

ULAŖTIRMA VE ALTYAPI
BAKANLIĐI
KİŖİSEL VERİ İHLAL YÖNETİM
SÜRECİ POLİTİKASI DOKÜMANI



[Handwritten signature]

[Handwritten signature]

1

[Handwritten signature] *[Handwritten signature]* *[Handwritten signature]*

ULAŖTIRMA VE ALTYAPI BAKANLIĐI KİŖİSEL VERİ İHLAL YÖNETİM SÜRECİ
POLİTİKASI DOKÜMANI BİLGİ FORMU

Doküman İsmi : UlaŖtırma ve Altyapı Bakanlığı KiŖisel Veri İhlal Yönetim Süreci Politikası
Dokümanı

Hedef Kitle : UlaŖtırma ve Altyapı Bakanlığı Merkez ve TaŖra TeŖkilatı personeli,
ziyaretçiler, stajyer öĐrenciler ile verisi işlenen tüm gerçek kiŖiler

Hazırlayan : Strateji GeliŖtirme Başkanlığı

Onaylayan : UlaŖtırma ve Altyapı Bakanlığı 6698 Sayılı Kanun (KiŖisel Verilerin
Korunması Kanunu) Uygulama Kurulu tarafından onaylanmıŖtır.



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

İçindekiler

1.BÖLÜM.....	4
1.1.Giriş.....	4
1.2.Amaç.....	4
1.3.Kapsam	4
1.4.Tanımlar	4
1.5.Politika'nın Yayımlanması, Güncellenmesi ve Saklanması.....	4
1.6.Politika'nın Yürürlüğü	5
2. BÖLÜM.....	5
2.1.Kişisel Verilerin Korunmasına İlişkin Hususlar	5
2.2.Kişisel Verilerin Güvenliğinin Sağlanması	5
2.2.1.Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak ve Kişisel Verilere Hukuka Aykırı Erişilmesini Önlemek İçin Alınan İdari Tedbirler	5
2.2.2.Verilerin Hukuka Uygun İşlenmesini Sağlamak ve Kişisel Verilere Hukuka Aykırı Erişilmesini Önlemek İçin Alınan Teknik Tedbirler	6
2.3.Özel Nitelikli Kişisel Verilerin Güvenliğinin Sağlanması	7
2.4.Birimlerin Kişisel Verilerin Korunması ve İşlenmesi Konusunda Farkındalıklarının Arttırılması	7
3.BÖLÜM.....	7
3.1.Sorumluluk.....	7
3.2.Verİ İhlalinin Kurula Bildirilmesi.....	7
3.3.Verİ İhlalinin İlgili Kişİye Bildirilmesi	8
3.4.Verİ Güvenliğı Olayları Yönetimi	8



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

1.BÖLÜM

1.1.Giriş

Ulaştırma ve Altyapı Bakanlığı (Bakanlık) olarak, kişisel verilerin korunmasıyla ilgili Anayasa'nın 20'nci maddesi ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) öncelikli olmak üzere yürürlükte bulunan ilgili mevzuata uyumlu davranmak için azami gayret gösterilmektedir. Tüm planlama ve faaliyetlerimizde de aynı öncelik ve hassasiyetle hareket edilmektedir.

1.2.Amaç

İşbu Politika ile kişisel verilerin korunması, güvenliğinin sağlanması, Kanunun 12'nci maddesinin 5'inci fıkrası kapsamında veri sorumlusu sıfatına haiz Bakanlığın merkez veya taşra teşkilatlarında veri ihlali yaşanması durumunda uygulanacak bütün idari ve teknik tedbirler ile ihlal durumunun Kişisel Verileri Koruma Kurulu (Kurul) ile kişisel verisi ihlal edilen ilgili kişiye bildirimine dair Bakanlık içinde izlenmesi gereken politikayı belirlemek amaçlanmaktadır.

1.3.Kapsam

İşbu Politika, Bakanlık tarafından, kişilerin otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen tüm kişisel verilerini, Kanun kapsamındaki bütün kişisel veri işleme faaliyetlerini ve bu verilerin sahiplerini kapsamaktadır.

Kanun ve ilgili mevzuat uyarınca, Kurula ve verisi ihlal edilen ilgili kişiye yapılması gereken bildirimlere ilişkin uygulanacak iş ve işlemler Politika kapsamında olup herhangi bir ihlal halinde bu Politikada açıklanan bildirim süreci uygulama alanı bulur.

1.4.Tanımlar

- (1) Bu Politika'da geçen;
- a) Belgenet: Kurumsal belgelerin yasal mevzuat ve standartlara uygun şekilde elektronik ortamda güvenli ve etkin olarak yönetilmesini sağlayan Web tabanlı "Elektronik Belge Yönetim Sistemi" yazılımını,
 - b) Form: Kişisel Verileri Koruma Kurulunun 24/01/2019 tarihli 2019/10 sayılı kararı ile yayınlanan "Kişisel Veri İhlali Bildirim Formu"nu,
 - c) Kurul: Kişisel Verileri Koruma Kurulunu,
 - ç) Kurum: Kişisel Verileri Koruma Kurumunu,
 - d) Politika: Kişisel Veri İhlal Yönetim Süreci Politikası Dokümanını,
 - e) Potansiyel veri ihlali: Bakanlık bünyesinde potansiyel olarak veri ihlali riski yaratan durumu,
 - f) Yönerge: Ulaştırma ve Altyapı Bakanlığı 6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Dair Yönergeyi,
- ifade eder.
- (2) Politika ve süreçlerde yer almayan tanımlar için Kanun ve Yönerge'de sayılan tanımlar geçerlidir.

1.5.Politika'nın Yayımlanması, Güncellenmesi ve Saklanması

İşbu Politika, Ulaştırma ve Altyapı Bakanlığı 6698 Sayılı Kanun Uygulama Kurulunca ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır. Basılı kâğıt nüshası KVKK koordinasyon biriminde muhafaza edilir. Kanunun tamamının veya



belirli maddelerinin yenilenmesi ile gerek duyulması halinde Ulaştırma ve Altyapı Bakanlığı 6698 Sayılı Kanun Uygulama Kurulunca işbu politikada değişiklik yapılır. Politika, Bakanlığın internet sitesinde (www.uab.gov.tr/kvkk) yayımlanır ve ilgili kişilerin erişimine sunulur.

1.6.Politika'nın Yürürlüğü

Ulaştırma ve Altyapı Bakanlığı 6698 sayılı Kanun Uygulama Kurulunca onaylanması ve Bakanlığın internet sitesinde yayımlanmasını müteakip işbu Politikanın yürürlüğe girdiği kabul edilir.

2. BÖLÜM

2.1.Kişisel Verilerin Korunmasına İlişkin Hususlar

Bakanlık tarafından, kişisel verilerin hukuka aykırı olarak açıklanmasını, erişimini, aktarılmasını veya başka şekillerde meydana gelebilecek güvenlik eksikliklerini önlemek için, korunacak verinin niteliğine göre gerekli her türlü idari ve teknik tedbirler alınmaktadır.

Bu kapsamda, Bakanlık bünyesinde denetim sistemi kurulmakta ve kişisel verilerin kanuni olmayan yollarla ifşası durumunda Kanunda öngörülen tedbirlere uygun olarak hareket edilmektedir.

2.2.Kişisel Verilerin Güvenliğinin Sağlanması

2.2.1.Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak ve Kişisel Verilere Hukuka Aykırı Erişilmesini Önlemek İçin Alınan İdari Tedbirler

– Bakanlık, kişisel verilerin işlenmesi ve korunmasına ilişkin olarak personele gerekli hizmet içi eğitimleri vermekte ve bilinçlendirilmelerini sağlamaktadır.

– Personel için yetki matrisi oluşturulmuş olup belli aralıklarla güncellenmektedir. Kullanıcı sadece yetkilendirildiği uygulama ve kaynaklara erişebilmektedir. Uygulamaya yapılan her istek için yetki denetimi kontrolü yapılmaktadır.

– Görev değişikliği olan ya da işten ayrılan personelin ve veri işleyenlerin bu alandaki yetkileri kaldırılmaktadır.

– Birimler içinde dairelere ait özel alanlar ve arşiv odalarına giriş ve çıkışları sınırlandırılarak kontrollü giriş ve çıkış sağlanmaktadır.

– Bakanlık içerisindeki yazışmalar, Belgenet üzerinden ve personelin adına açılmış olan mail yoluyla sağlanmaktadır.

– Kişisel veri güvenliğinin takibi yapılarak sorunların hızlı bir şekilde raporlanması yapılmaktadır.

– Kişisel veri içeren fiziksel alanların ve ortamların dış risklere (yangın, sel, vb.) karşı güvenliği sağlanmaktadır.

– Bakanlık yerleşkelerinin büyüklüğü ve bulunduğu coğrafi alanı ile orantılı olarak güvenlik personeli görevlendirilmekte, teknik güvenlik önlemleri (kamera izleme vb.) alınmakta ve güvenlik personelinin görevini yerine getirip getirmediği düzenli olarak kontrol edilmektedir.

– Birimlerde bilgisayarlar kullanılmadığında otomatik veya manuel olarak oturum kapalı hale getirilmektedir.

– Bakanlığın kayıtlı olduğu VERBİS sisteminin güncelliği sağlanmaktadır.



– Kişisel verilerin aktarımına konu olduğu durumlarda, Bakanlık tarafından kişisel verilerin aktarıldığı kişiler ile akdedilmiş olan sözleşmelere, kişisel verilerin aktarıldığı tarafın veri güvenliğini sağlamaya yönelik yükümlülükleri yerine getireceğine ilişkin hükümlerin eklenmesi temin edilmektedir.

– Yürütülen kişisel veri işleme faaliyetleri detaylı olarak incelenmekte, bu kapsamda, Kanunda öngörülen kişisel veri işleme şartlarına uygunluğun sağlanması için atılması gereken adımlar tespit edilmektedir.

– Bakanlık, Kanuna uyumun sağlanması için yerine getirilmesi gereken uygulamaları tespit ederek, bu uygulamaları iç politikalar ile düzenlemektedir.

2.2.2.Verilerin Hukuka Uygun İşlenmesini Sağlamak ve Kişisel Verilere Hukuka Aykırı Erişilmesini Önlemek İçin Alınan Teknik Tedbirler

– Kişisel verilerin işlenmesine ve korunmasına ilişkin olarak, teknolojinin imkân verdiği ölçüde teknik önlemler alınmakta ve alınan önlemler gelişmelere paralel olarak güncellenmekte ve iyileştirilmektedir.

– Teknik konularda, uzman personel istihdam edilmektedir.

– Güncel Anti Virüs programları kullanılmaktadır.

– Güvenlik duvarı kullanılmaktadır.

– Güvenlik ve zafiyet testleri belli aralıklarla yapılmaktadır.

– Log Kayıtları tutulmaktadır.

– Alınan önlemlerin uygulanmasına yönelik düzenli aralıklarla kontroller yapılmaktadır.

– Verilerin muhafaza edildiği sistemleri, sunucuları ve veri tabanlarını, veri güvenliği tehditlerine (siber saldırı, hash vb.) karşı korumak ve güvenliğini temin etmek için gerekli yazılım ve sistemler kurulmaktadır.

– Bilgiler, ancak iş sürecinin devamı, verilerin toplanma amacının gerektirdiği süre, mevzuatta özel süre öngörülüyor ise bu süreye uygun ve yasal zorunluluklar için gerekli oldukları sürece saklanmaktadır.

– Bakanlık bünyesinde işlenmekte olan kişisel verilere erişim yetkisi, belirlenen işleme amacı doğrultusunda ilgili personel veya veri işleyenler ile sınırlandırılmaktadır.

– Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta, bunların takibi de yapılmaktadır.

– Kullanılmayan hesaplar tespit edilmekte, belli bir süre boyunca hiç kullanılmamış olan hesaplar raporlanıp pasif duruma getirilmekte veya silinmektedir.

– Kullanıcı hesapları geçici olarak kilitlenebilmektedir.

– Kullanıcı parolalarının belli periyotlarda değiştirilmesine yönelik tedbirler alınmaktadır.

Her bir kullanıcı kendisinin belirleyebileceği bir parolaya sahiptir. “Kullanıcı adı” Bakanlık tarafından belirlenir, aynı kullanıcı adı iki farklı kişiye verilmez ve kişiye özeldir. “Parola” sadece kullanıcı tarafından bilinir. Kullanıcı parolasını değiştirme süresini beklemeden dilediği zaman değiştirebilir. Parola seçimi belli kriterlere göre karmaşıklık ister. Parola kullanılmasından doğacak problemler (güvenliği, saklanması, üçüncü kişilerin bilgisinden uzak tutulması vb.) kullanıcının sorumluluğundadır.

– Personelin veya gelen ziyaretçilerin Bakanlık ve birimlere giriş/çıkışları kayıt altına alınmaktadır.



2.3.Özel Nitelikli Kişisel Verilerin Güvenliğinin Sağlanması

Hassasiyet arz eden kişisel verilere, hukuka aykırı olarak işlendiğinde kişilerin mağduriyetine veya ayrımcılığa sebep olma riski nedeniyle Kanun kapsamında özel önem atfedilmiştir. Bu kapsamda, Bakanlık tarafından, kişisel verilerin korunması için alınan teknik ve idari tedbirler, özel nitelikli kişisel verilerin korunmasında Kanun ve ilgili diğer mevzuat hükümlerinde yer alan önlemler özenle uygulanmaktadır.

2.4.Birimlerin Kişisel Verilerin Korunması ve İşlenmesi Konusunda Farkındalıklarının Arttırılması

Bakanlık, kişisel verilerin hukuka aykırı olarak işlenmesini, verilere hukuka aykırı olarak erişilmesini önlemeye ve verilerin muhafazasını sağlamaya yönelik farkındalığın artırılması için birimlerine gerekli eğitimlerin düzenlenmesini sağlamaktadır.

Bakanlık, mevcut personeline ve bünyesine yeni dâhil olan personele kişisel verilerin korunması konusunda farkındalığın oluşması için gerekli eğitim ve bilgilendirme oturumları yapmakta, ilgili mevzuatın güncellenmesine paralel olarak yeni eğitimler düzenlemektedir.

3.BÖLÜM

3.1.Sorumluluk

– Bakanlık birimlerinde kişisel verileri işleyen ve verilere erişen ilgili kullanıcı; Bakanlık bünyesinde bir veri ihlali veya potansiyel veri ihlali olduğunda yapılacak bildirimler açısından, kanun, ilgili mevzuat hükümleri, işbu Politika ve birim yetkilisi tarafından verilecek talimatlara uymak zorundadır.

– Bakanlık nezdinde veri ihlali veya potansiyel veri ihlali meydana geldiğinin tespiti halinde, veri ihlali veya potansiyel veri ihlali meydana gelen birimin birim amiri, en kısa sürede engelleyici önlemleri alarak, veri ihlalinin derhal irtibat kişisine ve KVKK koordinasyon birimine bildirir.

– Potansiyel bir veri ihlali durumu mevcut ise, bu durumun veri ihlali olup olmadığı konusunda tespite yetkili organ Çalışma Ekibidir.

– Çalışma Ekibi olayların tespitinden sonra ihlalin araştırılması gündemiyle (delil toplama, önlem alma ve deneyim edinme konularında) çalışma gerçekleştirebilir.

– Çalışma Ekibi tekrar edebilecek ihlal olaylarını engellemek veya gerçekleşmesi durumunda müdahale edebilmek için ihlal olayları ile ilgili oluşturulan kayıtları inceler ve düzeltici ve önleyici faaliyet kapsamında tavsiyelerde bulunur.

– İhlal olayları ile ilgili oluşturulan kayıtlar/raporlar/tutanaklar Ulaştırma ve Altyapı Bakanlığı 6698 Sayılı Kanun Uygulama Kurulu toplantılarında paylaşılır ve görüşülür.

3.2.Verİ İhlalinin Kurula Bildirilmesi

– Bakanlık birimlerinde veri ihlali meydana gelmesi durumunda ihlalin gerçekleştiği/tespit edilmesini müteakip, 72 (yetmiş iki) saat içerisinde Kurula bildirilir.

– Kurula yapılacak bildirimde Kişisel Veri İhlal Bildirim Formu kullanılır.

– Form, İrtibat Kişisi başkanlığında toplanacak Çalışma Ekibi tarafından; idari, hukuki, teknik ve bilişim yönünden değerlendirilerek düzenlenir. Formun, “Veri sorumlusu adına bu bildiriye hazırlayan kişi” bölümüne irtibat kişinin bilgileri yazılır.



– İhlalin Kurula bildirilmesi için yukarıda tayin edilen sürenin yeterli olmaması ve bu durumun haklı bir gerekçeye dayanması halinde, yapılacak geç bildirimde “gecikmenin gerekçesi” de Kurula açıklanır.

– Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı durumlarda, bu bilgilerin gecikmeye mahal vermeyecek şekilde aşamalı olarak tamamlanarak gönderilmesi sağlanır.

– Çalışma Ekibi ihlale sebebiyet veren birim ile koordineli halde çalışılır. Veri ihlallerine ilişkin bilgiler, ihlalin etkileri ve ihlale karşı alınan önlemler kayıt altına alınır ve Kurulun incelemesine hazır halde bulundurulur.

– Veri aşağıda yer alan yollardan biriyle Kurula bildirilir.

- E-posta ile Bildirim: Bildirimin ilk bildirim olması halinde doldurulan form ihlalbildirimi@kvkk.gov.tr adresine “Kişisel Veri İhlali Bildirimi” konulu bir e-posta eki ile gönderilir. Eğer yapılacak bildirim bir takip bildirimi ise, Form ilk bildirimde gönderilen e-postanın ekine eklenir.

- Posta ile Bildirim: Formun posta ile gönderilmesine karar verilirse, “Kişisel Verileri Koruma Kurumu Nasuh Akar Mahallesi Ziyabey Cad. 1407 Sok. No:4, 06520 Çankaya/Ankara” adresine APS ile gönderilir.

- Web Sayfası Üzerinden Bildirim: Bildirimin Kurumun web sayfası üzerinden yapılması istenirse, <https://ihlalbildirim.kvkk.gov.tr/> adresli web sayfasından “Bildirim Oluştur” bağlantısına girilerek çıkan sayfadaki adımların takip edilmesi suretiyle ve Kurumun www.kvkk.gov.tr adresli web sayfasında yayımlanan “Kişisel Veri İhlali Bildirim Formu Klavuzu”na uygun olarak bildirim yapılır.

3.3.Verİ İhlalinin İlgili Kişİye Bildirilmesi

– Veri ihlaline konu ilgili kişi belirlendikten sonra en geç 72 (yetmiş iki) saat içerisinde KVKK koordinasyon birimince veri ihlali ilgisine bildirilir.

– İlgili kişiye yapılacak bildirimlerde; ihlalin ne zaman gerçekleştiği, kişisel veri kategorileri bazında (kişisel veri/özel nitelikli kişisel veri ayrımı yapılarak) ilgili kişinin hangi verilerinin ihlale konu olduğu, kişisel veri ihlalinin gerçekleşen ve gerçekleşme potansiyeli olan sonuçları, veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen veri güvenliği tedbirlerinin neler olduğu, ilgili kişinin veri ihlali ile ilgili Bakanlıktan detaylı bilgi alabilmesi için gerekli iletişim bilgileri (isim, telefon numarası, web sayfası adresi vb.) yer alır.

– İlgili kişinin iletişim adresi mevcutsa iletişim adresine gönderilir, iletişim adresine ulaşılamıyorsa Bakanlık’ın web sitesi üzerinden yayınlanır.

3.4.Verİ GüvenliĐi Olayları Yönetimi

Birim amiri/yetkilisi veri güvenliği ile ilgili olarak biriminde aşağıda yer alan aksiyonları almakla yükümlüdür:

- Veri ihlal olayı tespiti sonrası olayla ilgili delilleri toplamak,
- Toplanan delilleri müdahale için sınıflandırmak,
- Müdahaleden önce kayıtları toplamak, kayıtların bozulmasını engellenecek şekilde saklamak ve yetkisiz erişime karşı korumak,

- Olayların önceliklendirilmesi için olayın etkisini, kapsamını ve sınıflandırılmasını belirlemek amacıyla verileri incelemek,



- Kontroller veya bildirilen durumlar ile tespit edilen ve delilleri toplanan tüm olaylar için diğer işlemlerden önce olaya sebep olan zafiyet düzeltilmesi için gerekli önlemleri almak,
- Zafiyetlerin kapatılmasından sonra mutlaka kontrolleri tekrarlamak ve zafiyetin kapandığını onaylamak,
- Delilleri tahrip edecek veya bozacak hiçbir açıklık için kapatma işlemi gerçekleştirmemek,
- Gelen ihlal olayları bildirimleri kapsamında en kısa sürede delil toplayarak müdahale etmek,
- Olaya müdahale konusunda yeterli yetkinlik bilgi ve beceriye sahip olmaması durumunda Bakanlık içi veya Bakanlık dışı ilgili personel ya da üçüncü tarafla iletişime geçmek,
- İhlal olayı için işlemlerden önce kanıtları toplamak,
- Risk oluşturan varlığı en kısa süre içerisinde zarar verebileceği ortamdan uzaklaştırmak veya ayırmak,
- Kontroller sonucunda tespit edilen olaylar için mutlaka belirli bir süre daha benzer kontrolleri tekrarlamak,
- Müdahale esnasında raporlama için gerekli zafiyet analizi, adli analiz, maliyet tespiti ve ihlal sebepleri gibi gerekli bilgileri kapsayacak detayda verileri toplamak,
- Tespit edilen her bir olay için tekrar oluşmasını engellemek için önlemler almak,
- Olayın tespiti ve sorumlunun belirleneceği kayıtların bütünlüğünü bozmamak ve kontrol etmek,
- Veri ihlal olayları için toplanan delillerin ihlal süreci sonlandırıldıktan sonra 10 (on) yıl boyunca saklanmasını sağlamak için gerekli tedbirleri almak.



[Handwritten signature] *nb*

[Handwritten signature]

[Handwritten signature] *Ö.Ü. A M.*