KİŞİSEL VERİLERİN KORUNMASI KANUNU

(KVKK)

İDARİ VE TEKNİK TEDBİRLER

İçindekiler

Amaç ve Dayanak

Kanunun 12 nci maddesinin birinci fıkrasında;
“**Veri sorumlusu**;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
c) Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.”

hükmü yer almaktadır.

Kişisel Veri Güvenliğinin Takibi

Veri sorumlularının sistemleri çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olup çeşitli belirtilere rağmen bu durum uzun süre fark edilememekte ve müdahale için geç kalınabilmektedir.
Bu durumun önüne geçebilmek için;

a) Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi,
b) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi,
c) Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi),
ç) Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması,
d) Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması,

gerekmektedir.

Mevcut Risk ve Tehditlerin Belirlenmesi

Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir.

Bu riskler belirlenirken;

- Kişisel verilerin özel nitelikli kişisel veri olup olmadığı,
- Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği,
- Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır.

Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır.

Kişisel Verilerin korunmasında Veri Sorumlusunun Yükümlü Olduğu İdari ve Teknik Tedbirler

No	Tedbir	Tedbir Kapsamı	Açıklama
1	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi 1	**Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı.** 1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,
2	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik 2-a	a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,
3	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik 2-b	Çalışanlar ile Gizlilik sözleşmesi yapılması
4	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik 2-c	Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,
5	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik 2-ç	Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
6	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik 2-d	Görev değişikliği olan ya da işten ayrılan Çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade

			alınması,
7	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise 3-a	Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
8	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise 3-b	Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
9	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise 3-c	Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
10	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise 3-ç	Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
11	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise 3-d	Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
12	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise 3-e	Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,
13	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise 4-a	Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
14	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde	Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise	Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların

	Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	4-b	engellenmesi,
15	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel veriler aktarılacaksa 5- a	Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,
16	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel veriler aktarılacaksa 5- b	Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
17	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel veriler aktarılacaksa 5- c	Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,
18	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Özel nitelikli kişisel veriler aktarılacaksa 5- ç	Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” formatında gönderilmesi gerekir.
19	Kurul Kararları-Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler.	Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır. 6	
20	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin İdari Tedbirler	Risklerin ve tehditlerin belirlenmesi 2.1.	Bu riskler belirlenirken;● Kişisel verilerin özel nitelikli kişisel veri olup olmadığı,● Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği,● Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmış mıdır ?
21	Yayınlar- Kişisel Veri Güvenliği Rehberi-	Çalışanların Eğitilmesi ve Farkındalık Çalışmaları 2.2.	

	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Yayınlar- Kişisel Veri Güvenliği Rehberi-	
22	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Yayınlar- Kişisel Veri Güvenliği Rehberi-	Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi 2.3.
23	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Yayınlar- Kişisel Veri Güvenliği Rehberi-	Kişisel Verilerin Mümkün Olduğunca Azaltılması 2.4.
24	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Yayınlar- Kişisel Veri Güvenliği Rehberi-	Veri İşleyenler ile İlişkilerin Yönetimi 2.5.
25	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Özet Tablosu Yayınlar- Kişisel Veri Güvenliği Rehberi-	Kişisel Veri İşleme Envanteri Hazırlanması
26	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Özet Tablosu Yayınlar- Kişisel Veri Güvenliği Rehberi-	Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
27	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Özet Tablosu Yayınlar- Kişisel Veri Güvenliği Rehberi-	Sözleşmeler (Veri Sorumlusu – Veri Sorumlusu, Veri Sorumlusu – Veri İşleyen Arasında)
28	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Özet Tablosu Yayınlar- Kişisel Veri Güvenliği Rehberi-	Gizlilik Taahhütnameleri
29	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Özet Tablosu Yayınlar- Kişisel Veri Güvenliği Rehberi-	Kurum İçi Periyodik ve/veya Rastgele Denetimler
30	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Yayınlar- Kişisel Veri Güvenliği Rehberi-	Risk Analizleri

	Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Özet Tablosu Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Özet Tablosu		
31		İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi)	
32	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Özet Tablosu	Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimivb.)	
33	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Özet Tablosu	Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)	
34	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin İdari Tedbirler Özet Tablosu	Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim	
35	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler	Siber Güvenliğin Sağlanması 3.1.	
36	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler	Kişisel Veri Güvenliğinin Takibi 3.2.	Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi (a)
37	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler	Kişisel Veri Güvenliğinin Takibi 3.2.	Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi (b)
38	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler	Kişisel Veri Güvenliğinin Takibi 3.2.	Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi) (c)
39	Yayınlar- Kişisel Veri Güvenliği Rehberi-	Kişisel Veri Güvenliğinin Takibi 3.2.	Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde

	Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler		raporlanması (ç)
40	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler	Kişisel Veri Güvenliğinin Takibi 3.2.	Çalışanların sistem ve servislerdeki güvenlik zafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması (d)
41	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler	Kişisel Veri İçeren Ortamların GüvenliğininSağlanması 3.3.	
42	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler	Kişisel Verilerin Bulutta Depolanması 3.4.	
43	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler	Bilgi Teknolojileri Sistemleri Tedariği, Geliştirmeve Bakımı 3.5.	
44	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler	Kişisel Verilerin Yedeklenmesi 3.6.	
45	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Yetki Matrisi	
46	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Yetki Kontrol	
47	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Erişim Logları	
48	Yayınlar- Kişisel Veri	Kullanıcı Hesap Yönetimi	

	Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	
49	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Ağ Güvenliği
50	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Uygulama Güvenliği
51	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Şifreleme
52	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Sızma Testi
53	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Saldırı Tespit ve Önleme Sistemler
54	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Log Kayıtları
55	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Veri Maskeleme
56	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri	Veri Kaybı Önleme Yazılımları

	Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	
57	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Yedekleme
58	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Güvenlik Duvarları
59	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Güncel Anti-Virüs Sistemler
60	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Silme, Yok Etme veya Anonim Hale Getirme
61	Yayınlar- Kişisel Veri Güvenliği Rehberi- Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler Özet Tablo	Anahtar Yönetimi
62	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	1.Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurtiçinde güvenli bir şekilde depolanacaktır.
63	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	2. Kamu kurum ve kuruluşlarında yer alan kritik veriler, internete kapalı ve fiziksel Güvenliği sağlanmış bir ortamda bulunan güvenli bir ağda tutulacak, bu ağda kullanılacak cihazlara erişim kontrollü olarak sağlanacak ve log kayıtları değiştirilmeye karşı önlem alınarak saklanacaktır.
64	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı	3.Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri veya kurum kontrolündeki

	Cumhurbaşkanlığı Genelgesi Hakkında	yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır.
65	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	4.Mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilen yerli mobil uygulamalar hariç olmak üzere, mobil uygulamalar üzerinden, gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.
66	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	5.Sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.
67	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	6.Sosyal medya ve haberleşme uygulamalarına ait yerli uygulamaların kullanımı tercih edilecektir.
68	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	7.Kamu kurum ve kuruluşlarınca gizlilik dereceli bilgilerin işlendiği yerlerde yayma Güvenliği (TEMPEST) veya benzeri güvenlik önlemleri alınacaktır.
69	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	8.Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında mobil cihazlar ve veri transferi özelliğine sahip cihazlar bulundurulmayacaktır.
70	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	9.Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda (dizüstü bilgisayar, mobil cihaz, harici bellek vb.) bulundurulmayacaktır.
71	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	10.Kişisel olarak kullanılanlar da dâhil olmak üzere kaynağından emin olunmayan taşınabilir cihazlar (dizüstü bilgisayar, mobil cihazlar, harici bellek/disk, CD/DVD vb.) kurum sistemlerine bağlanmayacaktır. Gizlilik dereceli verilerin saklandığı cihazlar, ancak içerisinde yer alan veriler donanımsal ve/veya yazılımsal olarak kriptolanmak suretiyle kurum dışına çıkarılabilecek; bu amaçla

		kullanılan cihazlar kayıt altına alınacaktır.
72	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	11.Yerli ve milli kripto sistemlerinin geliştirilmesi teşvik edilerek, kurumlara ait gizlilik dereceli haberleşmenin bu sistemler üzerinden gerçekleştirilmesi sağlanacaktır.
73	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	12.Kamu kurum ve kuruluşlarınca temin edilecek yazılım veya donanımların kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınacaktır.
74	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	13.Yazılımların güvenli olarak geliştirilmesi ile ilgili tedbirler alınacaktır. Temin edilen veya geliştirilen yazılımlar kullanılmadan önce güvenlik testlerinden geçirilerek kullanılacaktır.
75	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	14.Kurum ve kuruluşlar, siber tehdit bildirimleri ile ilgili gerekli tedbirleri alacaktır.
76	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	15.Üst düzey yöneticiler de dahil olmak üzere, personelin sistemlere erişim yetkilendirmelerinin, fiilen yürütülen işler ve ihtiyaçlar nazara alınarak yapılması sağlanacaktır.
77	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	16.Endüstriyel kontrol sistemlerinin internete kapalı konumda tutulması sağlanacak, söz konusu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise gerekli güvenlik önlemleri (güvenlik duvarı, uçtan uca tünelleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınacaktır.
78	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	17.Milli Güvenliği doğrudan etkileyen stratejik önemi haiz kurum ve kuruluşların üst yöneticileri ile kritik altyapı, tesis ve projelerde görev alacak kritik önemi haiz personel hakkında ilgili mevzuat çerçevesinde güvenlik soruşturması

		veya arşiv araştırması yaptırılacaktır.	
79	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	18.Kamu e-posta sistemlerinin ayarlan güvenli olacak biçimde yapılandırılacak, e- posta sunucuları, ülkemizde ve kurumun kontrolünde bulundurulacak ve sunucular arasındaki iletişimin şifreli olarak yapılması sağlanacaktır.	
80	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	19. Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmayacak, kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.	
81	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	20. Haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmeciler Türkiye’de internet değişim noktası kurmakla yükümlüdür. Yurtiçinde değiştirilmesi gereken yurtiçi iletişim trafiğinin yurtdışına çıkarılmamasına yönelik tedbirler alınacaktır.	
82	“Bilgi ve İletişim Güvenliği Tedbirleri” konulu 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi Hakkında	21.İşletmeciler tarafından, kritik kurumların bulunduğu bölgelerdeki veriler, radyolink ve benzeri yöntemlerle taşınmayacak, fiber optik kablolar üzerinden taşınacaktır. Kritik veri iletişiminde, radyolink haberleşmesi kullanılmayacak; ancak kullanımın zorunlu olduğu durumlarda veriler milli kripto sistemlerine sahip cihazlar kullanılarak kriptolanacaktır.	
83	“Bilgi ve İletişim Güvenliği Rehberi”	Tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde yeni kurulacak bilgi sistemlerinde, Rehberde yer verilen usul ve esaslara uyulması zorunludur.	yayınlanacak
84	“Bilgi ve İletişim Güvenliği Rehberi”	Milli Güvenliğin sağlanması ve gizliliğin korunması kapsamında yürütülen görev ve faaliyetler hariç olmak üzere kurum ve kuruluşlar, Rehberin uygulanmasına ilişkin denetim mekanizmalarını oluşturacak ve yılda en az bir defa uygulamayı denetleyecektir. Denetim sonuçlan ile yapılan düzeltici ve önleyici faaliyetler,	yayınlanacak

		Rehberde belirtilen usul ve esaslara göre bir rapor halinde Dijital Dönüşüm Ofisine iletilecektir.
85	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	1. Ağ Güvenliği ve uygulama Güvenliği sağlanmaktadır.
86	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	2. Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
87	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	3. Anahtar yönetimi uygulanmaktadır.
88	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	4. Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
89	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	5. Bulutta depolanan kişisel verilerin Güvenliği sağlanmaktadır.
90	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	6. Çalışanlar için veri Güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
91	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	7. Çalışanlar için veri Güvenliği konusunda belli aralıklarla Eğitim ve farkındalık çalışmaları yapılmaktadır.
92	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	8. Çalışanlar için yetki matrisi oluşturulmuştur.
93	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	9. Erişim logları düzenli olarak tutulmaktadır.
94	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	10. Erişim, bilgi Güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlamıştır.
95	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	11. Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
96	VERBİS'e kayıtta veri envanterinde beyan	12. Gizlilik taahhütnameleri yapılmaktadır.

	edilecek veri güvenlik tedbirleri	
97	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	13. Görev değişikliği olan ya da işten ayrılan Çalışanların bu alandaki yetkileri kaldırılmaktadır.
98	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	14. Güncel anti-virüs sistemleri kullanılmaktadır.
99	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	15. Güvenlik duvarları kullanılmaktadır.
100	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	16. İmzalanan sözleşmeler veri Güvenliği hükümleri içermektedir.
101	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	17. Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
102	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	18. Kişisel veri Güvenliği politika ve prosedürleri belirlenmiştir.
103	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	19. Kişisel veri Güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
104	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	20. Kişisel veri güvenliğinin takibi yapılmaktadır.
105	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	21. Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
106	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	22. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı Güvenliği sağlanmaktadır.
107	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	23. Kişisel veri içeren ortamların Güvenliği sağlanmaktadır.
108	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik	24. Kişisel veriler mümkün olduğunca azaltılmaktadır.

	tedbirleri	
109	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	25. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin Güvenliği de sağlanmaktadır.
110	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	26. Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
111	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	27. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
112	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	28. Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
113	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	29. Mevcut risk ve tehditler belirlenmiştir.
114	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	30. Özel nitelikli kişisel veri Güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
115	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	31. Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve
116	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
117	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	32. Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
118	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	33. Saldırı tespit ve önleme sistemleri kullanılmaktadır.
119	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	34. Sızma testi uygulanmaktadır.
120	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	35. Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
121	VERBİS'e kayıtta veri	36. Şifreleme yapılmaktadır.

	envanterinde beyan edilecek veri güvenlik tedbirleri	
122	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	37. Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
123	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	38. Veri işleyen hizmet sağlayıcılarının veri Güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
124	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	39. Veri işleyen hizmet sağlayıcılarının, veri Güvenliği konusunda farkındalığı sağlanmaktadır.
125	VERBİS'e kayıtta veri envanterinde beyan edilecek veri güvenlik tedbirleri	40. Veri kaybı önleme yazılımları kullanılmaktadır.

Şirketimizde almış olduğumuz Veri Güvenliği tedbirleri

Veri Güvenliği Tedbiri
Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
Anahtar yönetimi uygulanmaktadır.
Bilgi teknolojileri sistemleri tedarik, gelistirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
Çalışanlar için yetki matrisi oluşturulmuştur.
Erişim logları düzenli olarak tutulmaktadır.

Veri Güvenliği Tedbiri
Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
Gizlilik taahhütnameleri yapılmaktadır.
Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
Güncel anti-virüs sistemleri kullanılmaktadır.
Güvenlik duvarları kullanılmaktadır.
İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
Kişisel veri güvenliğinin takibi yapılmaktadır.
Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
Mevcut risk ve tehditler belirlenmiştir.
Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
Saldırı tespit ve önleme sistemleri kullanılmaktadır.
Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.