilmesini sağlamak olmuştur.

Dolayısıyla hem Tebliğ'de hem de buna bağlı olarak çıkarılan Program'da bahsi geçen hususların açıklanması bir gereklilikten çok ihtiyaç haline gelmiştir.

Bu yazımız ile DPO ve Veri Koruma Görevlisi arasındaki ilişkiyi, bugüne kadarki uygulamada rol üstlenmiş olan irtibat kişilerini ve GDPR uygulamalarını kısaca izaha çalışılmıştır. Veri koruma görevlilerinin belirlenmesinde GDPR kapsamında aranan uzman bilgi sağlayabilme niteliğine Tebliğ'de **"yeterli bilgiye sahip olma"** şeklinde yer verilmesinden hareketle; hukuki nosyon üreticileri olan avukatlara yönelik herhangi bir düzenlemede bulunulmaması ve bu noktada yaşanabilecek hak kayıplarını daha geniş incelemek gerektiğinden bu yazıda yer verilememiştir. Ancak en kısa sürede ilgili düzenlemenin avukatlara yönelik birtakım usul ve esaslar ile regüle edilmesi gerektiği kanaatindeyiz.

Bu itibarla başta ülkemiz veri koruma mevzuatı ile yaşayan kültürün ileri sıçramasını sağlamasını dilediğimiz Tebliğ'e ilişkin bilgilendirme metnimizi tüm ekosistem paydaşlarının dikkatine sunarız.

Saygılarımızla,

İrem Alkan

GRC | LEGAL