T.C.
SAĞLIK BAKANLIĞI
Teftiş Kurulu Başkanlığı

7/18200 GK 28

Sayı : 55753567-610
Konu : Yazılı Soru Önergesi Cevabı

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi : 22.10.2024 tarihli ve 1515841 sayılı yazı.

Bursa Milletvekili Sayın Kayıhan PALA tarafından verilen "Kişisel verilerin çalındığı iddiasına ilişkin" 7/18200 sıra sayılı yazılı soru önergesinin cevabı ilişikte sunulmaktadır.

Arz ederim.

Prof. Dr. Kemal MEMİŞOĞLU
Sağlık Bakanı

EK: Önerge Cevabı

Üniversiteler Mah. Şehit Mehmet Bayraktar Cad. No: 3
Bilkent Yerleşkesi Çankaya/ANKARA 06800
Telefon No: (0312) 471 74 88
KEP Adresi: sb@hs01.kep.tr
e-posta: tkb@saglik.gov.tr İnternet Adresi: www.teftis.saglik.gov.tr

Bilgi İçin: Gülay ŞİMŞEK
Birim Sorumlusu

Bursa Milletvekili Sayın Kayıhan PALA tarafından verilen "Kişisel verilerin çalındığı iddiasına ilişkin" 7/18200 sıra sayılı yazılı soru önergesi cevabıdır.

SORULAR:

Sağlık Bakanlığına ait veri sisteminden verilerin çalındığına dair bugüne kadar birçok iddia ortaya atılmış, iddialar hakkında kamuyu bilgilendirmek amacı ile Bakanlığımızdan herhangi bir açıklama yapılmamıştır.

Sağlık veri standardizasyonunun sağlanması amacıyla, 2003 yılında duyurulan 'Sağlıkta Dönüşüm' programının bir parçası olarak kurulan; Sağlık Neti, Sağlık Net2 ve enabız sisteminde toplanan ve muhafaza edilen verilerin güvenliğinin sağlanamaması iddiaları başta olmak üzere; 2021 yılında e-nabız uygulamasına ait olduğu öne sürülen 7 milyon satırlık veri tabanının da yasadışı internet ortamlarında satışa çıkarıldığı iddia edilmektedir. Benzer şekilde, 26 Eylül ve 21 Kasım 2022 tarihlerinde Halk Sağlığı Yönetim Sisteminde oluşan bir açık nedeniyle ele geçirildiği iddia edilen 101 milyon (yaşayan ve hayatım kaybetmiş) kişinin verisi internet ortamında satışa çıkarılmıştır. Son olarak, 9 Eylül 2024 tarihinde ifade ve internet özgürlüğü alanında yayın yapan Free Web Turkey sitesi, Türkiye'deki resmî kurumlarda kaydı olan 108 milyon yurttaşın kişisel verilerinin çalındığım iddia etmiştir.

Bakanlığınız tarafından toplanan ve muhafaza edilen verilerin güvenliğinin ihlal edildiği ve kamuya açık bir şekilde satışa sunulduğu iddiaları hakkında Bakanlığınızın sessiz kalmasına karşın; 12 Eylül 2024 tarihinde Ulaştırma ve Altyapı Bakanı Abdulkadir Uraloğlu pandemi döneminde Sağlık Bakanlığı sisteminden kaynaklı bir sızıntı yaşandığını "Bu pandemi sürecindeki hatırlarsınız, sağlık sisteminden bir sızıntıdır. Onun haricinde yok İnsanların güncel verilerinin çalındığıyla ilgili bir veri yok. Pandemi sürecinde bazı bilgilerin maalesef belli şekliyle elde edilmiş olduğu doğru. O süreçte o maalesef önlenemedi." açıklaması ile kabul etmiştir.

Bu bağlamda;

1- Bakanlığınızın veri gizliliği politikası ne kadar kapsamlıdır? Bu politika çalışanlar, veriyi işleyenler ve veri sağlayan hastalar tarafından bilinmekte midir?
2- Bu verilerin toplanması ve işlenmesi için hangi yasal dayanağınız bulunmaktadır? Verilerin toplanması ve saklanması süreçlerinde Kişisel Verilerin Korunması Kanununa uygunluk sağlanmakta mıdır?
3- Veriler üçüncü kişilerle paylaşılmakta mıdır? Paylaşılıyor ise hangi kurum veya kişilerle ve hangi amaçla paylaşılmaktadır?
4- Kurumunuzun elektronik ağ altyapısı nasıl korunmaktadır?
5- Bakanlığınızda tutulan veriler şifrelenmekte midir? Eğer şifrelenmişse hangi şifreleme algoritması kullanılmaktadır?
6- Kurumunuzda sızma tespit sistemleri kullanılmakta mıdır? Bu sistemlerin ne sıklıkla güncellendiği ve test edildiği konusunda raporlar bulunmakta mıdır?
7- Sisteme erişimde ağ trafiği düzenli olarak izlenmekte midir? Şüpheli aktiviteler için uyarı sistemleri mevcut mudur?
8- Veri saklama ve işleme sisteminize erişimi olan kullanıcılar kimlerdir? Bu kullanıcıların erişim yetkileri nasıl belirlenmektedir? Veri tabanlarına erişim nasıl kontrol edilmektedir? Yetkilendirme ve kimlik doğrulama mekanizmaları nelerdir?
9- Veri tabanına sızan işlemleri hangi aşamalarından geçerek gerçekleşmiş ve hangi güvenlik açıkları kullanılmıştır?
10- Veri güvenliği ihlallerinin nasıl gerçekleştiği konusunda yapılan teknik inceleme sonucunda ne gibi sonuçlara varılmıştır? Her bir olay için tek tek açıklanmak üzere;
a-Verilerin ne kadar süre boyunca yetkisiz erişime açık olduğu tahmin edilmektedir?
b-İddia edilen tüm veri güvenliği ihlallerinde sızdırılan verilerin tam listesi nedir? Sızdırılan veriler arasında hangi kategorilerdeki bilgiler yer almaktadır (örneğin, T.C. kimlik numarası, adres, telefon numarası, sağlık bilgileri vb.)?
c-Sızdırılan verilerin boyutları nedir?
d-Veriler nasıl sızdırılmıştır (örneğin, brute force saldırısı, SQL injection, phishing vb.)?

e-Sızmaların gerçekleştiği nokta tam olarak neresidir? Sistemin hangi kısmında bir güvenlik zafiyeti oluşmuştur?

f-Sızma anında sistemde hangi güvenlik önlemleri aktifti? Bu önlemler neden sızıntıyı engelleyemedi?

g-Sızıntılar ne zaman fark edildi? İlk belirtiler neydi?

h-Sızıntıların fark edilmesinde gecikme yaşanmasının nedenleri nelerdir?

i-Sistemde tespit edilen güvenlik açıkları nelerdir? Bu açıkların varlığı ne kadar süredir biliniyordu?

j-Nüfus Vatandaşlık İşleri (NVİ) üzerinden alınan veriler yaşayan siber saldırılarda kaybedilmiş midir?

11- Sızıntıların sorumluluğu kimdedir? Sorumlular hakkında ne gibi disiplin işlemleri başlatılmıştır? Olaylarla ilgili iç soruşturma başlatılmış mıdır? Soruşturma kapsamında kimler sorguya çekilmiştir? Soruşturmaların sonuçları açıklanmış mıdır/ ne zaman açıklanacaktır?

12- Olaylarla ilgili yasal süreç başlatılmış mıdır? Başlatılmışsa, her olay için ayrı ayrı bilgi verilmek üzere süreç hangi aşamadadır?

13- Kurumunuzun veri güvenliği sistemleri denetlenmekte midir? Denetleniyor ise, hangi sıklıkta ve ne zamandan denetlenmektedir?

14- Suç teşkil eden bu tür ihlallerin tekrarlanmaması için kurumunuzda ne gibi yapısal değişiklikler yapılmıştır?

15- Bu olayların yaşanması nedeniyle veri sahipleri nasıl bilgilendirilmiştir? Mağdurların mağduriyetlerinin giderilmesi için ne gibi önlemler alınmaktadır?

16- Bakanlığınız, sağlık hizmetleri veren kamu özel ve vakıf üniversiteleri kuruluşları için kişilere ait verileri nüfus vatandaşlık işleri (nvi) sisteminden sorgularken, sağlık kuruluşlarında kullanılan sağlık yazılımları veri tabanlarına kişisel verileri kaydetmekte midir? Kaydediliyor ise bu verilerin güvenliğini nasıl sağlanmaktadır?

17- Kişisel sağlık verileri özel sigorta şirketlerinin eline nasıl geçmiştir?

CEVAPLAR:

Bakanlığımız Sağlık Bilgi Sistemleri Genel Müdürlüğü Bilgi Güvenliği Politikaları Kılavuzu'nda yer alan tedbirler başta olmak üzere her türlü teknik ve idari tedbir alınmaktadır.

Bakanlığımız tarafından işlenen kişisel veriler 6698 sayılı Kanun'un 8'inci, 9'uncu ve 28'inci maddelerinde yer alan istisnai şartlar haricinde üçüncü kişiler veya diğer kurum ve kuruluşlar ile paylaşılmamaktadır. 6698 sayılı Kanun ve ikincil düzenlemelerine, Kişisel Sağlık Verileri Hakkında Yönetmeli ve Hasta Hakları Yönetmeliği'ne aykırı hiçbir işlem gerçekleştirilmemektedir. Kişisel verilerin pandemi sürecinde sızdırıldığı ve satıldığı iddiaları ise gerçeği yansıtmamaktadır.

Son kullanıcı kaynaklı bir veri ihlali olması durumunda ise "Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarihli ve 2019/10 sayılı Kararına İlişkin Duyuru" kapsamında Kişisel Verileri Koruma Kurumuna ihlal bildiriminde bulunulmakta olup ayrıca Cumhuriyet Başsavcılıklarına konunun adli yönden de araştırılması için suç duyurusunda bulunulmaktadır.

Ayrıca, Bakanlığımızca işlenen kişisel verilere ilişkin alınan tüm idari ve teknik tedbirlere yönelik detaylı bilgiye https://verbis.kvkk.gov.tr/ adresinden Bakanlığımız sorgulanarak erişim sağlanabilmektedir.

Konuya gösterilen ilgiye teşekkür ederim.