**KİŞİSEL VERİLERİN KORUNMASI KONTROL LİSTESİ**

1. Gerçek kişiye ilişkin kişisel veri işliyor musunuz?
2. Tamamen otomatik mi işliyorsunuz kişisel verileri?
3. Kısmen otomatik kısmen kağıt ortamında mı işliyorsunuz?
4. Otomatik olmayan yolla kişisel veri işliyor musunuz? (tamamen kağıt ortamda)?
5. Cevap evet ise, kağıt ortamda işlediğiniz bu kişisel veriler bir veri kayıt sisteminin parçası mı?
6. Cevabınız hayır ise kanunun kapsamında değilsiniz.
7. Cevabınız evet ise kanunun kapsamındasınız.
8. Hangi tür kişisel verileri işliyorsunuz?
   1. Normal kişisel veriler
   2. Özel nitelikli kişisel veriler (Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir).
9. İşlediğiniz kişisel verileri, sizin talimatlarınız doğrultusunda, sizin adınıza işleyen, teknik olarak bu verilerin korunmasını sağlamanıza yardımcı olan üçüncü taraf VERİ İŞLEYEN şirket var mıdır? (Örneğin; Koç Sistem, Garanti Teknoloji, Doğuş Teknoloji gibi)
10. Kişisel verileri hangi amaçla işliyorsunuz?
11. İşlediğiniz kişisel verileri ne kadar süre saklıyorsunuz?
    1. Verileri saklama sürenizi öngören bir kanun var mıdır? (İş kanunu, Vergi Usul Kanunu, Türk Ticaret Kanunu gibi…)
    2. Herhangi bir kanun hükmü yoksa, kişisel verileri işleme amacınız çerçevesinde ne kadar süre saklıyorsunuz?
12. Normal kişisel verileri işlerken
    1. İlgili kişiyi veri işleme amacınız, kişisel veriyi saklama süreniz, yurt içi veya yurt dışı üçüncü taraflarla paylaşıp paylaşmayacağınız, kişisel veriyi toplama yönteminiz konusunda ve 6698 sayılı kanunun 11. Maddesinde sayılı hakları konusunda bilgilendirdiniz mi?
    2. Bu bilgilendirme üzerine İlgili kişinin açık rızasını aldınız mı?
    3. İlgili kişinin açık rızasını almadan istisnai olarak aşağıdaki hallerde normal kişisel veri işlemeniz mümkündür:
       1. Kanunlarda açıkça öngörülmesi.
       2. Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
       3. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
       4. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
       5. İlgili kişinin kendisi tarafından alenileştirilmiş olması.
       6. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
       7. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.
13. Özel nitelikli (hassas) kişisel verileri işlerken
    1. İlgili kişiyi veri işleme amacınız, kişisel veriyi saklama süreniz, yurt içi veya yurt dışı üçüncü taraflarla paylaşıp paylaşmayacağınız, kişisel veriyi toplama yönteminiz konusunda ve 6698 sayılı kanunun 11. Maddesinde sayılı hakları konusunda bilgilendirdiniz mi?
    2. Bu bilgilendirme üzerine ilgili kişinin açık rızasını aldınız mı?
    3. İlgili kişinin açık rızasını almadan istisnai olarak aşağıdaki hallerde özel nitelikli kişisel veri işlemeniz mümkündür:
       1. İlgili kişinin açık rızası ile,
       2. Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin işlenmesini kanunlar öngörmüşse,
       3. Sağlık ve cinsel hayata ilişkin kişisel veriler ise; ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.
14. Kişisel verileri yurt içinde üçüncü taraflara aktarıyor musunuz? Cevabınız evet ise;
    1. Paylaştığınız normal kişisel veri ise 6698 sayılı kanunun 5. Maddesindeki şartların gerçekleşmesi gerekir.
    2. Paylaştığınız özel nitelikli kişisel veri ise 6698 sayılı kanunun 6. Maddesindeki şartların gerçekleşmesi gerekir.
15. Veri sorumlusu olarak, kişisel verisini işlediğiniz ilgili kişiyi aydınlatmak ve hakları konusunda bilgi vermek için, bu amaca özel bir e-posta adresi/telefon numarası oluşturdunuz mu? Aktif olarak işletiyor musunuz?
    1. Çalışanlarınız için bu e-posta adresini/telefon numarasını herhangi bir yöntemle ve şekilde duyurabilirsiniz
    2. Müşterileriniz için bu e-posta adresini/telefon numarasını, web sayfanızdaki “kullanım koşulları ve gizlilik” veya sadece “gizlilik” politikanız içerisinde açıklayınız.
16. Yeni çalışanların iş akitlerine kişisel verilerin korunmasına ilişkin hüküm ilave ettiniz mi?
17. Mevcut çalışanlar için, iş akitlerinin bir parçası teşkil edecek nitelikte açık rızalarını aldınız mı?
18. Veri sorumlusu temsilcisi seçtiniz mi? Cevap evet ise, bu temsilcinin ismini, Veri Sorumluları Siciline bildirdiniz mi? (sicile bildirim tarihi daha sonra belli olacak)
19. İlgili kişi veri sorumlusuna haklarını kullanmak amacıyla, belirttiğiniz e-posta adresi/telefon numarası üzerinden başvurduğunda, bu başvuruya en geç 30 gün içinde cevap vermek için gerekli süreçleri oluşturdunuz mu? *(İlgili kişinin talebi şirket için operasyonel ve finansal anlamda maliyet yaratıyorsa, bu maliyet Kişisel Verileri Koruma Kurulu’nun ilan edeceği tarifede yer alan ücret çerçevesinde ilgili kişiye yansıtılacaktır)*
20. İşlediğiniz kişisel verilerin hukuka aykırı işlenmesini, hukuka aykırı erişimleri önlemek ve muhafazasını sağlamak içini hangi tür idari ve teknik tedbirleri aldınız mı?
21. Şirket içinde farklı departmanlarca işlenen kişisel verilere erişimler için, o departmanda çalışanlar arasında bir erişim kısıtlaması, yetki ve roller ayrımı mevcut mu?
22. Kişisel verileri barındırdığınız IT sistemlerinizin hukuka aykırı erişimlere karşı korunmasını sağlamak amacıyla sızma testi yaptırdınız mı?
23. Şirket içi veya şirket dışından gelebilecek saldırılar/kötüye kullanımlar gibi durumlar yüzünden hiç kişisel veri kaybı/ihlali yaşadınız mı Cevabınız evet ise bu durumu derhal ilgili kişiye ve Kişisel Verileri Koruma Kuruluna bildirdiniz mi?
24. Kişisel verilerinizi işleyen VERİ İŞLEYEN şirket ile aranızdaki sözleşmede, veri güvenliğine ilişkin teknik ve idari tedbirlerin alınması noktasında müşterek ve müteselsilen sorumlu olacaklarına dair hüküm ilave ettiniz mi?
25. 6698 sayılı kanuna uyum için şirketinizde iç denetim yapıyor veya bu konuda dış denetim yaptırıyor musunuz?
26. Veri sorumlusu olarak, VERİ İŞLEYEN şirketin de sizin de süresiz olarak sır saklama yükümlülüğünüz olduğunu sözleşmelerinize ve çalışanlarınızla ilgili iş akitlerine ilave ettiniz mi?
27. Şirketiniz hangi tarihten itibaren elektronik ortamı kullanmaya başladı?
28. Şirketinizde varlık yönetimi ile ilgili herhangi bir çalışma var mı? Verilerinizi, belgelerinizi sınıflandırdınız mı?
29. İster VERİ İŞLEYEN ister iş yaptığınız herhangi bir üçüncü şirket olsun,
    1. Sözleşme imzalamadan önce kullandığınız NDA’lere kişisel verilerin gizliliği ve korunmasına ilişkin hükümler ilave ettiniz mi?
    2. İmzalanacak Sözleşmelerinize kişisel verilerin gizliliği ve korunmasına ilişkin hükümler ilave ettiniz mi?
    3. Mevcut sözleşmelerine bu hükümleri ilave edecek şekilde ek protokol yaptınız mı?
30. Kişisel verileri yurt dışına aktarıyor musunuz? Cevabınız evet ise;
    1. İlgili kişinin açık rızası var mı?
    2. Yoksa;
       1. işlediğiniz kişisel veri normal kişisel veri ise, 6698 sayılı kanunun 5. Maddesinin 2. Fıkrasındaki istisnalardan birine giren bir durum var mı?
       2. İşlediğiniz veri özel nitelikli veri ise 6698 sayılı kanunun 6. Maddesindeki koşullar gerçekleşmişse yurt dışına aktarım mümkün olabilecektir ve ayrıca
       3. Kişisel verileri aktaracağınız ülkede yeterli koruma var mı? Varsa aktarım mümkün olacaktır. Yoksa Sizin ve yurt dışındaki partner’ınızın yeterli korumayı yazılı olarak taahhüt etmesi ve Kişisel Verilerin Korunması Kurulu’nun izninin bulunması şarttır.
31. Yurt dışından Şirketinize kişisel veri aktarımı söz konusu mu?
    1. Cevabınız evet ise; ilgili ülkede yeterli koruma var mı?