çelebi | eğitim danışmanlık mühendislik dış ticaret

KURUMSAL TEKNİK VE ORGANİZASYONEL TEDBİRLER

Doküman Tarih ve Sayısı: 22 Aralık 2017 - ÇLB-YNT-05/2017

Gaziantep - Turkey

Çelebi Eğitim Danışmanlık Mühendislik Dış Ticaret Ltd. Şti.
İncilipınar Mah. Prof. Muammer Aksoy Blv. Nişantaşı Sok.
Prestij Ap. A-Blok No:5/11 Şehitkamil - Gaziantep
www.byclb.com - iletisim@byclb.com

Bu doküman Çelebi Eğitim Danışmanlık Mühendislik Dış Ticaret Ltd. Şti. tarafından hazırlanmış olup, üçüncü kişiler tarafından kopyalanamaz ve kullanılamaz

çelebi | eğitim danışmanlık mühendislik dış ticaret

ÇLB-YNT-05-2017.22122017

Sayı : ÇLB-YNT-05-2017 22 Aralık 2017

Konu : Kurumsal Teknik ve Organizasyonel Tedbirler

İlgi

a) 24.03.2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu

b) 28.10.2017 tarihli ve 30224 sayılı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

c) Avrupa Parlamentosu ve Konseyi'nin (AB) 2016/679 sayılı Genel Veri Koruma Tüzüğü (GDPR)

d) Çelebi Kurumsal Etik İlkeler Yönetmeliği (12.12.2009 – ÇLB-YNT-01-2009)

e) Çelebi Kurumsal Gizlilik İlkeleri Yönetmeliği (18.12.2009 – ÇLB-YNT-02-2009)

f) Çelebi Kurumsal Yönetim İlke ve Prosedürleri Yönetmeliği

Amaç

Teknik ve Organizasyonel Tedbirlerin (TOM) amacı; Çelebi Danışmanlık bünyesinde yürütülen kişisel veri işleme ve veri koruma faaliyetlerinin ulusal ve uluslararası mevzuata (İlgi a, b ve c) uygunluğunu sağlamak üzere uygulanacak usul ve esasları belirlemektir.

Çelebi Danışmanlık'ın;

- Kurumsal Etik İlkeler Davranış Kodu,
- Kurumsal Gizlilik İlkeleri,
- Kurumsal Yönetim İlke ve Prosedürleri

bu dokümanın ayrılmaz, tamamlayıcı ve bütünleyici parçalarıdır ve Teknik ve Organizasyonel Tedbirler ile birlikte değerlendirilir.

Kapsam ve Sorumluluk

Teknik ve Organizasyonel Tedbirler, Çelebi bünyesinde çalışan tüm personeli kapsar. Tüm çalışanların bu dokümanda belirtilen ilkelere uyması zorunludur. Çelebi çalışanları; bu ilkelerin uygulanmasından, uygunsuzlukların tespitinden ve düzeltici önlemlerin alınmasından sorumludur.

Yürürlük

Bu dokümanda ana çerçevesi belirtilen Çelebi Danışmanlık Teknik ve Organizasyonel Tedbirleri, şirket kurucuları tarafından kabul edilmiştir.

Kamuya Açıklık

Teknik ve Organizasyonel Tedbirler kamuya ve tüm çalışanlara açık şekilde ilan edilir. Bu dokümanda yapılacak her türlü değişiklik için de aynı yükümlülük geçerlidir.

Aysun ÇELEBİ	Ömer Cengiz ÇELEBİ
Genel Müdür	Genel Müdür

İçindekiler

1 Veri Koruma ve Veri Güvenliği Kavramı 1
2 Gizlilik 1
2.1 Erişim Kontrolü 1
2.1.1 Fiziksel Güvenlik 1
2.1.2 Güvenlik Bölgeleri 1
2.1.3 Erişim Kontrol Türü 1
2.1.4 Erişim Yetkilendirmesinin Düzenlenmesi 1
2.2 Veri İşleme Sistemlerine Erişim Kontrolü 2
2.2.1 Erişim Yetkilendirme Kontrolü 2
2.2.2 Uzaktan Erişim İçin Ek Tedbirler 2
2.3 Erişim Kayıtlarının Tutulması 2
2.4 Erişim Kontrolü / Kullanıcı Kontrolü 2
2.4.1 Yetkilendirme Kavramı 3
2.4.2 Erişim Kontrolü 3
2.4.3 Veri Saklama Ortamlarının Kullanımında Güvenlik 3
3 Bütünlük 1
3.1 İletim Kontrolü / Aktarım Kontrolü 1
3.1.1 Elektronik Aktarıma İlişkin Düzenlemeler 1
3.1.2 Taşınabilir Ortamlarda Saklamaya İlişkin Düzenlemeler 1
3.1.3 Veri Saklama Ortamlarının İmhasına İlişkin Düzenlemeler 1
3.2 Girdi Kontrolü / Veri Saklama Ortamı Kontrolü / Saklama Kontrolü 1
4 Erişilebilirlik ve Dayanıklılık / Kurtarılabilirlik 1
4.1 Yedeklerin Oluşturulması ve Muhafazası 1
4.2 Günlük Operasyonların Güvence Altına Alınması 1
4.2.1 Dayanıklılık 1
4.2.2 Kesintisiz Güç Kaynağı 1
4.2.3 İklimlendirme 1
4.2.4 İnternet Bağlantısı 1
4.3 Organizasyonel Tedbirler 1
5 Düzenli İzleme, Değerlendirme ve Denetim Prosedürü 1

5.1 Veri Koruma Yönetimi 1
5.2 Olay Müdahale Yönetimi 1
5.3 Tasarım Yoluyla ve Varsayılan Olarak Veri Koruma 1
5.4 Talimatlara Uygunluk Kontrolü 1
EK – Denetçiler için Teknik ve Organizasyonel Tedbirler Kontrol Listesi 3
A. Genel Veri Koruma Yönetimi 3
B. Gizlilik – Fiziksel Güvenlik 3
C. Veri İşleme Sistemlerine Erişim 3
D. Bütünlük 4
E. Erişilebilirlik ve Dayanıklılık 4
F. Veri İşleyen / Taşeron Kontrolü 4
G. Denetçi Notları 4

1 Veri Koruma ve Veri Güvenliği Kavramı

Çelebi Danışmanlık; kişisel verilerin işlenmesi sırasında, ilgili mevzuat (**İlgi** a, b ve c) kapsamında öngörülen teknik ve organizasyonel tedbirleri almakta, mümkün olan durumlarda kişisel verileri anonimleştirmekte veya takma adlandırmaktadır.

Uygulanan tüm tedbirler; ilgili veri işleme faaliyetinin doğurduğu riskler dikkate alınarak, güncel teknik seviyeye uygun şekilde belirlenir.

Tedbirlerin etkinliği; gizlilik, bütünlük, erişilebilirlik ve kapasite hedefleri doğrultusunda değerlendirilir.

Güvenlik Kavramlarının Tanımları:

- **Gizlilik:** Yetkisiz erişim ve ifşaya karşı verilerin korunması
- **Bütünlük:** Verilerin doğruluğu ve eksiksizliği
- **Erişilebilirlik:** Bilgi ve sistemlerin gerektiğinde kullanılabilir olması
- **Dayanıklılık:** Sistemlerin arıza, yoğunluk veya kesinti durumlarında çalışmaya devam edebilme yeteneği

Çelebi Danışmanlık kişisel verileri;

- Şirket içi bilgi işlem sistemlerinde ve depolama alanlarında,
- Üçüncü taraf hizmet sağlayıcıya ait uzak sunucularda saklamaktadır.

Bu dokümanda açıklanan tedbirler her iki ortam için de geçerlidir.

2 Gizlilik

Gizliliğin korunmasını sağlamak amacıyla uygun teknik ve organizasyonel tedbirler uygulanmaktadır. Tekniğin güncel durumu, uygulama maliyetleri ile veri işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçları; ayrıca gerçek kişilerin hak ve özgürlükleri açısından ortaya çıkabilecek risklerin olasılığı ve ağırlığı dikkate alınarak, kişisel verilerin gizliliğini temin etmek üzere aşağıdaki tedbirler alınmaktadır.

2.1 Erişim Kontrolü

Kişisel verileri işleyen ve/veya kullanan veri işleme sistemlerine yetkisiz kişilerin erişimini engellemek amacıyla aşağıdaki tedbirler uygulanmaktadır:

2.1.1 Fiziksel Güvenlik

- Binadaki tüm kapılar, giriş için birbirinden farklı ve benzersiz anahtarlar gerektirmektedir.
- Ana giriş kapısı, ofis içerisinden diyafon sistemi aracılığıyla uzaktan kontrol edilmektedir.
- Ana girişte, düşük görüş koşulları için aydınlatma sistemi bulunmaktadır.
- Yetkisiz kişilerin bina içerisinde tek başına dolaşması yasaktır; bu kişiler ancak bir güvenlik görevlisi eşliğinde binada bulunabilir.
- Otopark alanı güvenlik görevlileri tarafından kontrol edilmektedir.
- Yetkisiz kişilerin kontrollü otopark alanına giriş yapması ve araç park etmesi yasaktır.
- Ofis girişi güçlendirilmiş kapı ile korunmakta olup, aynı anda birden fazla anahtar kombinasyonu gerektirmektedir.
- Ofis girişi diyafon ve aydınlatma sistemi ile kontrol edilmektedir.
- Ofise erişim yalnızca yetkili kişilere verilmektedir.

2.1.2 Güvenlik Bölgeleri

Veri sunucusu, ofis alanlarından ayrılmış, erişimi sınırlandırılmış ve gözetim altında tutulan bir alanda, üçüncü taraf bir hizmet sağlayıcı tarafından muhafaza edilmekte ve işletilmektedir.

2.1.3 Erişim Kontrol Türü

- Kişisel erişim kartları ve akıllı kart okuyucular aracılığıyla giriş-çıkış kayıtlarının tutulduğu otomatik kimlik doğrulama sistemi uygulanmaktadır.
- Ofisler, mekanik anahtar sistemi ile güvence altına alınmıştır.

2.1.4 Erişim Yetkilendirmesinin Düzenlenmesi

- Erişim yetkilendirmeleri, uygun yetkilendirme prosedürleri çerçevesinde düzenlenmekte ve verilmektedir.
- Anahtarların kaybolması durumunda uygulanacak kurallar ve takip tedbirleri bulunmaktadır.
- Bakım ve onarım personeli gözetim altında tutulmaktadır.
- Erişim yetkisinin verilmesi ve geri alınması süreçleri gözden geçirilebilir niteliktedir.

2.2 Veri İşleme Sistemlerine Erişim Kontrolü

Yetkisiz kişilerin veri işleme sistemlerini kullanması aşağıdaki tedbirlerle engellenmektedir:

2.2.1 Erişim Yetkilendirme Kontrolü

- Kullanıcılara erişim yetkileri, yetkilendirme prosedürleri doğrultusunda tanımlanmaktadır.
- Her kullanıcıya özel kullanıcı kimliği (User ID) ve başlangıç şifresi tahsis edilmektedir.
- Sisteme erişim, yalnızca kimlik doğrulama (kullanıcı adı ve şifre) sonrasında sağlanmaktadır.
- Ekran oturumları, belirli bir süre sonra parola gerektiren ekran koruyucular ile otomatik olarak korunmakta ve ayrıca manuel olarak kilitlenebilmektedir.
- Parola güvenliğine (uzunluk, karmaşıklık ve saklama) ilişkin tedbirler ve parola kullanım kuralları uygulanmaktadır.
- Parolaların kaybolması veya unutulması durumunda izlenecek kurallar belirlenmiştir.
- Yetkilendirme süreçlerinde "bilmesi gereken" ve "yapması gereken" ilkelerini zorunlu kılan bir kural uygulanmaktadır.
- Yönetici hesapları yalnızca sınırlı faaliyetler için kullanılmaktadır.
- Kullanıcılar, yalnızca kendilerine tanımlanan yetkiler (rol bazlı yetkilendirme) kapsamında kişisel verilere erişebilmektedir.
- Kişisel veriler, CIMS (Çelebi Bilgi Yönetim Sistemi) içerisinde güvenli şekilde saklanmaktadır.

2.2.2 Uzaktan Erişim İçin Ek Tedbirler

- Ağ erişim güvenliği, donanım ve yazılım tabanlı önlemlerle sağlanmaktadır.
- İnternet üzerinden yetkisiz erişim donanımsal güvenlik önlemleri ile engellenmektedir.
- Yetkisiz erişim girişimleri, ilgili yazılımlar aracılığıyla tespit edilebilmektedir (izinsiz giriş tespiti).
- Mevcut oturumların başka kullanıcılar tarafından ele geçirilmesine karşı (oturum ele geçirme) koruma sağlanmaktadır.

2.3 Erişim Kayıtlarının Tutulması

- Veri işleme sistemlerine ve iş istasyonlarına erişimler kayıt altına alınmaktadır (örneğin log dosyaları aracılığıyla).
- Veri işleme sistemlerinin kullanımı doğrulanabilir niteliktedir (erişim kayıtları tutulmaktadır).
- Uzaktan erişimler SSL aracılığıyla güvence altına alınmaktadır.

2.4 Erişim Kontrolü / Kullanıcı Kontrolü

Veri işleme sistemlerinin kullanımı sırasında, yetkili kişilerin yalnızca kendilerine tanımlanan erişim yetkileri kapsamındaki verilere erişebilmesi; kişisel verilerin işlenmesi, kullanılması ve saklanması esnasında ve sonrasında yetkisiz şekilde okunmasının, kopyalanmasının, değiştirilmesinin veya silinmesinin önlenmesi sağlanmalıdır. Bu amaçla aşağıdaki tedbirler uygulanmaktadır:

2.4.1 Yetkilendirme Kavramı

- Erişim yetkilerinin verilmesi ve yönetilmesine ilişkin kurallar oluşturulmuştur.
- Bireysel erişim hakları ve kullanıcı grupları tanımlanmıştır.
- Verilen yetkiler düzenli olarak gözden geçirilmektedir.

2.4.2 Erişim Kontrolü

- Şifreleme yöntemlerinin kullanımı sağlanmıştır.
- Ağ içi erişim güvenliği tesis edilmiştir.
- Yalnızca onaylı donanım ve yazılımlar kullanılmaktadır.
- Ağ bileşenleri korunmaktadır.
- Test ortamları ile canlı (üretim) ortamları birbirinden ayrılmıştır.
- Veritabanı (SQL) sorgu yetkileri sınırlandırılmıştır.

2.4.3 Veri Saklama Ortamlarının Kullanımında Güvenlik

- Veri saklama ortamlarının muhafazası kontrol altında tutulmaktadır.
- Veri saklama cihazları onarılmamakta; bunun yerine güvenli silme veya imha işlemlerine tabi tutulmaktadır.
- Veri saklama cihazlarının ortamdan çıkarılmasına yetkili kişiler belirlenmiştir.

3 Bütünlük

Kişisel verilerin işlenmesi sürecinde, tüm bilgi ve verilerin fiilî ve teknik doğruluğu ile bütünlüğü ve eksiksizliği güvence altına alınmaktadır. Hatalı verilerin tespit edilmesi ve düzeltilmesi sağlanmalıdır. Aşağıda belirtilen kontroller, kişisel verilerin bütünlüğünü temin etmeye yöneliktir:

3.1 İletim Kontrolü / Aktarım Kontrolü

Elektronik iletim veya veri aktarımı sırasında yetkisiz okuma, kopyalama, değiştirme veya silme işlemlerinin önlenmesi gerekmektedir. Bu amaçla aşağıdaki tedbirler uygulanmaktadır:

3.1.1 Elektronik Aktarıma İlişkin Düzenlemeler

- Veri aktarımı, şirket içi ve şirket dışı ağlar üzerinden gerçekleştirilmektedir.
- Harici ağlar kontrollü ve güvenli şekilde kullanılmaktadır.
- Donanımsal güvenlik önlemleri ile yetkisiz bilgi işlem sistemlerine bağlantı kurulması ve bu sistemlerden bağlantı sağlanması engellenmektedir.
- Veriler ve dosyalar, harici sunuculara şifrelenmiş veri aktarım katmanları (SSL ve TLS) kullanılarak aktarılmaktadır.

3.1.2 Taşınabilir Ortamlarda Saklamaya İlişkin Düzenlemeler

- Kural olarak, kişisel verilerin taşınabilir veri saklama ortamlarında tutulması öngörülmemektedir.
- Kişisel veriler yalnızca güvenli erişime sahip, tahsis edilmiş bilgisayarlar ve sunucular üzerinde saklanmakta ve muhafaza edilmektedir.
- Kural olarak, işyeri içerisinde kişisel/özel veri saklama cihazlarının kullanımı yasaktır.

3.1.3 Veri Saklama Ortamlarının İmhasına İlişkin Düzenlemeler

Veri saklama ortamları, veri koruma mevzuatına uygun şekilde imha edilmektedir.

3.2 Girdi Kontrolü / Veri Saklama Ortamı Kontrolü / Saklama Kontrolü

Veri işleme sistemlerinde kişisel verilerin kim tarafından, ne zaman ve hangi işlemle girildiğinin, değiştirildiğinin veya silindiğinin sonradan kontrol edilebilir ve tespit edilebilir olması sağlanmalıdır. Bu amaçla aşağıdaki tedbirler uygulanmaktadır:

- Veri girişine ilişkin sorumluluklar, vekâlet/yerine geçme düzenlemeleri dâhil olmak üzere yetkilendirme yoluyla belirlenmektedir.
- Tüm veri girişleri, değişiklikleri ve silme işlemleri kayıt altına alınarak işlemi yapan kişi, zaman ve değişiklik içeriğinin izlenebilirliği sağlanmaktadır.
- İlgili kullanıcı faaliyetleri (gönderen, zaman damgası ve değişiklik içeriği) kaydedilmektedir.
- Toplanan kayıtlar (loglar), log değerlendirme sistemleri aracılığıyla analiz edilmektedir.

4 Erişilebilirlik ve Dayanıklılık / Kurtarılabilirlik

Kişisel verilerin kazara yok edilmesi veya kaybolması riskine karşı korunması güvence altına alınmalıdır. Bu amaçla aşağıdaki tedbirler uygulanmaktadır:

4.1 Yedeklerin Oluşturulması ve Muhafazası

- Dosya ve veritabanlarının kontrollü ve düzenli olarak yedeklenmesi sağlanmaktadır.
- Veri yedeklerinin test edilmesi düzenli aralıklarla gerçekleştirilmektedir.
- Veri yedekleri, yetkisiz erişime karşı korunmaktadır.
- Yedekleme diskleri, asıl verilerden ayrı ve güvenli ortamlarda muhafaza edilmektedir.

4.2 Günlük Operasyonların Güvence Altına Alınması

4.2.1 Dayanıklılık

- Yerel bilgisayarlardaki verilerin geri yüklenmesi şirket bünyesinde gerçekleştirilirken, uzak sunuculardaki verilerin geri yüklenmesi hizmet sağlayıcı tarafından yürütülmektedir.
- Paralel hesaplama, sunucu kümeleme ve birden fazla fiziksel sunucu üzerinde yedekli iş yüklerini destekleyici önlemler hizmet sağlayıcı tarafından sağlanmaktadır.

4.2.2 Kesintisiz Güç Kaynağı

- Sunucular için, üçüncü taraf hizmet sağlayıcı tarafından yeterli kapasiteye sahip kesintisiz güç kaynağı (UPS) kurulmuştur.
- UPS sistemlerinin düzgün çalışması, hizmet sağlayıcı tarafından düzenli testler aracılığıyla güvence altına alınmaktadır.

4.2.3 İklimlendirme

- Sunucuların bulunduğu alanda, hizmet sağlayıcı tarafından sağlanan yedekli iklimlendirme (klima) sistemleri bulunmaktadır.
- Ortam sıcaklığı izleme bilgileri hizmet sağlayıcı tarafından iletilmektedir.

4.2.4 İnternet Bağlantısı

Yedekli internet bağlantısı mevcuttur.

4.3 Organizasyonel Tedbirler

- Süreç ve program dokümantasyonuna ilişkin gereklilikler belirlenmiştir.
- Kullanılan donanım ve yazılımlar, hem şirket bünyesinde hem de hizmet sağlayıcı tarafından, yedekleme cihazları aracılığıyla kopyalardan orijinal verilerin yeniden üretilebilmesini sağlayacak şekilde hazır ve çalışır durumdadır.
- Operasyonel erişilebilirlik, hem şirket bünyesinde hem de hizmet sağlayıcı tarafından düzenli olarak kontrol edilmektedir.

- Hem şirket bünyesinde hem de hizmet sağlayıcı nezdinde yeterli personel kaynakları bulunmaktadır.

5 Düzenli İzleme, Değerlendirme ve Denetim Prosedürü

Uygulanan tedbirlerin etkinliği, özellikle organizasyonel düzeyde olmak üzere, iç süreçler ve prosedürler aracılığıyla düzenli olarak gözden geçirilmeli, değerlendirilmelidir.

5.1 Veri Koruma Yönetimi

İlgili mevzuatın ve düzenlemelerin getirdiği kapsamlı yükümlülükler, yapılandırılmış bir yaklaşım ve uygun bir yönetim sistemi temelinde oluşturulmuş bütüncül bir stratejiyi gerekli kılmaktadır. Veri korumanın sağlanması için gerekli tüm bileşenler, veri koruma yönetimi kapsamında sistematik olarak koordine edilmektedir. Bu kapsamda aşağıdaki tedbirler uygulanmaktadır:

- Veri koruma organizasyonu oluşturulmuştur.
- Veri koruma stratejisi doğrultusunda yapılandırılmış bir yaklaşım benimsenmektedir.
- Gizlilik politikaları ve operasyonel prosedürler ilan edilmiş olup, uyum düzenli olarak izlenmektedir.
- Yeni veri işleme süreçleri ve mevcut süreçlerde yapılacak önemli değişiklikler için resmî onay prosedürleri oluşturulmuştur.

5.2 Olay Müdahale Yönetimi

Gerekli hallerde olaylara müdahale edilebilmesi için ilgili bildirim kanallarının tanımlanması ve sorumlulukların belirlenmesi gerekmektedir. Bu amaçla aşağıdaki tedbirler uygulanmaktadır:

- Yöneticilere bu konuda gerekli eğitimler verilmiştir.
- Olaylara ilişkin bildirim noktaları ve kanalları tanımlanmıştır.
- Sistematik ve organize bir yaklaşım benimsenmiştir.
- Elde edilen deneyimler, süreçlerin geliştirilmesi ve iyileştirilmesi amacıyla kullanılmaktadır.

5.3 Tasarım Yoluyla ve Varsayılan Olarak Veri Koruma

Varsayılan ayarlar, kişisel verilerin yalnızca belirlenen işleme amacı doğrultusunda işlenmesini güvence altına almaktadır. Bu durum; toplanan kişisel veri miktarı, işleme kapsamı, saklama süresi ve erişilebilirlik açısından geçerlidir. Bu kapsamda aşağıdaki tedbirler uygulanmaktadır:

- Veri koruma yönetimi kapsamında sürdürülen farkındalık ve eğitim faaliyetleri sayesinde, yöneticiler kişisel verilerin işlenmesinde dikkatli davranmakta ve veri minimizasyonu ilkesini teknik ve iş süreçlerinin geliştirilmesinin ayrılmaz bir parçası olarak kabul etmektedir.

5.4 Talimatlara Uygunluk Kontrolü

Yetkilendirilmiş (emanet/taşeron) kişisel veri işleme faaliyetlerinin yalnızca veri sorumlusunun talimatları doğrultusunda gerçekleştirilmesi sağlanmalıdır. Veri sorumlusunun uygun talimatı olmaksızın kişisel veri işleme faaliyeti yürütülmez. Bu amaçla aşağıdaki tedbirler uygulanmaktadır:

- Yetkilendirilmiş kişisel veri işleme faaliyetlerine ilişkin gerekli sözleşmelerin tamamlanmasını sağlayan iç süreçler oluşturulmuştur.

- Veri sorumlusu ile veri işleyen arasında her durumda yazılı bir sözleşme bulunmaktadır.
- Veri sorumlusu, veri işleyene yazılı talimatlar vermektedir.
- Veri işleyen, verilen yetki ve veri sorumlusunun ilgili talimatları doğrultusunda yeterli iç düzenlemeleri sağlamıştır.
- Olası alt veri işleyenlerin veri koruma yükümlülüklerine uyumunu sağlayacak yeterli tedbirlerin alınması, veri sorumlusu tarafından kontrol edilebilmektedir.
- Yetkili denetim otoritesi tarafından veri işleyen nezdinde bir denetim gerçekleştirilmiş olması halinde, veri sorumlusu denetim raporunu talep edebilir; aynı husus olası alt veri işleyenler için de geçerlidir.

EK – Denetçiler için Teknik ve Organizasyonel Tedbirler Kontrol Listesi

A. Genel Veri Koruma Yönetimi

Kontrol Noktası	Uygun	Kısmen	Uygun Değil	N/A
Veri koruma organizasyonu tanımlanmış mı?	☐	☐	☐	☐
KVKK / GDPR uyum stratejisi mevcut mu?	☐	☐	☐	☐
Politika ve prosedürler yazılı ve güncel mi?	☐	☐	☐	☐
Çalışanlara veri koruma farkındalık eğitimi veriliyor mu?	☐	☐	☐	☐
Yeni veya değişen veri işleme süreçleri için onay mekanizması var mı?	☐	☐	☐	☐

B. Gizlilik – Fiziksel Güvenlik

Kontrol Noktası	Uygun	Kısmen	Uygun Değil	N/A
Bina ve ofis girişleri kontrollü mü?	☐	☐	☐	☐
Yetkisiz kişilerin erişimi engelleniyor mu?	☐	☐	☐	☐
Ziyaretçi giriş-çıkışları kayıt altına alınıyor mu?	☐	☐	☐	☐
Otopark ve bina çevresi güvenlik altında mı?	☐	☐	☐	☐

C. Veri İşleme Sistemlerine Erişim

Kontrol Noktası	Uygun	Kısmen	Uygun Değil	N/A
Rol bazlı yetkilendirme uygulanıyor mu?	☐	☐	☐	☐
Parola politikası mevcut mu?	☐	☐	☐	☐
Oturum kilitleme kullanılıyor mu?	☐	☐	☐	☐
Uzaktan erişim SSL/TLS ile güvenli mi?	☐	☐	☐	☐

D. Bütünlük

Kontrol Noktası	Uygun	Kısmen	Uygun Değil	N/A
Veri giriş, değişiklik ve silme işlemleri loglanıyor mu?	☐	☐	☐	☐
Log kayıtları düzenli analiz ediliyor mu?	☐	☐	☐	☐
Veri transferleri şifreli mi?	☐	☐	☐	☐
Veri imha süreçleri tanımlı mı?	☐	☐	☐	☐

E. Erişilebilirlik ve Dayanıklılık

Kontrol Noktası	Uygun	Kısmen	Uygun Değil	N/A
Düzenli veri yedekleme yapılıyor mu?	☐	☐	☐	☐
Yedekler güvenli ortamda mı?	☐	☐	☐	☐
Yedek geri yükleme testleri yapılıyor mu?	☐	☐	☐	☐
UPS ve internet yedekliliği mevcut mu?	☐	☐	☐	☐

F. Veri İşleyen / Taşeron Kontrolü

Kontrol Noktası	Uygun	Kısmen	Uygun Değil	N/A
Veri işleyenlerle yazılı sözleşme mevcut mu?	☐	☐	☐	☐
Yazılı talimatlar ile veri işleme yapılıyor mu?	☐	☐	☐	☐
Alt veri işleyenler denetleniyor mu?	☐	☐	☐	☐

G. Denetçi Notları

……...

……...

……...

……...