VERİ İHLALİ MÜDAHALE PLANI

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

Madde 1 – Bu Planın amacı, **Çanakkale Otoyol ve Köprüsü İnşaat Yatırım ve İşletme A.Ş. ("ÇOK A.Ş.")** olarak kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüklerini yerine getirmek amacıyla işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu sıfatıyla ÇOK A.Ş. tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konulara ilişkin rolleri ve sorumlulukları tanımlamak, usul ve esasları düzenlemektir.

Kapsam

Madde 2 – Bu Planın kapsamı, ÇOK A.Ş. tarafından fiziki veya elektronik ortamda işlenen kişisel verilerin işlenmesinde görevli çalışanları içermektedir.

Tanımlar

Madde 3 – Bu Planın uygulanmasında;

a) **Açık rıza:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

b) **İlgili kişi:** Kişisel verisi işlenen gerçek kişiyi,

c) **Kanun:** 6698 sayılı Kişisel Verilerin Korunması Kanununu,

d) **Kişisel veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

e) **Kişisel verilerin işlenmesi:** Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

f) **Kurul:** Kişisel Verileri Koruma Kurulunu,

g) **Plan:** ÇOK A.Ş. Veri ihlali müdahale planını,

h) **Veri İhlali:** Veri sorumlusu tarafından işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesini,

i) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

j) Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

k) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ifade eder.

İKİNCİ BÖLÜM

Veri İhlali

Veri İhlali

Madde 4 – Kanunun 12'nci maddesinin 5'inci fıkrası gereğince, ÇOK A.Ş. tarafından işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesidir.

Yukarıdaki tanıma ilaveten; iletilen, saklanan veya işlenen kişisel verilerin kazara yasadışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması ve/veya bunlara erişime yol açan bir güvenlik ihlalinin meydana gelmesi de yine Plan kapsamında Veri İhlali olarak nitelendirilecektir.

ÜÇÜNCÜ BÖLÜM

Hedefler, Görevliler ve Sorumluluklar

Hedefler

Madde 5 – Bir Veri İhlali yaşanması durumunda, ÇOK A.Ş.'nin Plan çerçevesinde hedefleri:

1. Veri İhlaline sebep olan olayı dahili olarak tüm ilgili departmanlar nezdinde araştırmak (gerektiği hallerde kolluk kuvvetleri ve diğer kamu kurum ve kuruluşları ile iş birliği içerisinde),
2. Veri İhlalinin kaynağını tespit etmek,
3. Veri İhlalinden etkilenen kişisel veri kategorilerini tespit etmek,
4. Veri İhlalinden etkilenen kişi gruplarını/tarafları tespit etmek,
5. Veri İhlalinden etkilenen tarafların mevcutta uğradıkları ve uğramaları muhtemel potansiyel etkileri tespit etmek ve varsa bu etkilerden doğan zararların en asgariye indirilmesini sağlamak,
6. Veri İhlali neticesinde ÇOK A.Ş.'nin organizasyonuna olan etkilerinin, ticari kaybın, operasyonlardaki azalmanın, itibarî kayıpların ve/veya finansal zararların boyutlarını tespit etmek ve hukuka uygun bir şekilde en asgariye indirilmesini sağlamak,
7. Veri İhlali sonrasındaki iyileşmenin zamanını tespit etmek,
8. Eğer siber saldırı varsa;

a. Bilgi sistemlerinin siber saldırıdan etkilenip etkilenmediğini,

b. Siber saldırı var ise saldırı sonucu gerçekleşen ihlal unsurunu,

c. Siber saldırının ÇOK A.Ş.'nin organizasyonuna olan etkilerini, ve

d. Siber saldırı sonrasındaki iyileşmenin zamanını tespit etmek,

9. İhlalin tekrarlanmaması için atılan adımları belirlemek ve bunların tahminen ne kadar zamanda tamamlanacağını hesaplamak,

10. Veri İhlaline sebep olan olayı veya olay sonucu ortaya çıkan kaybı,

    a. Kanuna uygun şekilde Kurula 72 saat içerisinde,

    b. Veri İhlalinden etkilenen ilgili kişilere en kısa sürede uygun yöntemlerle,

    c. Çalışanlara en kısa sürede,

    d. Eğer gerekiyorsa yurtiçinde bulunan diğer organizasyon veya kurumlara ilgili yasal yükümlülüklere uygun sürede,

11. Yurtdışında bulunan diğer veri koruma otoriteleri veya ilgili kurumlara ilgili yasal yükümlülüklere uygun sürede, bildirmek,

12. Gelecekte meydana gelmesi ihtimaline karşı olası Veri İhlallerinin en aza indirilmesi için Veri İhlaline yol açan olay sonrası iç denetimi tertiplemek, eğitim faaliyetleri düzenlemek ve iç iletişimi sağlamak; ve

13. Veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurmaktır.

Görevliler ve Sorumluluklar

Madde 6 – Veri İhlali yaşanması halinde bu Plan gereğince ÇOK A.Ş. bünyesinde görevli departmanlar, Veri İhlaline neden olan olayın niteliğine göre belirlenir; ancak her koşulda aşağıdaki tabloda yazan departmanlardan her birinden en az bir temsilci görevlendirilecektir. Temsilcilerin sorumluluklarına da aynı tabloda belirtilmiştir.

Görevli Departman	**Veri İhlali Halinde Sorumlulukları**
Danışman	1. Veri İhlaline sebep olan olayı dahili olarak tüm ilgili departmanlar nezdinde (gerektiği hallerde kolluk kuvvetleri ve diğer kamu kurum ve kuruluşları ile iş birliği içerisinde) araştırmak. 2. Veri İhlalinin kaynağını tespit etmek.

	3. Veri İhlalinden etkilenen kişisel veri kategorilerini tespit etmek. 4. Veri İhlalinden etkilenen kişi gruplarını/tarafları tespit etmek. 5. Veri İhlalinden etkilenen tarafların mevcutta uğradıkları ve uğramaları muhtemel potansiyel etkileri tespit etmek ve varsa bu etkilerden doğan zararların en asgariye indirilmesini sağlamak. 6. Veri İhlali neticesinde ÇOK A.Ş.'nin organizasyonuna olan etkilerinin, ticari kaybın, operasyonlardaki azalmanın, itibarî kayıpların ve/veya finansal zararların boyutlarını tespit etmek ve hukuka uygun bir şekilde en asgariye indirilmesini sağlamak. 7. Veri İhlali sonrasındaki iyileşmenin zamanını tespit etmek. 8. İhlalin tekrarlanmaması için atılan adımları belirlemek ve bunların tahminen ne kadar zamanda tamamlanacağını hesaplamak. 9. Veri İhlaline sebep olan olayı veya olay sonucu ortaya çıkan kaybı, Kanuna uygun şekilde Kurula 72 saat içerisinde bildirmek. 10. Yurt dışında bulunan diğer veri koruma otoriteleri veya ilgili kurumlara ilgili yasal yükümlülüklere uygun sürede, bildirmek. 11. Veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurmak. 12. Gelecekte meydana gelmesi ihtimaline karşı olası Veri İhlallerinin en aza indirilmesi için Veri İhlaline yol açan olay sonrası iç denetimi tertiplemek, eğitim faaliyetleri düzenlenmesini ve iç iletişimi sağlamak. 13. Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyenin bu konuda herhangi bir gecikmeye yer vermeksizin veri sorumlusuna bildirimde bulunması durumunda yine Kurula gerekli bildirimin yapılmasını sağlamak. 14. Planın, yürürlük tarihinden itibaren her 6 (altı) ayda bir gözden geçirilmesini sağlamak.

Bilgi Teknolojileri	Veri ihlalinin siber saldırı veya diğer başka bir elektronik yolla gerçekleşmesi halinde; 1. Bilgi sistemlerinin Veri İhlalinden etkilenip etkilenmediğini tespit etmek. 2. Veri İhlali sonucu gerçekleşen ihlal unsurunu tespit etmek. 3. Veri İhlalinin ÇOK A.Ş.'nin organizasyonuna olan etkilerini tespit etmek. 4. Veri İhlali sonrasındaki iyileşmenin zamanını tespit etmek.
İnsan Kaynakları	1. Veri ihlalinin ÇOK A.Ş. çalışanı tarafından gerçekleştirilip gerçekleştirilmediğini tespit etmek. 2. ÇOK A.Ş. çalışanlarının Veri İhlalinden etkilenip etkilenmediğini tespit etmek. 3. Veri İhlali sonucu gerçekleşen ihlal unsurunu, Veri İhlalinin ÇOK A.Ş.'nin organizasyonuna olan etkilerini ve Veri İhlali sonrasındaki iyileşmenin zamanını tespit etmek. 4. Veri İhlaline yol açan olay sonrası eğitim faaliyetleri hazırlamak ve iç iletişimi gerçekleştirmek. 5. Veri İhlaline sebep olan olayı veya olay sonucu ortaya çıkan kaybı çalışanlara en kısa sürede bildirmek.
Hukuk Departmanı	1. Veri İhlaline yol açan olay sonrası iç denetimi gerçekleştirmek. 2. Veri İhlaline sebep olan olayı veya olay sonucu ortaya çıkan kaybı, Veri İhlalinden etkilenen ilgili kişilere en kısa sürede uygun yöntemlerle bildirmek. 3. Eğer gerekiyorsa yurtiçinde bulunan diğer organizasyon veya kurumlara ilgili yasal yükümlülüklere uygun sürede bildirmek.

Tablo 1: Veri İhlali Müdahale Planı Kapmasında Görevliler ve Sorumlulukları

DÖRDÜNCÜ BÖLÜM

Bildirim

Veri Sorumlusu Tarafından Bildirim

Madde 7 – Veri İhlal bildirimleri, ihlalden etkilenen kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkân verecek önlemler alınmasını sağlamak amacıyla Kurula ve ihlalden etkilenmiş kişilere yapılmalıdır. Buna ilişkin Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararı doğrultusunda hazırlanan işbu Plan gereğince ÇOK A.Ş.'nin;

1. Veri İhlalini öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesi,

2. Söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapması,

3. Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanması,

4. Kurula yapılacak bildirimde ekte yer alan "EK-1 Kişisel Veri İhlal Bildirim Formu"nun kullanılması,

5. Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgilerin gecikmeye mahal verilmeksizin aşamalı olarak sağlanması, ve

6. Veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulması gerekmektedir.

ÇOK A.Ş. bildirime ilişkin yukarıda sayılı tüm işlemleri işbu Planın 5'inci maddesinde belirtilen ve aynı madde içerisindeki tabloda detaylı şekilde verilen birimlerince yürütür.

Veri İşleyen Tarafından Bildirim

Madde 8 – Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyenin bu konuda herhangi bir gecikmeye yer vermeksizin veri sorumlusu olan ÇOK A.Ş.'ye bildirimde bulunması gerekmektedir. Veri işleyenin bildirimini müteakip ÇOK A.Ş. tarafından, Planın 6'ncı maddesindeki süreç izlenerek Kurula bildirim yapılacaktır.

Yurt Dışı Veri İhlali

Madde 9 – Veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de faydalanmaları durumunda, bu veri sorumlusu tarafından da Planın 6'ncı maddesinde belirtilen esaslar çerçevesinde Kurula bildirimde bulunulacaktır.

BEŞİNCİ BÖLÜM

Çeşitli Hükümler

Yürürlük

Madde 10 – Şirket tarafından hazırlanan bu Plan ÇOK A.Ş.'ye ait internet sitesinde yayınlandığı tarih itibariyle yürürlüğe girmiştir.

Planın Gözden Geçirilmesi

Madde 11 – Hazırlanan ve yürürlüğe konulan bu Plan, her 6 (altı) ayda bir periyodik olarak gözden geçirilir.

GÜNCELLEME TABLOSU

Bu Plan'da yapılan değişiklikler aşağıdaki tabloda yer almaktadır.

GÜNCELLEME TARİHİ/VERSİYON	**GÜNCELLEMELERİN KAPSAMI**
20.01.2020	Plan yayın tarihi