Gizlilik

Amaç

Etkilenen Platformlar

Tüm Platformlar

Ilgili COBIT Konulari

PO8 – Tüm alanlar tekrar gozden gecirildi

PO8.4 – Gizlilik,Entellektüel Özellik ve Veri Akişi

Mevzuat

Avustralya

Avusturalya Hükümetinin belirledigi 10 National Privacy Principles (NPP's) Ulusal Gizlilik İlkesi (UGI) kısmen Privacy Act.'nin iyilestirilmis halidir. Ilgili dokümanin tamamina ulasmak icin;

http://www.privacy.gov.au/publications/npps01.html

UGI ve (Privacy Act.) fazlaca kompleks olmadiginda diger ülkelerde yasalardan kacinma ve korunmada oldukca iyi calismaktadir.Yükümlülük bilgiyi toplama ve saklama esnasinda güvenlik saglanana kadar Şirkete aittir, bu zamana kadar da kullanici haklari gizlidir (Privacy Act.).

Kısaltılmış olarak 10 İlke (prensip) asagidaki gibidir;

1-) Toplama: Eger ticari anlamda kesinlikle faydali olacaksa, verileri birseysel olarak toplayabilir ve saklayabilirsiniz.

2-) Kullanim ve Patent Hakki Bildirimi: 3. Şahıslara gizli bilgiler, açıklamar ve patent hakki veremezsiniz.

3-) Veri Kalitesi: topladiginiz verilerin doğrulugunu ve güncelligini garantiye almalisiniz.

4-) Veri Güvenligi: Veri güvenliginiz icin verilerinizi dataya erisimi olmayan kullanicilardan korumalisiniz.

5-) Açıklik: Gizlilik İlkeleriniz doğrultusunda datanizin hangi kismini sakladiginizi kullanicilara bildirecek metni hazirlamalisiniz.

6-) Kullanim ve Doğrulama: Kullanicilara Veriyi yeniden incelemeleri icin izin vermelisiniz.

Insanlar verinin silinmesini talep edebilirler.

7-) Tanimlayici Bilgiler (Kimlik) : Kişisel bilgilerinizde resmi kimlikleri kullanamazsiniz (Pasaport, ehliyet vb.)

8-) Anonimlik (Yaraticinin Bilinmemesi): Eger mümkünse kullanicilar anonimlik hakkini kullanmalidirlar.

9-) Veri Akişini Sinirlamak: Avustralya sinirlari disina gizli veri yollayamazsiniz.

10-) Hassas Açıklamalar (Bilgiler): Açıklamalariniz da politik, siyasi, saglik durumu vb. Bilgiler bulunduramazsiniz.

Şirketler, kuruluslar, topluluklar kullanacaklari verileri toplarken, bazi detaylarda bu noktalarin gizliliğini isteyebilirler. Ornek vermek gerekirse, esas olarak sinav ortaminda Kişisel bilgi kullanmak yasak olsa da, kullanici Kişisel anlasmaniz onceden bu bilgilerin kullanima açık oldugu sartini iceriyorsa, kullanilabilmektedir.

Cezalar sert ve kesin daha da iyisi single offences, kaydadeger, önemli personel bilgilerini saglama almak icin profesyonel hukuki bilgi destegi almalisiniz, edinmelisiniz.

EU

Avrupa Birligi Talimatlari 95/46/EC ihtiyac doğrultusunda Avrupa Birligi bünyesinde belirli istekleri ortebilir saklayabilir. Özetlemek gerekirse, bilgiler sadece gerektigi zaman toplanir, istenmedikce bilgiler değiştirilemez ve bilgiler politik, ırkci, dinsel düşünce & açıklama iceremez.

Her üye ülkenin bu konu altinda kendi yasalari vardir.

UNITED KINGDOM

United Kingdom Veri Güvenligi Geçmişi

(1998http://www.opsi.gov.uk/acts/acts1998/19980029.htm) personel veri stogunu kullanmak ve islemek icin 8 Veri Güvenligi İlkesi belirlemiştir.

Not: Personel data “Duyarlı (Özel) Personel Verileri” icinde ırk, din, sex yasami, politik gorüsler, dini inanclar vb. Bunlar yüksek seviyeli personel verileridir.

1-) Personel verileri dürüstce ve adil bir şekilde islenmelidir,

(a) At least one of the conditions in Schedule 2 [processing of personal data] is met, and

(b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 [processing of sensitive personal data] is also met.

2-) Kişisel veriler yalnizca bir kez ya da oldukça açık olduğunda ve yasalara uygun amaclar olduğunda edinilebiliri ve bu amaç ya da amaçlarla birlikte bağdaşmayan tarzlar (davranıs biçimleri) daha fazla islenememelidir.

3-) Kişisel veriler konuyla ilgili ve asırı olmayan baglantıda amac ya da amaclar icin islem yapmak icin yeterli olmalidir.

4-) Kişisel veriler kesin ve gerekli olmalidir, kept up to date yapmak icin.

5-) Amac ya da amaclar icin islenen Kişisel veriler amac ya da amaclar icin gerekli olandan daha uzun süre saklanamaz.

6-) Bu Act. Altinda veri konusunun doğrulari ile uyum icinde Kişisel veriler islenebilir.

7-) YetKişi olmayanlar verileri dikkatle inceleyerek personel verilerine ulasabilir, zarar verebilir, kullanabilir, silebilirler.

8-) Personel veri Güvenligi saglanana kadar personel verileri bir baska ülke ve ya bolgeye transfer edilmemeli, Avrupa Birligi sinirlari disina cikarilmamalidir.

Özetle, The Act. Veri doğrulugunun tanimlanmasi:

- Personel Verilerine Doğru Erisim: Personel hakkinda ki verilerin ne amacla toplandigini ve bunu kimin gorecegini bilmek isteyebilir.
- Where data controller is credit reference agency: Kredi acentalari sadece finansal durum hakkinda açıklama yapabilirler, spesifik detaylara girmezler: Ama ihtiyac doğrultusunda buna haklari vardir (Diger Acts.)
- Direk Pazarlamanin Önüne Doğru Şekilde Gecmek: Veri pazarlama (alisveris) amacli kullanilirsa, personel veri islenmesinin sonlandirilmasini isteyebilir.
- Doğru Olarak Otomatik Iliskilendirmek: Personel yalnizca önemli olmayan kararlarin otomatik olarak alinmasini isteyebilir. Ornek olarak, Kredi kullanim talebi. Bu durumda veri sahibi bu talebe otomatik cevap verilmedigininden emin olmalidir.
- Doğrulama, Engelleme, Silme ve Yok Etme: In a court, Veride yanlis birsey varsa silinebilir. 3. Şahıslar bilgilendirilir. Veriye ek olarak doğru bilgilerin girilmesi istenir.

Kayitli, islenmis verilere ek olarak isteklerde bulunulabilir Act. Onlari atladik (burada yazmadik) .

Herhangi biri veri isleme yapiyorsa veri isleme bir yetkili tarafindan kayit altina alinmalidir: this includes describing the measures taken under point 7 of the Privacy Principles (see above).

GERMANY (Almanya)

Almanya Federal Veri Güvenligi Kanunu Kişisel bilginin kullanimini yukardakilere benzer şekilde sinirlar. Kanunlarin amaci Kişisel bilgileri, kullanırken gizliligin bozulmasindan ve bireylere karşı kullanilmasindan korumaktir.

Bilgi toplanmadan once, kullanici veriyi nasil kullanacagini bildirmek zorundadir:

Veri sahibinden kullanim izni ciktigi zaman, Kişi verisinin depolanma amacini bildirmelidir ve alikoymaya izin vermenin sonucunda verinin iletisime açık oldugunu goz önünde bulundurmalidir.Kişiler Özel durumlar olmadikca yazima izin vermelidirler.Eger izin verildiyse, diger yazili açıklamalar ile beraber izinin açıklamasi görünüsde ayirtedilebilir olmalidir. Kişi bazi durumlarda bilgi isteyebilirler.

Veri sahibi bilginin saglanmasini su durumlarda isteyenilir;

1-) Onunla alakali depolanan bilgi, alicinin ya da kokeninin referans icermesini isteyebilir, ve

2-) Depolama amacini bilmek isteyebilir.

3-) Eger veri otomatik olarak isleniyorsa, Kişi ya da gruplar veriden kimin duzenli olarak haberdar oldugunu bilmek isteyebilir.

UK (United Kingdom)daki yasalara benzer olarak, bilgiye sahip olmak isteyen bazi insanlar veri erisimine sahip olabilirler. Ayrica, veriyi güvenli olarak saklamak zorundadirlar. Veri islemede kullanilan Kişiler yetkileri disinda Kişisel veriyi kullanamaz ya da isleyemez. Gorev alan Kişiler, olabildigince gizli gruplar icin calisirlar ve gizliligi sürdürmeyi garantiye almalidirlar. Bu garanti faaliyetin bitisinden sonra da sürdürülmelidir.

Kurumlar ya da Kişiler depolanan gizli bilgiyi, verinin ornegini iceren bildirinin ve verinin depolanmasi ve toplanmasindaki amacin kendileri icin kayit altina almak isteyeceklerdir. Yasalarda otomatik sistemler (Bilgisayarlar) icin verilerin toplanmasi ve depolanmasinda oldukca açık zorunluluklar vardir ;

- YetKişi olmayan Kişilerin veri islem sistemine giris yapmasinin önüne gecmek icin veri girisleri kontrol edilmelidir. (Access Control = Giris Kontrolu)
- Basinin yetKişi disinda, verileri okumasi, kopyalamasi, değiştirmesi ya da silmesi engellenmelidir (Storage Media Control)
- Bellek icine yetKişiz girdiler ve yetKişiz kontroller değişim ya da depolanan Kişisel bilgilerin silinmesin önüne gecilmelidir (Memory Control = Bellek Kontrolu)
- Bilgi taşınması kolayligina yardim ile yetKişiz Kişiler tarafindan kulllaniminin bilgi isleme sistemi tarafindan önüne gecilmesi gerekmektedir (User Control = Kullanici Kontrolu)
- Veri isleme sistemine erisim hakki olmayanlarin önüne gecilmellidir (Access Control = Erisim Kontrolu)
- Gruplarin Kişisel datalarinin taşınmasında ki kolaylikdan dolayi iletisime açık olabilir bu nedenle bunlarin kontrol edilebilir ve ulasilabilir olmasinin önüne gecilmedilir (Communication Control = Iletisim Kontrolu)
- Ne zaman ve kim tarafindan veri isleme sistemi icine girdi yapildigi kontrol edilmeli ve sinirlandirilmadilir (Input Control = Girdi Kontrolu)
- Kişisel datayi yetkili islemleme durumunda, İlkelerin açıklanmasi ile uygunlugu verinin islenmesinde kati bir şekilde belirtilmelidir (Job Control = Is Kontrolu)

- Depolanan araclarin taşınması ya da Kişisel datanin taşınması durumunda verinin yetKişi olmayan Kişiler tarafindan okunmasi, değiştirilmesi, kopyalanmasi ve silinmesin onune gecilmelidir.
- Kuruluslarin ya da Yetkililerin organizasyon icinde duzenlenmesi sirasinda korunan datanin Özel gereksinimi karşılanmak zorundadir (Data Protection = Veri Korunmasi)

Bu kontroller aslinda tamamen uzatılmış ve önemli basari elde etmistir. Bu duzen icinde uygulama, kontrol ve diger aktiviteler icin kurum bir Veri Güvenligi Sorumlusu (Data Protection Officer) bulundurmalidir. Bu sorumlular Şirket yoneticilerine ya da sahibine direk olarak rapor tutmak zorundadir. Bunun icin Şirketde 5 ya da daha fazla personel bulundurulmalidir. Bu düşünce zor gelebilir çünkü pozisyon icin Veri Güvenligi Sorumlusunun ustun niteliklere sahip olmalidir ornek vermek gerekirse, devir alinan gorev basit degildir.

France (Fransa)

Law No. 78/17 (1978) Data Processing, Data Files and Individual Liberties

US

Kişilerin doğru gizlilik İlkesi icin tek bir kanun yoktur. The Privacy Act 1974, bu kanunla federal ya da eyalet hukumetleri sorumluluk almistir. Şirketlerin ve şahıslarin konusu yasamanin (yapilan kanunlarin) cok fazla sayıda olmasidir. Spesifik durumlar icin bu kanunlar oldukca serttir (ornegin 13 yasindan kucuk bir cocuklar) , ama koruma agir basmamaktadir.

- Privacy Act (1974)
- Electronic Communications Privacy Act (1986)
- Computer Matching and Privacy Protection Act (1988)
- Right to Financial Privacy Act (1978)
- Children's Online Privacy Protection Act (1998)
- HIPAA
- SOX

Kişisel bilgileri gizleme

Saldırıya açık olup olmadığınızı anlama (yolları)

Kendinizi Koruma Yolları

- Takip edilmeyin

- E-posta bağlantısı

Ön Belleğe Almak (Caching)

Data taşınmasında kullanici savunmasız olmadiginda da çevresel kullanimi ortulu olarak surekli kontrol etmelidir. Halka açık Internet Kafelerde ya da is yerinden interneti kullanan kullanicilar kendi sistemlerini yapilandiracak kadar yetenekli olmadiklarindan bu tipik bir durum degildir. Ornegin, dosya ya da web sayfasina yapilan basvuru girisleri browsers cachelerde depolanabilir. Daha sonra bu bilgiler Kişitlama olmaksızin geri alinabilir ve erisilebilir.

Saldırıya açık olup olmadığınızı anlama (yolları)

Kendinizi Koruma Yolları

Kredi Kartları

Kredi Kartı sahteciligi (dolandirilicigi) buyuk marketler ile online yapilan alisverislerde ortaya cikabilir. Kredi Kartı Güvenliginde tipik olarak kredi Kartı numarasi, son kullanim tarihi, sahibinin adresi ve kredi Kartının arkasinda yazan CVVden ibarettir. Online Islemlerde (Online Transaction), imza ve kimlik doğrulamasi yapilamaz.

Saldırıya açık olup olmadığınızı anlama (yolları)

- Kredi Kartı numaranizi islem bittikden sonra sakliyormusunuz?
- Kayit altina alinan dosyalar Kredi Kartı numaranizi iceriyor mu?

Kendinizi Koruma Yolları

VISA ve MASTERCARD kredi kartlari iKişi birden hangi bilgilerin yazdirilabilir ve kayit altina alinabilir oldugunu gosterir ornek olarak alisverislerinizde sliplerde Kredi Kartınizin ilk 6 ve son 4 hanesi gorulebilir, son kullanim tarihi vb. seyler gotuntulenemez . Kesinlikle kredi kartı kullanma kilavuzu ve PCI kullanim klavuzunu gozden gecirmeniz onerilir.

E-mail adreslerini gizlemek

Saldırıya açık olup olmadığınızı anlama (yolları)

Kendinizi Koruma Yolları

Arama motorları ve robotlar

İzlemeye engel ol ve robots.txt

Saldırıya açık olup olmadığınızı anlama (yolları)

Kendinizi Koruma Yolları

Doğru cache opsiyonlarını kullan

Saldırıya açık olup olmadıgınızı anlama (yolları)

Kendinizi Koruma Yolları

Kalıcı olmayan cookieler

Kısa zaman aşımını (idle timeout) tartış

Saldırıya açık olup olmadıgınızı anlama (yolları)

Kendinizi Koruma Yolları

GET verisi kullanımını önle

Saldırıya açık olup olmadıgınızı anlama (yolları)

Kendinizi Koruma Yolları

Create a P3P Pact

Saldırıya açık olup olmadıgınızı anlama (yolları)

Kendinizi Koruma Yolları

İleri Okuma

Kriptoğrafi hakkında bilginin bulunabileceği iyi bir SSS

http://www.interhack.net/people/cmcurtin/snake-oil-faq.html

Dökümanın Aslı : OWASP GUIDE 2.0.1

Çeviri **:** Taygun Alban - Taygun.ALBAN@gmail.com