



**KİŞİSEL VERİ
İHLALİ BİLDİRİM FORMU
KILAVUZU**

KİŞİSEL VERİLERİ KORUMA KURUMU

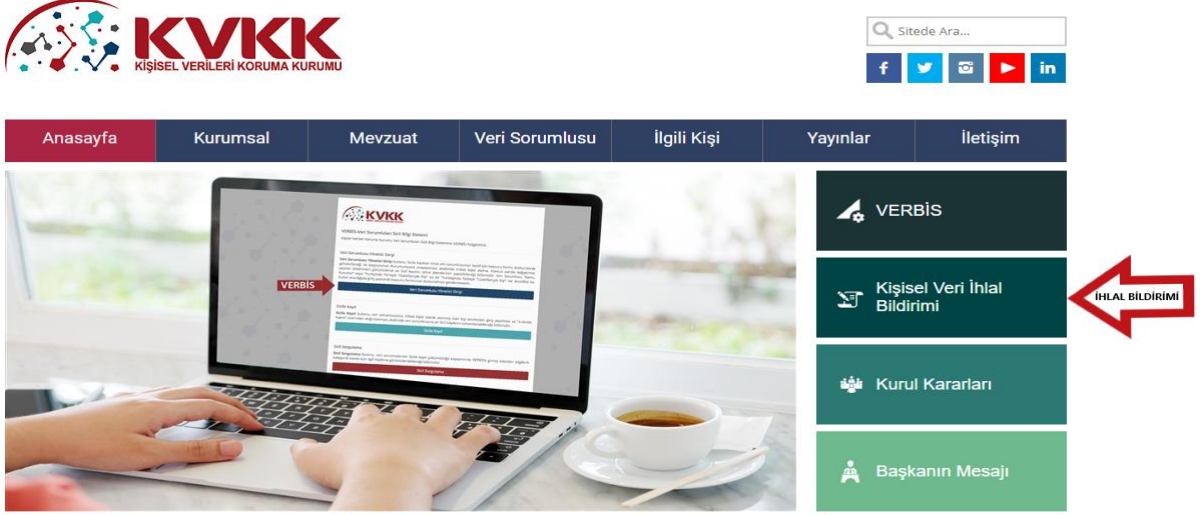
KİŞİSEL VERİLERİ KORUMA KURUMU

KİŞİSEL VERİ İHLALİ BİLDİRİM FORMU KILAVUZU

1. KİŞİSEL VERİ İHLALİ BİLDİRİM FORMUNA GİRİŞ	3
2. İHLAL BİLDİRİM FORMU ANASAYFASI	4
3. BİLDİRİM OLUŞTUR	5
3.1. Hakkınızda.....	5
3.2. İhlal Hakkında	6
3.3. Bildirim	10
3.4. Olası Sonuçlar	12
3.5. Önlemler	12
3.6. Ekler	13
4. BİLDİRİM SORGULA / BİLDİRİM GÜNCELLE	14

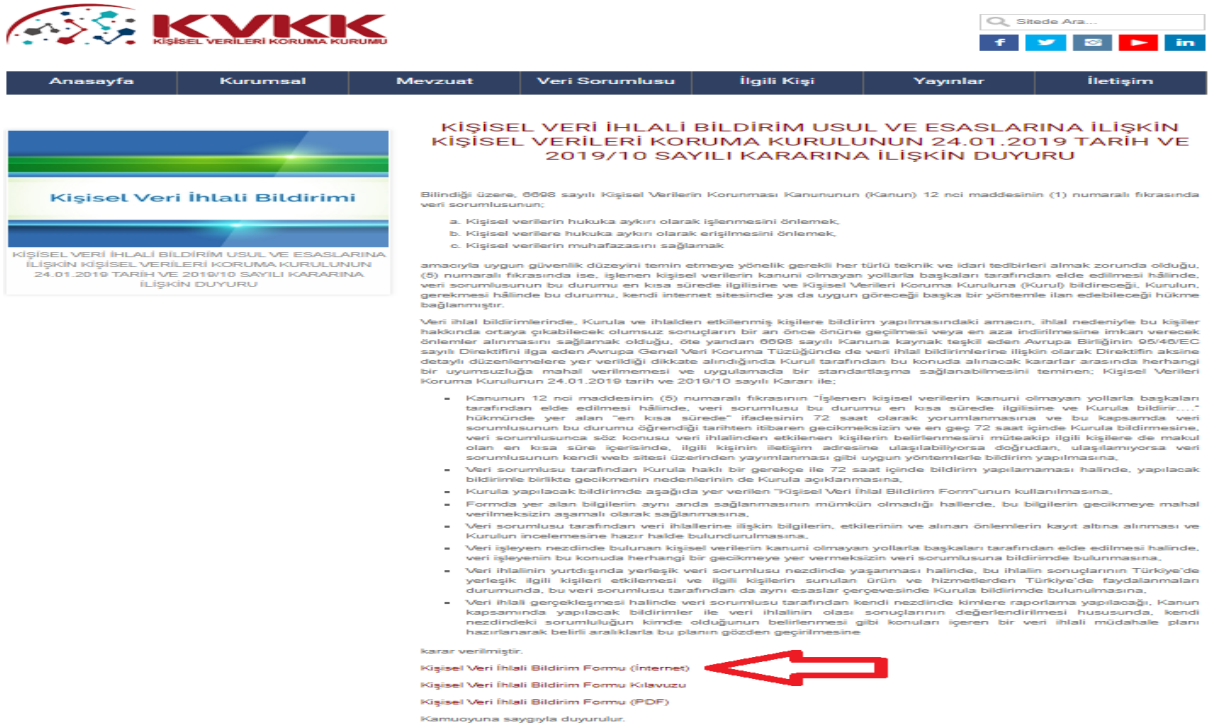
1. KİŞİSEL VERİ İHLALİ BİLDİRİM FORMUNA GİRİŞ

Kişisel Verileri Koruma Kurumunun internet sayfası olan www.kvkk.gov.tr adresine giriş yaptıktan sonra Anasayfa'da sağ taraftaki menüler içerisinde yer alan Kişisel Veri İhlal Bildirimi ikonuna tıklanarak kişisel veri ihlal bildirim alanına giriş yapılacaktır.



Şekil 1.1

Giriş yapılan sayfada “*KİŞİSEL VERİ İHLALİ BİLDİRİM USUL VE ESASLARINA İLİŞKİN KİŞİSEL VERİLERİ KORUMA KURULUNUN 24.01.2019 TARİH VE 2019/10 SAYILI KARARINA İLİŞKİN DUYURU*” yer almaktadır. Söz konusu duyuru sayfasının altında yer alan Kişisel Veri İhlal Bildirim Formuna (İnternet) tıklanarak bildirim sayfasına geçilebilmektedir. Form el ile doldurulmak isteniyorsa Kişisel Veri İhlal Bildirim Formuna (PDF) tıklanır.



Şekil 1.2

2. İHLAL BİLDİRİM FORMU ANASAYFASI

Açılan ihlal bildirim ana sayfasında, ihlal bildirim oluşturmak, Kuruma göndermek için “Bildirim Oluştur” ve ihlal bildirim sorgulamak ve güncellemek için “Bildirim Sorgula/Bildirim Güncelle” olmak üzere iki bölüm bulunmaktadır.



KİŞİSEL VERİLERİ KORUMA KURUMU İHLAL BİLDİRİM İŞLEMLERİ

İhlal Bildirimi oluşturmak için bu butonu kullanabilirsiniz.

+ Bildirim Oluştur

İhlal Bildirimi sorgulamak ve güncellemek için bu butonu kullanabilirsiniz.

Q Bildirim Sorgula / Bildirim Güncelle

Kişisel Veri İhlali Bildirim Formu Kılavuzu'nu görüntülemek için bu butonu kullanabilirsiniz.

📄 Kişisel Veri İhlali Bildirim Formu Kılavuzu



Şekil 2.1

KİŞİSEL VERİLERİ

3. BİLDİRİM OLUŞTUR

3.1. Hakkınızda

Bu bölümdeki alanların (Şekil 3.1) tamamının doldurulması zorunlu olup eksiksiz ve doğru bir şekilde doldurulduktan sonra “Kaydet” butonu tıklanarak kaydedilmesi gerekir.

“Veri Sorumlusunun Unvanı/İsmi” ve “Veri Sorumlusunun Adresi” alanlarına veri ihlalinin gerçekleştiği gerçek veya tüzel kişiliğin adı ve adresi yazılır.

“Veri Sorumlusu adına bu bildirim hazırlayan kişi” başlığı altındaki alanlar doldurulurken veri sorumlusu nezdinde çalışan yetkilendirilmiş bir personel tarafından veri ihlal bildirim yapıyor ise ilgili alanlar eksiksiz ve doğru bir şekilde doldurulur. Ancak, veri sorumlusu adına bir avukat, danışman vb. tarafından yapılan bir veri ihlal bildirim ise alanların doldurulmasının yanı sıra tevsik edici sözleşme veya vekaletname gibi belgeler “Ekler” bölümüne eklenmelidir.



A) Hakkınızda	B) İhlal Hakkında	C) Bildirim	D) Olası Sonuçlar	E) Önlemler	F) Ekler
---------------	-------------------	-------------	-------------------	-------------	----------

HAKKINIZDA

- Veri Sorumlusunun Unvanı/İsmi (*)
- Veri Sorumlusunun Adresi (*)
- Veri sorumlusu adına bu bildirim hazırlayan kişinin:
(Bu bildirim veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından doldurulması/gönderilmesi durumunda teşvik edici belgeleri (sözleşme, vekaletname vb.) ekleyiniz.)

Adı ve Soyadı (*)	<input type="text"/>
Görevi/Unvanı (*)	<input type="text"/>
E-postası (*)	<input type="text"/>
Telefonu (*)	<input type="text"/>
Adresi (*)	<input type="text"/>

Cevap:

Kaydet

Şekil 3.1

Şekil 3.1’deki alanlar doldurulup kaydedildikten sonra Şekil 3.2’de görüldüğü üzere tekil şekilde oluşturulan bir güvenlik kodu (takip numarası) ekrana gelecektir. Ekrana gelen bu kod tarafınızca kaydedilmelidir. Bu kod sonraki aşamalarda bildirim sorgulanması ve güncellenmesi açısından son derece önemlidir. Bu kodun kaybedilmesi durumunda veriguvenligi@kvkk.gov.tr adresine e-posta gönderip güvenlik kodunu sorgulayabilirsiniz.

Lütfen güvenlik kodunuzu(takip numarası) kaybetmeyiniz. Bildirim ile ilgili güncelleme yapabilmek için güvenlik kodunu girmeniz gerekecektir.

Güvenlik kodunuz: P6jRDWo5nbqZjYpv

Şekil 3.2

3.2. İhlal Hakkında

Bu bölümde “Bildirim Türü” alanına veri ihlali ile ilgili ilk kez bildirim yapılacaksa “İlk Bildirim” kutucuğu işaretlenir.

İhlalin başlama tarihi, veri sorumlusu tarafından yapılan incelemeler sonucunda veri ihlalinin başladığı tarihi ifade eder.

İhlalin sona erme tarihi, veri sorumlusu tarafından yapılan incelemeler sonucunda veri ihlalinin sona erdiği tarihi ifade eder.

İhlalin tespit tarihi ise, veri sorumlusunun ihlalden ilk haberdar olduğu tarihi ifade eder.

Şekil 3.3’deki alanlardan zorunlu seçeneği olanlar doldurulup bu bölümün diğer sorularıyla devam edilir.



Lütfen güvenlik kodunuzu(takip numarası) kaybetmeyiniz. Bildirim ile ilgili güncelleme yapabilmek için güvenlik kodunu girmeniz gerekecektir.

Güvenlik kodunuz: P6jRDWo5nbqZjYpv

A) Hakkınızda B) İhlal Hakkında C) Bildirim D) Olası Sonuçlar E) Önlemler F) Ekler

İHLAL HAKKINDA

4. Bildirim Türü (*)	<input type="checkbox"/> İlk Bildirim <input type="checkbox"/> Takip Bildirimi
Takip Numarası	<input type="text"/>
5. İhlalin başlama tarihi ve saati (*)	<input type="text"/> x [grid]
6. İhlalin sona erme tarihi ve saati	<input type="text"/> x [grid]
7. İhlalin tespit tarihi ve saati (*)	<input type="text"/> x [grid]

Şekil 3.3

Veri ihlalinin, veri işleyen nezdinde gerçekleşmesi ve veri sorumlusuna bildirilmesi durumunda Şekil 3.4’deki alanlar eksiksiz doldurulur. Veri ihlali, veri işleyen nezdinde gerçekleşmemişse bu alanın doldurulmasına gerek yoktur.

Veri işleyenin tespit tarihi, veri işleyen nezdinde gerçekleşen veri ihlalinin başladığı tarihi ifade eder.

Veri işleyenin veri sorumlusuna bildirdiği tarih, veri sorumlusunun veri ihlalden haberdar olma tarihini ifade eder.

Veri sorumlusunun veri işleyen tarafından nasıl haberdar edildiğine dair belgeleri (yazı, e-posta vb.) Ekler bölümüne eklemesi gerekmektedir.

8. İhlal veri işleyen tarafından veri sorumlusuna bildirildiyse:
(Yazı, e-posta mesajı vb. tevsik edici belgeleri bu bildirim ekinde gönderiniz.)

Veri işleyenin Unvanı/İsmi

Veri işleyenin Adresi

Veri işleyenin tespit tarihi ve saati x ☰

Veri işleyenin veri sorumlusuna bildirdiği tarih ve saat x ☰

Şekil 3.4

Veri ihlalinin kaynağı Şekil 3.5’de yer alan kutucuklardan işaretlenecek olup, aynı anda birden fazla seçenek de işaretlenebilir. Bununla birlikte veri ihlalinin nasıl gerçekleştiği hakkında verilecek bilgiler “Cevabınızı detaylı bir şekilde açıklayınız.” alanına yazılır. İhlalin kaynağı Şekil 3.5’deki mevcut seçeneklerden biri değilse “Diğer” kutucuğu işaretlenip ihlalin kaynağı ve nasıl gerçekleştiği ile ilgili bilgiler “Cevabınızı detaylı bir şekilde açıklayınız.” alanına yazılır. Örneğin; veri ihlali Siber Saldırı yöntemlerinden zararlı yazılım yüklenmesi ile gerçekleşmiş ise bu zararlı yazılımın ne olduğu, nasıl bulaştığı, hangi sistemleri etkilediği gibi detaylara yer verilerek “Cevabınızı detaylı bir şekilde açıklayınız.” alanına yazılır.

9. İhlalin kaynağı ve nasıl gerçekleştiği hakkında bilgi veriniz. (*) (Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz.)

Belge/cihaz hırsızlığı veya kaybolması

Verilerin güvensiz ortamlarda depolanması

Sabotaj

Kaza/ İhmal

Siber Saldırı

Zararlı yazılımlar

Sosyal mühendislik

Hizmet dışı bırakma (DoS-DDoS)

Fidyeye yazılımı (Ransomware)

Parola saldırısı (Brute-Force Attack)

Diğer

Diğer

Cevabınızı detaylı bir şekilde açıklayınız: (*)

Şekil 3.5

Veri ihlalinin etkisi Şekil 3.6’da görülen kutucukların işaretlenmesi ile belirtilir. Bu bölümde işaretlenecek olan;

Veri Gizliliği : Verinin yetkisiz kişilerce ele geçirilmesinin engellenmesidir.

Veri Bütünlüğü : Verinin olması gerektiği şekilde tutulması ve korunmasıdır.

Veriye Erişim : Verinin her an ulaşılabilir ve kullanılabilir olmasıdır.

Aynı anda birden fazla seçenek işaretlenebilir ve veri ihlalinin etkisi Şekil 3.6’da bulunan “Cevabınızı detaylı bir şekilde açıklayınız.” alanına yazılmalıdır.

10. İhlal etkisini belirtiniz. (*)	(Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz.)
	<input type="checkbox"/> Veri gizliliği
	<input type="checkbox"/> Veri bütünlüğü
	<input type="checkbox"/> Veriye erişim/ulaşılabilirlik
Cevabınızı detaylı bir şekilde açıklayınız:	(Cevabınızı detaylandırınız.)
	<input type="text"/>

Şekil 3.6

Şekil 3.7’deki alana veri ihlalinin nasıl ve kim tarafından tespit edildiği detaylı bir şekilde yazılacak olup varsa ihlal ile ilgili tevsik edici belgeler (yazılı metin, e-posta, fotoğraf vb.) “Ekler” bölümüne eklenir. Örneğin, veri sorumlusu fidye yazılımının sistemlerine yüklenmesine maruz kalıp saldırganlardan e-posta aldı ise bu tespit şekil 3.7’deki ilgili alana yazılır.

11. İhlalin nasıl tespit edildiği hakkında bilgi veriniz. (*)	(Varsa tevsik edici belgeleri bu bildirim ekinde gönderiniz.)
	<input type="text"/>

Şekil 3.7

Veri ihlalden etkilenen kişisel veri kategorileri Şekil 3.8’de yer alan kutucuklardan işaretlenecek olup, birden çok veri kategorisi olması halinde ilgili seçenekler birlikte işaretlenir. Veri ihlalden etkilenen kişisel veri kategorileri içerisinde uygun seçenek bulunmadığı takdirde “Diğer” seçeneği işaretlenir. Aynı zamanda veri ihlalden etkilenen özel nitelikli kişisel veriler varsa bu alandaki kutucuklar da aynı şekilde işaretlenir. Ayrıca ihlalden etkilenen kişisel veriler Şekil 3.8’deki *Cevabınızı detaylı bir şekilde açıklayınız.* alanına detaylı bir şekilde yazılır.

Örneğin, *Kimlik* verileri içerisinde ad-soyad, vatandaşlık numaraları, pasaport numaraları gibi; *İletişim* verileri içerisinde telefon numaraları, e-posta adresi gibi kişiyi ilgilendiren veriler yer almakta olup, bunlar “Cevabınızı detaylı bir şekilde açıklayınız.” alanına yazılır.

KİŞİSEL VERİLERİ KORUMA KURUMU KİŞİSEL VERİ İHLALI BİLDİRİM FORMU

12. İhlalden etkilenen kişisel veri kategorileri:
(Birden çok uyan seçeneğe bulunması halinde hepsini işaretleyiniz.)

Kişisel Veri (*)	<input type="checkbox"/> Kimlik	Özel Nitelikli Kişisel Veri (*)	<input type="checkbox"/> İrk ve Etnik Köken
<input type="checkbox"/> İletişim	<input type="checkbox"/> Lokasyon	<input type="checkbox"/> Siyasi Düşünce	<input type="checkbox"/> Felsefi İnanç, Din, Mezhep ve Diğer İnançlar
<input type="checkbox"/> Özlük	<input type="checkbox"/> Hukuki İşlem	<input type="checkbox"/> Kılık ve Kıyafet	<input type="checkbox"/> Demek Üyeliği
<input type="checkbox"/> Müşteri İşlem	<input type="checkbox"/> Fiziksel Mekan Güvenliği	<input type="checkbox"/> Vakıf Üyeliği	<input type="checkbox"/> Sendika Üyeliği
<input type="checkbox"/> İşlem Güvenliği	<input type="checkbox"/> İşlem Güvenliği	<input type="checkbox"/> Sağlık Bilgileri	<input type="checkbox"/> Cinsel Hayat
<input type="checkbox"/> Risk Yönetimi	<input type="checkbox"/> Risk Yönetimi	<input type="checkbox"/> Ceza Mahkumiyeti ve Güvenlik Tedbirleri	<input type="checkbox"/> Biyometrik Veri
<input type="checkbox"/> Finans	<input type="checkbox"/> Finans	<input type="checkbox"/> Genetik Veri	<input type="checkbox"/> Yoktur
<input type="checkbox"/> Mesleki Deneyim	<input type="checkbox"/> Mesleki Deneyim		
<input type="checkbox"/> Pazarlama	<input type="checkbox"/> Pazarlama		
<input type="checkbox"/> Görsel ve İşitsel Kayıtlar	<input type="checkbox"/> Görsel ve İşitsel Kayıtlar		
<input type="checkbox"/> Diğer	<input type="checkbox"/> Diğer		
<input type="checkbox"/> Yoktur	<input type="checkbox"/> Yoktur		

Cevabınızı detaylı bir şekilde açıklayınız: (Cevabınızı detaylandırınız.)

Şekil 3.8

Şekil 3.9'daki alana veri ihlalden etkilenen kişi ve kayıt sayısı yazılır. İhlalden etkilenen kişi ve kayıt sayısının tespit edilememesi durumunda bunun nedeni açıklanır. Kayıt sayısı ile ihlalden etkilenen kişi sayısı veri kategorilerine göre değişiklik gösterebilir. Bu sayı hesaplanırken ilgili kişinin ihlale uğrayan tüm verilerinin sayısı dikkate alınır. Örneğin, 10 kişinin TC Kimlik numarası ve adresi veri ihlalden etkilenmiş ise kişi sayısı 10, kayıt sayısı ise 20 olacaktır.

13. İhlalden etkilenen kişi ve kayıt sayısı:

Kişi Sayısı (*)

Kayıt Sayısı (*)

Kişi ve/veya Kayıt Sayıları Tahmini ise Kesin sayıların tespit edilememesi nedenini açıklayınız. (Kişi ve/veya Kayıt Sayıları Tahmini ise Kesin sayıların tespit edilememesi nedenini açıklayınız.)

Şekil 3.9

Veri ihlalden etkilenen ilgili kişi grupları ve ihlalin ilgili kişiler üzerindeki etkileri Şekil 3.10'da yer alan kutucuklardan işaretlenecek olup, ilgili kişi grubu ve ihlalin ilgili kişiler üzerinde etkisinin birden fazla olması durumunda birden fazla seçeneğe işaretlenmelidir. Bu kategoriler dışında bir seçeneğe olması halinde "Diğer" seçeneği işaretlenir ve cevap gelecek boşluğa girilir.

Bu alanın da tamamlanması sonrasında, "Kaydet" butonuna tıklanarak, "Bildirim" bölümüne geçilir.

14. İhlalden Etkilenen İlgili Kişi Grupları ve Etkileri:
(Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz.)

İlgili Kişi Grupları (*) (Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz.)

Çalışanlar
 Kullanıcılar
 Aboneler/Üyeler
 Öğrenciler
 Müşteriler ve potansiyel müşteriler
 Hastalar
 Çocuklar
 Korunmaya muhtaç yetişkinler
 Henüz bilinmiyor
 Diğer

İlgili Kişiler Üzerindeki Etkileri (*) (Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz.)

Kişisel Veriler Üzerinde Kontrol Kaybı
 Kimlik Hırsızlığı
 Ayrımcılık
 Hakların Kısıtlanması
 Dolandırıcılık
 Finansal Kayıp
 İtibar Kaybı
 Kişisel Verilerin Güvenliği Kaybı
 Diğer

Kaydet

Şekil 3.10

3.3. Bildirim

Şekil 3.11’de bulunan alan geç bildirimde bulunan veri sorumluları tarafından doldurulur. İhlalin tespitinden ihlalin Kurula bildirimine kadar geçen süre 72 saati aşmış ise bunun nedenleri bu alana girilmelidir.

BİLDİRİM

15. Kurula bildirimde tespit tarihinden sonra 72 saat geçirilmiş ise geç bildirim sebebini açıklayınız

Şekil 3.11

Şekil 3.12’de ilgili kişilere ihlal bildirim yapıp yapılmadığına dair seçenekler işaretlenir. Eğer “Evet, ilgili kişilere bildirim yapıldı” veya “İlgili kişilere halihazırda bildirim yapılmaktadır.” kutucukları işaretlenmiş ise bildirimle ilgili tevsik edici belgeler “Ekler” bölümüne eklenmelidir. “Diğer” seçeneği seçilmişse, cevap detaylı bir şekilde açıklanır.

16. İlgili kişilere ihlal bildirim yapıldı mı? (*)

Evet, etkilenen ilgili kişilere bildirim yapıldı
 İlgili kişilere halihazırda bildirim yapılmaktadır
 Hayır, ancak bildirilecek
 Diğer (Aşağıda detayları belirtiniz)

Cevabınızı detaylı bir şekilde açıklayınız: (Cevabınızı detaylandırınız.)

Şekil 3.12

Şekil 3.13’de bulunan alana ilgili kişilere yapılan veya yapılması planlanan bildirim tarihi eklenir.

17. İlgili kişilere yapılan/yapılacak bildirim tarihi	<input type="text"/>
-------------------------------------------------------	----------------------

Şekil 3.13

Şekil 3.14’te yer alan alana ilgili kişilere yapılan veya yapılması planlanan bildirim yöntemi yazılır. Bu bildirimler e-posta, mektup, sms vb. şekilde olabilmektedir. Ayrıca bu bildirim bir örneği “*Ekler*” bölümüne eklenmelidir.

18. İlgili kişilere hangi yöntemle bildirim yapıldı/yapılacağı hakkında detaylı bilgi veriniz.	(Varsa bildirim örneğinin bir nüshasını bu bildirim ekinde gönderiniz)
<input type="text"/>	<input type="text"/>

Şekil 3.14

Şekil 3.15’te bulunan alana ilgili kişilerin veri ihlali ile ilgili bilgi alabileceği iletişim kanalları yazılacaktır. Örneğin, veri sorumlusu tarafından veri ihlali hakkında bilgi verecek çağrı merkezi veya veri ihlaline dair bilgilerin bulunduğu internet adresi.

19. İlgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak iletişim yollarını belirtiniz.	(İnternet adresi, çağrı merkezi vb. bilgiler)
<input type="text"/>	<input type="text"/>

Şekil 3.15

Veri ihlali ile ilgili Türkiye’de yer alan yargı, kolluk kuvvetleri veya diğer kamu kurumlarının görev alanına giren bir husus olması durumunda ve bu ihlal hakkında bu organizasyon veya kurumlara bilgi verilmiş/verilecek ise Şekil 3.16’daki kutucuklardan “Evet” seçeneği işaretlenir. Aksi durumda “Hayır” seçeneği işaretlenir. “Evet” seçeneğinin işaretlenmesi durumunda tevsik edici belgeler “*Ekler*” bölümüne tercihe göre eklenebilir. Örneğin, şikâyetçi ifade tutanağı, olay yeri inceleme raporu, suç duyurusu vb.

20. Yurtdışında bulunan diğer organizasyon veya kurumlara ihlal hakkında bilgi verildi mi veya vermeyi düşünüyor musunuz ?	(Örn. polis, diğer denetim ya da gözetim kurumları. Diğer kurumlar ile iletişime geçmeniz gerekebilir.)
<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır

Şekil 3.12

Veri ihlali ile ilgili yurtdışında bulunan yargının, kolluk kuvvetlerinin veya diğer kamu kurumlarının görev alanına giren bir husus olduğu durumda ve bu ihlal hakkında bu yurtdışında bulunan organizasyon veya kurumlara bilgi verilecek ise Şekil 3.17’deki kutucuklardan “*Evet*” seçeneği işaretlenir. Aksi durumda “*Hayır*” seçeneği işaretlenir. “Evet” seçeneğinin seçilmesi durumunda tevsik edici belgeler “*Ekler*” bölümüne tercihe göre eklenebilir. Bu işlem tamamlandıktan sonra “*Kaydet*” butonuna tıklanır ve “*Olası Sonuçlar*” bölümüne geçilir.

21. Yurtdışında bulunan diğer organizasyon veya kurumlara ihlal hakkında bilgi verildi mi veya vermeyi düşünüyor musunuz ?

(Örn. polis, diğer denetim ya da gözetim kurumları.)

seçimimi kaldır

Evet

Hayır

Kaydet

Şekil 3.17

3.4. Olası Sonuçlar

Bu bölümde “ilgili kişilerin olumsuz etkilere maruz kalma olasılığı” seçeneklerinden bir tanesi veri sorumlusu tarafından işaretlenir. Şekil 3.18’de bulunan açıklamalar dikkatli bir şekilde okunup yaşanılan veri ihlali ile karşılaştırılır ve en uygun seçenek işaretlenir.

OLASI SONUÇLAR

22. İlgili Kişilerin Olumsuz Etkilere Maruz Kalma Olasılığı (*)

(Gerçekleşen veri ihlalinin düzeyinin belirlenmesinde ilgili kişiler üzerinde ne kadar bir potansiyel etkiye neden olduğunun değerlendirilmesi gerekmektedir. Söz konusu potansiyel etkinin değerlendirilmesinde ise ihlalin niteliği, nedeni, ihlale maruz kalan verinin türü, ihlalin etkisinin azaltılmasında alınan önlemler ile ihlalden etkilenen ilgili kişi kategorileri göz önünde bulundurulmalıdır)

- Çok Yüksek (İlgili kişiler üstesinden gelebilecekleri zorluklar ve geri döndürülemez sonuçlar ile karşılaşabilir (işin durması, uzun süreli psikolojik veya fiziksel rahatsızlık, ölüm vb.))
- Yüksek (İlgili kişiler zorluklara rağmen üstesinden gelmeleri gereken ciddi sonuçlarla karşılaşabilirler. (Maddi zarar, iş kaybı, adli soruşturma, sağlığın kötüleşmesi vb.))
- Orta (İlgili kişiler zorluklara rağmen üstesinden gelebilecekleri olumsuzluklarla karşılaşabilirler (Fazla efor, ek maliyet, stres, küçük fiziksel rahatsızlıklar vb.))
- Düşük (İlgili kişiler üstesinden gelebilecekleri küçük olumsuzluklarla karşılaşabilirler (fazla zaman harcama, sıkıntı vb.))
- Henüz Bilinmiyor

Şekil 3.18

“İhlalin Organizasyonunuza Olan Etkileri”, Şekil 3.19’da görülen kutucuklar yanlarında yer alan açıklamalarla birlikte dikkatli bir şekilde okunup yaşanılan veri ihlali ile karşılaştırılarak veri sorumlusu tarafından işaretlenir. Örneğin, veri sorumlusunun sistemindeki tüm kişisel veriler geri döndürülemez şekilde tamamen (yedekleriyle beraber) yok edilmiş ve veri sorumlusunun tüm organizasyonu (iş akışı) yok edilen bu verilere bağlı ise bu ihlalin veri sorumlusunun organizasyonuna etkisi “Çok Yüksek” olarak işaretlenecektir. Sonrasında Kaydet butonuna tıklanır ve bir sonraki “Önlemler” bölümüne geçilir.

23. İhlalin Organizasyonunuza Olan Etkileri (*)

- Çok Yüksek (Her türlü hizmet sunma yetisinin kaybedilmesi.)
- Yüksek (Önemli hizmetleri sunma yetisinin kaybedilmesi.)
- Orta (Bazı hizmetlerin sunumunda kontrol kaybı ve eksikliğin oluşması.)
- Düşük (Herhangi bir etkinlik ve kontrol kaybının olmaması.)
- Bilinmiyor

Kaydet

Şekil 3.19

3.5. Önlemler

Şekil 3.20’te görülen alana çalışanların kişisel verilerin korunması hususunda son bir yıl içinde aldığı eğitimler yazılır. Çalışanların aldığı eğitimlere dair tevsik edici belgeler “Ekler” bölümüne eklenmelidir.

ÖNLEMLER

24. İhlal ile ilgili olan çalışanların son bir yıl içerisinde aldığı eğitimler nelerdir? (Varsa tevsik edici belgeleri bu bildirim ekinde gönderiniz.)

Şekil 3.20

Veri sorumlusu, veri ihlalinden önce aldığı teknik ve idari tedbirleri Şekil 3.21’de görülen alanları doldurarak bildirir. Söz konusu tedbirlerle ilgili varsa gerekli açıklamalar en altta yer alan “Açıklamalar” alanına yazılabilir. Ayrıca ihlalden önce alınmış tedbirlere dair tevsik edici belgeler “Ekler” bölümüne eklenmelidir.

25. Bu tür ihalleri engellemek için ihlalin gerçekleşmesinden önce almış olduğunuz teknik ve idari tedbirlerinizi belirtiniz.: (Varsa tevsik edici belgeleri bu bildirim ekinde gönderiniz.)

Teknik Tedbirler (*)

İdari Tedbirler (*)

Açıklama

Şekil 3.21

Veri sorumlusu, veri ihlalinden sonra aldığı teknik ve idari tedbirleri Şekil 3.22’de görülen alanları doldurarak bildirir. Tedbirlerle ilgili varsa gerekli açıklamalar en altta yer alan “Açıklamalar” alanına yazılabilir. Ayrıca ihlalden sonra alınmış tedbirlere dair tevsik edici belgeler “Ekler” bölümüne eklenir.

26. İhlal sonrası almış olduğunuz veya almayı planladığınız teknik ve idari tedbirleri belirtiniz ve bunların tahminen ne zaman tamamlanacağı hakkında bilgi veriniz.: (Problemi çözmek ve olumsuz etkilerini ortadan kaldırmak adına almış olduğunuz önlemleri belirtiniz; örneğin yanlışlıkla gönderilmiş olan verilerin yok edilmesi, şifrelerin güvenliğinin sağlanması, veri güvenliği eğitimi planlanması vb. ayrıca bu tedbirlere ait varsa tevsik edici belgeleri bu bildirim ekinde gönderiniz.)

Teknik Tedbirler (*)

İdari Tedbirler (*)

Açıklama

Kaydet

Şekil 3.22

3.6. Ekler

İhlal Bildiriminin son bölümü olan Ekler bölümüne (Şekil 3.23) veri ihlali ile ilgili tevsik edici belgeler konusuna göre “İlgili Soru” kısmından seçilerek “Dosya Seç” butonuna tıklanarak geçerli dosya formatları halinde yüklenir. Yüklenecek tevsik edici belgenin konusu “İlgili Soru” kısmında bulunmuyorsa “Diğer” seçeneği işaretlenir. Geçerli formatta bir dosya seçilmediği takdirde Şekil 3.24’teki gibi uyarı mesajı görülür. Kaydet butonuna tıklandığında

o ana kadar bütün bölümlerde yapılan işlemler kaydedilir ve istenilen bölümde değişiklik yapma imkanı devam eder.

A) Hakkınızda	B) İhlal Hakkında	C) Bildirim	D) Olası Sonuçlar	E) Önlemler	F) Ekler
Dosya Açıklaması	<input type="text"/>				
İlgili Soru	<input type="text" value="İlgili Soru seçiniz."/>				
Dosya Yükleme	<input type="button" value="Dosya Seç"/> Dosya seçilmedi				
<input type="button" value="Kaydet"/>			<input type="button" value="Kaydet ve Kuruma Gönder"/>		

Şekil 3.23

▲ Geçerli bir dosya seçmediniz. Seçtiğiniz dosya .jpg , .jpeg , .png , .gif , .doc , .docx , .pdf , .xls , .xlsx , .txt uzantılarından birine sahip olmalıdır.

Şekil 3.24

Kaydet ve Kuruma Gönder butonuna tıklandığında kayıt işlemi tamamlanır, Şekil 3.25'teki uyarı mesajı çıkar ve sadece “Ekler” bölümünde değişiklik yapılabilir

Giriş yaptığınız bilgilerle kaydınız yapılmış ve kuruma gönderilmiştir. Güvenlik kodunuzu(takip numarası) kullanarak bildirime dosya yüklemesi yapabilirsiniz.

Şekil 3.25

4. BİLDİRİM SORGULA / BİLDİRİM GÜNCELLE

İhlal Bildirim aşamasını tamamladıktan sonra doldurulan bildirim görmek için Şekil 4.1'de görülen Bildirim Sorgula / Bildirim Güncelle seçeneğine tıklanarak giriş yapılır.



KİŞİSEL VERİLERİ KORUMA KURUMU İHLAL BİLDİRİM İŞLEMLERİ

İhlal Bildirimi oluşturmak için bu butonu kullanabilirsiniz.

+ Bildirim Oluştur

İhlal Bildirimi sorgulamak, güncellemek ve pdf oluşturmak için bu butonu kullanabilirsiniz.

Q Bildirim Sorgula / Bildirim Güncelle

Şekil 4.1

Çıkan sorgu ekranına Şekil 3.2’de yer alan ve her bir ihlal bildirimini için verilen güvenlik kodu Şekil 4.2’de bulunan alana girilip “Sorgula” butonuna tıklandıktan sonra bildirim düzenlemeye yarayan sayfa çıkacaktır.



KİŞİSEL VERİLERİ KORUMA KURUMU İHLAL BİLDİRİMİ SORGULAMA

Güvenlik Kodu:

Güvenlik Kodu Giriniz..

Cevap:

43 + 4 = ?

Cevap

Sorgula

Şekil 4.2

Şekil 4.3’te görüldüğü üzere Bildirimi Düzenle butonuna tıkladığında; bildirim düzenleme yöntemi, bildirim hazırlayan kişinin kaydetme şekline göre değişiklik göstermektedir. Eğer bildirim hazırlayan kişi, Şekil 3.23’te görüldüğü üzere “Kaydet” butonuna tıklayıp çıkış

yaptığı takdire bütün bölümlerde güncelleme yapabilir. Fakat “Kaydet ve Kuruma Gönder” butonuna tıkladığı takdirde sadece “Ekler” bölümünde düzenleme yapabilir.



KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

KİŞİSEL VERİLERİ KORUMA KURUMU
İHLAL BİLDİRİMİ SORGULAMA

[Bildirim Düzenle](#)

Giriş yaptığınız kodla yukarıdaki işlemi yapabilirsiniz.

Güvenlik Kodu:

FyfD9GB6rAHayVYV

Cevap:

37 + 4 = ? 47

[Sorgula](#)

Şekil 4.3