



ESOMAR ONLINE ARAŞTIRMA KILAVUZU

ESOMAR'ın dünya genelindeki tüm araştırma kodları ve kılavuzları güncellenmiş versiyonları ile www.esomar.org adresinde mevcuttur.

ÇEVİRİM İÇİ ARAŞTIRMALAR İÇİN ESOMAR KILAVUZU

Bu kılavuz istek olması durumunda yenilenecektir. Bununla beraber kılavuz web dökümanı olarak diğer Esomar kılavuzları ve yararlı kaynaklar ile aktive bir şekilde bağlantılıdır. Kılavuza çevrimiçi olarak www.esomar.org websitesinden kılavuzlar bölümündeki bilgi ve standartlar butonunu tıklayarak ulaşabilirsiniz.

İÇİNDEKİLER

1. GİRİŞ
 - 1.1 Online araştırmada basilica ilkeler
2. AHLAKİ SORUNLAR
 - 2.1 Kişisel verilerin işlenmesi
 - 2.1.1 Kimlik saptayıcılar
 - 2.2 Bilgilendirme ve Mail
 - 2.2.1 Özel Şartlar
 - 2.3 Gizlilik Politikaları
 - 2.3.1 Tavsiye Edilen İçerik
 - 2.4 Çocuklar ve Gençler
 - 2.4.1 Elde Edilen İzinler
3. MEVZUAAT KONULARI
 - 3.1 Kişisel Veriler ve IP Adresi
 - 3.2 Milli Yargı
 - 3.2.1 Uzak Mesafe Veri Toplama ve Veri Transferi
 - 3.3 Kayıt
 - 3.4 Güvenlik
 - 3.5 Güvenlik Yönetimi
4. ONLİNE TEKNOLOJİLERİ ARAŞTIRMA İÇERİSİNDE KULLANMA
 - 4.1 Araştırmalarda Kullanılan Kimlik Saptama ve İzleme Teknojileri
 - 4.1.1 Özel Teknolojiler
 - 4.1.2 Kimlik Saptama ve İzleme Teknolojiler İçin Kamuyu Aydınlatma
 - 4.2 Araştırma Firmaların Uyarlaması Gereken Uygulamalar
 - 4.3 Kabul Edilemez Uygulamalar
 - 4.4 İnteraktif Mobil Aletler ve Akıllı Telefonlar
 - 4.4.1 İnteraktif Mobil Aletlerin Kullanımı
5. ARAŞTIRMANIN METODUNA YÖNELİK SORUNLAR
 - 5.1 Online Örneklem
 - 5.2 Erişim Paneli
 - 5.3 Teknik Detaylar

6. TANIMLAMALAR VE YARARLI KAYNAKLARA İLİŞKİN BİLGİLER

İlave 1- ICC/Esomar Kodu'nun ana etkenleri
İlave 2- Gizlilik Potikaları Örnekleri

GİRİŞ

Pazar ve Sosyal Araştırmalara yönelik hazırlanan ICC/Esomar Kodu teknolojiden bağımsız online araştırmalarda olduğu gibi diğer veri toplama yöntemlerinde de uygulanabilir. Bundan dolayı, ICC/ESOMAR kodunda bulunan temel öğeler ESOMAR ONLINE ARASTIRMA KILAVUZUNUN ana temelini de oluşturmaktadır.

İnternet araştırmalarında yer alan teknik unsurlar ve yöntemlere ilişkin hususlar 2005 yılında güncellenen kılavuzda aydınlatılmıştır. Uluslararası Yasal İnternet Yönetimi geliştirilmeye devam edilmektedir. Bundan dolayı, online araştırma yöntemleri diğer araştırma yöntemlerine göre daha zayıf hatlarla tanımlanmış yasal çerçeveye sahiptir. Bu durum özellikle birden fazla ülkede gerçekleştirilen araştırmalar için söz konusudur. Kılavuzun amacı ICC/ESOMAR kodunun temel ilkelerini dünya genelindeki güncel yasa ve mevzuatlarına nasıl uyarlanacağını açıklamak ve online araştırmalarda kullanılacak yeni teknolojilerde yasal ve ahlaki olarak uyulması gereken hususların altını çizmektir.

ESOMAR Pazar Araştırmaları ile pazarlama arasındaki ayrımın vurgulanmasına önem vermektedir. Pazar araştırmaları ticari bir iletişim yöntemi değildir ve dünya genelinde daha az kısıtlayıcı bir yasal düzenlemeye sahiptir. Pazarlama ile Pazar araştırmaları arasındaki fark kolay bir şekilde açıklanabilir: Pazar araştırmalarında toplanan veri sadece araştırma amaçlı kullanılır ve pazarlama amaçlı doğrudan ifşa edilmez. (Bakınız ESOMAR KILAVUZ_ Pazar araştırmalarını diğer veri toplama yöntemlerinden ayıran özellikler)

ESOMAR öncelikle CASRO ile yakın bir çalışma yapmıştır. Kılavuzun Araştırmada teknolojilerin kullanımına ilişkin bölümü CASRO kılavuzu baz alınarak sıralanmış ve yapılmıştır.

Bu Belgenin geliştirilmesi üzerinde halen çalışılmaktadır. Kılavuz 5.2'de yer alan erişim paneli ilk yayınlanan haliyle aynıdır, fakat yakın bir zaman içerisinde yenilenecektir. Bunun yanı sıra, diğer ilgili konulara ilişkin de kılavuz hazırlanması amaçlanmaktadır.

1.1 ONLİNE ARAŞTIRMALARDA ONCELİKLI İLKELE

Online araştırmalarda araştırmacılara yol gösteren 3 temel ilke bulunmaktadır.

İLK OLARAK- Deneklere (Ya da araştırmaya katılmayı düşünen bireylere) saygı duyulmalıdır. Online araştırmada yer alacak kişinin yaşayacağı deneyimin iyi olacağı konusunda emin olması sağlanmalı ve katılımcı ile karşılıklı güven ve saygıya dayalı bir iletişim kurulmalıdır.

İKİNCİ OLARAK- Araştırmacılar müşterilerin endişelerine karşı duyarlı olmalı ve pazar araştırmalarında başarılı olunmasının ana koşulunun halkın güveninin kazanılması olduğunu unutmamalıdır. Araştırmacılar pazar araştırmaları sektörüne karşı halkın güvenini yok edecek teknoloji ve aktivitelerden sakınmalıdırlar.

ÜÇÜNCÜ OLARAK- Araştırmacılar, araştırmaya ile direkt pazarlama ve reklam arasındaki fark korunmaya özen göstermelidirler. Görüşme tekniği gibi araştırma tekniklerinin araştırma amacı dışında kullanıldığı aktivitelerde yer aldıklarında bu faaliyetleri Pazar, sosyal ya da fikir araştırması olarak tanımlamamalıdırlar.

Bunlara ek olarak araştırmacılar Pazar ve sosyal araştırmalarda ICC/ESOMAR Uluslararası Kodu'nun 7C Makelesinde belirtilen Veri Koruma Şartlarına sadık kalmalıdırlar. Aşağıdaki gibidir,

- Kodda belirtilen noktalara göre toplanan ve saklanan veriler
- Sadece araştırma amacı ile kullanılmalı, başka amaçlar için kullanılmamalıdır.
- Araştırmanın amacı ile ilgili olmayan yada araştırmanın amacını aşan bilgi toplanmamalı ve işlenmemelidir.
- Araştırma amaçlı toplanan ya da işlenen veri gerekenden daha fazla saklanmamalıdır.

Araştırmacılar ulusal idarelerin aşağıda belirtilen mevzuatları doğrultusunda deneklerin saptanabilir kişisel bilgilerine yönelik görüşme gerçekleştirebilirler.

- I. Denekler belirgin ve net bir şekilde bu konuda isteklerini belirtmişlerse
- II. Deneklerin açık ve net bir onay söz konusuysa
- III. Deneklerin bilgileri ICC/ESOMAR Pazar ve Sosyal Araştırmalar Kodu Makale 1D'de tanımlanan ticari aktivitelerle direkt bir bağlantı içerisinde olmayacaksa

2-AHLAKİ SORUNLAR

2.1 KİŞİSEL VERİLERİN KULLANILMASI

Deneklerden toplanan veriler gizlidir ve deneklerin kimliği saklanmalıdır. Deneklerin kimliği, onayları olmadan yayınlanmalıdır. ICC/ESOMAR Uluslararası Kodu 7.Makalede belirtilen faaliyetlerde kullanılmalı, sadece araştırma amaçlı kullanıldığının garantisi verilmelidir. Katılımcının kişisel bilgilerinin saptanabileceği bilgiler, direkt pazarlama, liste hazırlama, finansal kaynak toplama gibi araştırma amacı taşımayan pazarlama aktivitelerinde yer almamalıdır. (Bakınız ICC/ESOMAR Uluslararası Kodu 1.Makale Notları)

2.1.1 KİMLİK SAPTAYICILAR

Deneklerin mail adresi ya da diğer kimlik saptayıcılar (internet /bilgisayardaki kullanıcı adları yada deneğin kimliğini ortaya çıkarabilecek diğer bilgiler) kişisel veri olarak tanımlanır ve diğer kimlik saptayıcılar gibi korunması gerekmektedir.

Bireylerin kimliklerini ifşa edebilecek tüm veriler veri kayıtlarından çıkarılmalıdır (kimlik bilgileriyle bağlantısı olan seri numaraları da dahil olmak üzere) Kisisel bilgilerin yer almadığı veriler veri koruma kanununa yönelik bir kısıtlamaya maruz kalmaz.

2.2 BİLGİLENDİRME VE MAIL

Araştırmacılar deneklerin gizlilik konusundaki endişelerine özen göstermeli ve potansiyel deneklerin mail adreslerini kendi rızaları olmadan buldukları ülkenin kanunları izin verse dahi, deneklerin onayını almalıdırlar. Bununla beraber makul sebeplerin olması durumunda deneklerle irtibata geçilebilir.

Araştırmacılar deneklere mail gönderirken araştırma ve amacına ait ön bir bilgi yazarak, rahatsızlık yaratması olası durumları azaltabilirler. Yukarıda belirtilen koşullar diğer elektronik mesajlar için de geçerlidir (Acil mesajlar, SMS gibi..) Bakınız İnteraktif mobil iletişim bölüm 4

2.2.1 ÖZEL KOŞULLAR

Araştırmacıların deneklerin mail adreslerini müşterileriyle ya da iş yerlerine yönelik araştırmalar kapsamında deneğin izni olmadan paylaşmaları genel pazar araştırma prensiplerine aykırıdır.

- I. Araştırmacılarından mail aracılığıyla görüştüğü kişilere makul bir sebepten dolayı kendileriyle iletişime geçildiğini açıklaması beklenmektedir. Bu anlaşmada aşağıda belirtilen tüm koşulların yer aldığı ön görülmektedir.

Araştırma organizasyonu, müşteriler ve gorusulecek kisilerin listesini hazırlayan kurumlar ile bireyler arasında geçmişe dayalı bir iletişimin olması gerekir . Bu araştırma örnekleminin yapılması için de gereklidir (İkincisi bu şekilde tespit edilmektedir)

- II. Araştırma kapsamında gorusulecek bireylerle geçmişe dayalı ilişkiden kaynaklanan geçerli bir sebep varsa iletişim kurulabilir.
- III. Bireyler açık ve net bir şekilde gönderilen her araştırma davetinde ilerki dönemlerde kurulacak elektronik iletişimden ayrılma teklifi sunulmalı
- IV. Davet listesi daha önce araştırmaya katılmaya uygun bulunmuş ama listeyi hazırlayan kuruma listeden çıkarılma talebini iletmemiş kişileri kapsamamalıdır.

Araştırmacılar potansiyel deneklerin elektronik adresleri kaçak yollardan temin etmemeli, kamu alanları , diğer aktivitelerde yer alan bilgiler aracılığıyla ya da teknoloji kullanımıyla mail adreslerini toplamamalıdır.

Denekler, ilerki dönemlerde iletişim kurmak için araştırma organizasyonun internet adresini talep ederlerse, Araştırmacılar doğru mail adresini vermekle yükümlüdürler .

İşyerleri ile yapılan araştırmalarda mail ile gönderilen anket davetlerinde yukarıda belirtilen 3. Ve 4. Kısımına ilaveten mail ya da internet servis sağlayıcılarının anti-virus programlarını da uygulamalıdır. Bu koşul kamu alanlarında e-mail adresi yayınlanmış profesyoneller için de geçerlidir, doctor-avukat gibi...

Araştırmacılar müşterilerinden ya da katılımcıların listesini hazırlayan kurumlardan mail listesini aldıklarında onlardan (musteri ve liste hazırlayıcılar) sürekliliği olan ve mail temin etme nedenlerini akılcı bir şekilde açıklayan yazılı bir form almalıdırlar.

Katılımcıların kişisel bilgilerine ulaşılmasına onay verme durumunu gösteren belgenin kopyasının saklanması araştırmacıların yararına olacaktır. Bu durum bazı ülkelerde yasal bir gerekliliktir. Örneğin: Avrupa Birliği Ülkeleri, Arjantin, Avustralya, Kanada, Yeni Zellanda ve Amerika Birlesik Devletleri ve Amerika- Avrupa Birliği Guvenlik Limani çerçevesinde yer alan sirketler...

2.3 Gizlilik Politikası

Araştırmacılar gizlilik politikası bildirimlerini kendi internet sitelerinde yayınlamalıdırlar. Bu bildirim anlaşılabilir, öz ve dikkat çekici olmalıdır.

2.3.1 Tavsiye Edilen İçerik

Bu gizlilik politikası, deneklerin kişisel bilgilerin kullanıldığı tüm çevrimici araştırmalarla link halinde olmalı. Böylece katılımcılar bilgilendirilebilir ve 3. Kişilerin bu bilgilere ulaşması durumunda bilgiler koruma altına alınabilir. Bu öğeler tüm araştırmalar için standart olmalıdır. Diğer yaklaşımlar örnekleme yöntemine göre değişim gösterecektir. Bazı özel araştırmalarda araştırmaya katılma davetinde veri gizliliğine ilişkin bilgilerin gizlilik politikası uygulamalarında genel beyanlara ilaveten ön açıklama olarak yer alması gerekebilir.

Veri Gizlilik bildiriminde kelime ve ifade sirasi tercihe bağlıdır. ESOMAR, firmalara 3 aşamalı veri gizliliği bildirisini kullanmalarını tavsiye eder. Birinci basamak gizlilik politikası hakkında özet bilgi sunarken, 2. Basamak pazarlama araştırmalarına ve gizlilik uygulamalarına ilişkin kısa bir genel bakış sunmalıdır. 3. Basamak ise firmanın gizlilik politikalarına ait kapsamlı bir bilgi vermelidir. İlaveler 2 Aşamalı veri gizliliği bildirimine örnektir.

A- Tüm Gizlilik Bildirimlerinde Bulunacak Standart Ogeler

Araştırma yapanın kim olduğunu açıklayan bildirim. Bu bildirim daha detaylı bilgi sunumu için firmanın internet sayfasına bağlantı içermelidir.

Kimin İçin: Tüm araştırmalar araştırmanın yapıldığı firma ve organizasyonu tanıtan açıklamayı içermelidir, açıklamanın yer almamasını gerektiren gerekceli bir neden olmadığı sürece. Eğer araştırma şirketi veri toplama hizmeti sunan bir firmaysa , kişisel verilerin gönderildiği firmanın kimlik ve iletişim bilgileri ve buna bağlı olarak

“ Avrupa birliğinde kullanılan terminolojiyle “Veri Kontrolcu” bilgileri tedarik edilmelidir. Bu konuyla ilgili daha detaylı bilgiye ICC/ESOMAR Uluslararası Kodu Makale 4’te bildirim nasıl uygulanacağını anlatan bölümden ulaşabilirsiniz.

Bireysel katılımcıların kimlikleri ve cevapları her koşulda gizli bilgi olarak ele alınacağı ve sadece araştırma amaçlı kullanılacağı garanti edilmelidir. Katılımcıların kimlikleri ve cevapları 3. Kisilerle paylaşılması katılımcı tarafından onaylanmadığı ve talep edilmediği sürece 3. Sahıslara iletilemez.

Deneklerin işbirliğini elde ederken denekler, araştırmanın yapısı ve bulguların kullanımını konusunda yanlış yönlendirilmeyecek.

Tüm Pazar, sosyal ve fikir araştırmalarında deneklerin işbirliği gönüllüdür. Deneklerin kişisel bilgileri kendilerinin onayı ya da bilgisi olmadan araştırılmayacaktır.

Denekler, görüşmenin herhangi bir aşamasında görüşmeyi sonlandırmak ya da sonrasında görüşme kaydının silinmesini talep etme hakkına sahiptirler. Mantıklı ve uygulanması mümkün talepler uygulanacaktır.

Kimlik Tespiti ve Teknoloji İzleme:

Araştırmanın uygulanmasında kullanılan tüm teknolojilere ilişkin açıklayıcı bildiri. Deneğin makinasına ya da bilgisayarına indirilebilecek özel bir yazılım sayesinde internet araştırmaları kapsamında deneğin bilgisi olmadan browser türü, kullanıcı adı ve bilgisayar kimliği gibi bilgileri saptanabilir. Araştırma organizasyonu tarafından yapılacak beyan acık bir şekilde görüşme sırasında hangi bilgilerin saptandığını belirtmelidir (izleme amaçlı toplanan ve tarayıcıya uygunluğu optimize edilen veriler) ya da araştırmanın yönetsel raporunun bir parçası olarak tutulan başka bir rapor varsa, bu da beyanın içerisinde yer almalıdır.

Tanımlama Bilgileri: Bu tanımlama bilgileri kullanıldığı zaman, bunu açıklayan anlaşılabilir bir beyan yapılmalıdır. Örneğin “ Biz tanımlama bilgileri ya da benzer araçları yedek olarak, sadece kalite kontrol, doğrulama ve araştırma tekrarının yaratacağı rahatsızlığı engellemek amacıyla kullanıyoruz.” Tanımlama bilgileri kullanıldığı zaman deneklere bilgisayarlarının kabul ettiği tanımlama bilgilerini kontrol etme olanağı sağlayan hatırlatıcıları kullanmamaları tavsiye edilir. Web tarayıcısına tanımlama bilgilerinin yerleşmesi durumunda araştırmacıları ikaz edecek şekilde yapılandırıldığının garantisi deneklere verilmelidir. Ayrıca tarayıcıların ayarları tüm tanımlama bilgilerini silecek şekilde düzenlenbilir.

Çocuklar: Çocuklarla yapılacak görüşmelerin nasıl yapılacağına dair açık bir biliri sunulmalıdır. Örneğin: “Çocuklarla yapılan arařtırmalarda ebeveynlerden, yasal koruyuculardan görüşmeye başlamadan önce kanıtlanabilir onay alınır.”

Bize Ulaşmak İçin: Deneklerin arařtırmaya ilişkin endişeleri konuşmak ve sorularına cevap vermek amacıyla posta, mail adresleri ya da ücretsiz arama yapabilecekleri telefon numaraları verilecektir.

Güvenlik Önlemleri:

İnternet sitemizde verdiğimiz bilgilerin değİstirilme, suistimal edilme ve kaybolma durumlarına karşı korumak için güvenlik önlemleri yer almaktadır. Sadece yetkilendirilmiş çalışanlarımız veri kontrolü ve analizi amaçlı bu verilere ulaşabilirler. Kişisel verilerin 3. Partilere transfer edilmesi durumunda, bu güvenlik önlemlerinin tüm çalışanlar için aynı düzeyde uygulanacağını garanti ederiz.

İstenmeyen Mail: İstenmeyen mail gönderilmeyeceğini ya da bu amaçla baskalarına verilmeyeceğine ilişkin açıklama

Kişisel Bilgilere Ulaşma: Bilgilere nasıl ulaşılacağı ve gerekli olma durumunda bilgiyi düzeltme

Veri Nerede Tutuluyor ve Nerede İşleniyor: Birçok firma uluslararası olarak çalışıyor, bu sebeble verilerin toplanması ve işlenmesi farklı ülkelerde yapıyor olabilir.

Kayıtlı Adres: Organizasyonun resmi adresi

Yönetmenliğin En Son Güncellendiği Tarih:

3 İLAVE UNSUR POTANSİYEL DENEKLERLE İLETİŞİMDE KULLANILAN YÖNTEMLERE BAĞLI OLARAK YER ALMALIDIR

- I. Deneklerin araştırma amaçlı davet edildikleri yer

Kayıt İşlemleri: Kayıt işlem tanımları

Panel Veritabanı: Arařtırmaya katılan kişilerin bilgilerinin tutulduğu yer tanımlanmalı, panel yönetimi, kontrolü ve örnekleme seçimi ile güncellenme işlemi, bilgilerin ya da kişisel tanımlayıcıların silinmesi

İletişim Kurma Sıklığı: Katılımcıların yer aldıkları arařtırmaya dair gösterge, Ne sıklıkta, ne kadar süre gibi...

Parola Tanımlama Sistemi: Kullanılması durumunda, nasıl kullanıldığı ve sağladığı güvenlik önlemleri

Sisteme Giriş ve Çıkış: Sisteme giriş ve çıkış yönetmeliği araştırmadan çok iletişime yöneliktir. Panellerin devamı ya da ödül düzeneği gibi..Hangi iletişim yönteminin kullanılacağı, hangisinin daha opsiyonel olduğu ve 3.partiler adına gerçekleşmesi olası olan görüşmeler belirtilmeli.

Ödül: Ödül planı ve kontrakt için geçerli olan esaslar açıklanmalı

- II. Deneklere araştırmaya katılma daveti göndermek için mail adreslerinin temin edildikleri yer

Bilgi Kaynağı: Mail adreslerinin temin edildikleri yer açık bir şekilde belirtilmelidir ya da bu açıklama araştırmanın içerisinde verilen bilginin içerisinde yer almalıdır. Mail adresini tedarik edenlerin, araştırmacıların listede yer alan bireylerle mail aracılığıyla görüşme yapılmasını onayladığı doğrulanmalıdır.

Virus: Araştırmaya katılmak isteyen kişilere bilgileri dahilinde olmadan gönderilen mail. Araştırmacılar ilerki süreçlerde araştırmada yer almak istemeyen kişilerin isimlerinin listeden çıkartabilecek bir mekanizmaya sahip olmalı ve mail listesi tedarikçileri bu konuda bilgilendirilmelidirler.

Parola Tanıma Sistemi: Kullanılması durumunda nasıl çalıştığı ve sağladığı güvenlik önlemleri açıklanmalı

Görüşmeye Başlama ve Bitirme İşlemleri: Eger mümkünse nasıl yapılacağını ve kullanılması için saklanacak bilgiler açıklanmalı

- III. **Araştırma Kesişimi :** İnternet sitesi ziyaretçilerinin örnekleme ya da başka tekniklerle deneklerin seçildiği yer

Denek bulma yöntem ve tekniklerini açıkla;tesadüfi seçme gibi...

Parola Tanıma Sistemi: Kullanılması durumunda nasıl çalıştığı ve sağladığı güvenlik önlemleri açıklanmalı

Görüşmeye Başlama ve Bitirme İşlemleri: Eger mümkünse nasıl yapılacağını ve kullanılması için saklanacak bilgiler açıklanmalı

Görünmez İşlemler: Denek bulmada herhangi bir gizli işlem ya da deneği başka tarafa yönlendirecek bir uygulama kullanıldıysa nasıl yapıldığı anlatılmalı

2.4 Çocuklar ve Gençler

Araştırmacılar ebeveynlerin müşteri gruplarının ve yasa koyucuların çocukların ve gençlerin internette kötü amaçlı çıkarlar doğrultusunda kullanılması olasılığına karşın hassas olmalılar. Çocuk ve gençlerin kimliklerinin internet ortamında tanınması olasılığı olmasa bile çocukları araştırmaya davet ederken için yasal koruyuculardan tüm kanıtlanabilir ve kesin izinler alındıması için tüm gerekli adımlar atılmalı ve bunun garantisi verilmelidir.

2.5 İzin Alınması

Araştırmacılar çocuk ve gençlerle ilgili tüm kanun ve yasa tanımlamasının ülkeden ülkeye değiştiğini göz önünde bulundurmalıdırlar. Ulusal bir tanımlamanın olmadığı bölgelerde ESOMAR kılavuzu Çocuk ve Gençlerle yapılan anket görüşmelerinde 14 yaş altının "Çocuk", 14 ile 17 arasındakilerin "Genç" olarak kabul edilmesini tavsiye eder. Çünkü Pazar araştırmaları sosyal bilimler içerisindedir; fiziksel ve zihinsel gelişimin farklı aşamalarını kabul eder.

Çocuklar için internet üzeri hazırlanan soru formlarında kişisel bilgiler istenilmeden önce Çocugun yaşı sorulmalıdır. Eğer çocuğun yaşı ulusal olarak belirlenen yaş sınırının altında ise ve onaylanmış bir izin alınmamışsa, sonrasındaki soruları cevaplandırması için herhangi bir davet gönderilmemelidir. Bu konuda yapılacak bildiri açıklayıcı ve belirgin olmalı, kanunun ve alınan izinin nerede kullanılacağı belirtilmelidir. Ebeveynlerden izin isteği formu araştırmacıların internet sitesinde yer almalı ya da ebeveynlere mail olarak gönderilmelidir.

Çocuklardan toplanan veriler sadece araştırma amaçlı kullanılacak, başka bir amaçla kullanılmayacaktır. Ebeveynlerden mail ya da başka yollarla alınan izin, ilgili kanun ve kodlara uygun olmalıdır.

Araştırma organizasyonu, ebeveynlerin çocuklarıyla mail, mektup ya da telefon ile irtibata geçilmesini kabul ettiğini doğrulamak için gerekli adımları atmalıdır. Örneğin, çocuklardan ailelerin iletişim bilgilerinin istenmesi ailelerden izin alınabilmesini sağlar.

Öncelikli parental izne gerek duyulmaktadır.

- Ebeveynlerden mail adresi yalnızca veri toplamaya dair bilgilendirme ve izin almak için istenmeli
- Öncelikle çocuğun yaşı araştırma kapsamına alma ya da araştırma kapsamından çıkarma kararını vermek için toplanmalı. Yaş elemesi sonrasında

çocugun yaşı araştırma için uygun bulunursa, ebeveynlerden ankete devam etmek için izin alınmasına başlanabilir.

Araştırmaya katılan deneklerin katılımlarından dolayı herhangi bir zarara uğramayacakları garanti edilmeli ve tüm gerekli önlemler alınmalıdır. Mümkün olduğu sürece hassas konulara ilişkin çocuklara ve gençlere soru sorulmamalıdır.

Diğer kişilere ilişkin bilgiler çocuklardan toplanamamalıdır. Araştırmacılar devamlılığı olan araştırmalar için çocuklarla çalışmanın zorluklarını göz önünde bulundurmalılar.

- Uygun yaşta olan çocuklarla birlikte ebeveynlerin secilmesi ve araştırmanın ondan sonra yönetilmeye başlanması; araştırma aktivitelerini, ailelerin onayı ve işbirliği ile gerçekleştirmek. Ayrıca ailelerin etkinliklerini izlemesini sağlamak
- Araştırmaya sadece ailelerin bildiği parola sistemi ile girilmesi, çocukların araştırmaya başlamadan önce ailelerin onayını alması gerekliliğini sağlayacaktır.

Where necessary, researchers should consult their national research association or the Esomar guideline for advice

3- MEVZUAT SORUNLARI

3.1 Kişisel Veri ve IP Adresi

Veri gizliliği yönetmeliği sadece kimliği saptanabilir veriler üzerinde uygulanabilir, bireylerin kimliliğinin bilinmesinin mümkün olmadığı veriler için geçerli değildir. Kurallara bağlı olarak kişilerin kendi isimleri ile kayıt edilen verilere ulaşma ve yanlış bir bilgiyi düzeltme hakları vardır. Bu erişim hakkı kişisel kimlik saptama öğeleri veri kümesinden çıkarıldıktan sonra uygulanamaz.

Veri kümesine dahil öğeler; isim, mail adresleri ve telefon numarası kişisel verileri oluşturabilir. Coğrafi konumu ya da posta kodu veri kümesinde diğer bilgilerle birleştirilebilir. Araştırmacılar veri kümesinin araştırma amaçlı toplandığına emin olmalılar. Kişisel veriler güvenli bir şekilde muhafaza edilir ve sadece araştırma amaçlı kullanılır.

IP adresinin internetle direkt linkle bağlantılı olması gereklidir ve bu IP adresi düzenli olarak sunucular üzerinden çalışan yazılım ve internet siteleri ile internete bağlı olan kişisel bilgisayarlar tarafından yakalanırlar. Genel olarak, kullanıcılar IP adreslerinin

ele geçirilmesini engelleme imkanına sahip değildir. IP adresi kimliği saptanabilen veriler ile kişisel verilerin kombinasyonundan oluşabilir, fakat IP adresi konusunda fikir birliğine varılmış uluslararası bir IP Adresi statusü yoktur.

3.2 Ulusal Yargı

ICC/Esomar uluslararası kodu spesifik pazarda geçerli olan yasa kanunları ve kurallara dayalı olarak uygulanır. Bununla beraber veri gizliliği için istenen şartlar ve sorumluluklar uluslararası düzeyde tanımlanmıştır.

ESOMAR, deneklerin bakış açısının göz önünde bulundurulmasını tavsiye eder. Ankete katılan denekler kendi ülkesindeki yasal şartların geçerli olacağını varsayabilir. Araştırmaya katılan tüm deneklerin yaşadığı ülkenin bilinmesi ve Avrupa Birliğine bağlı ülkelerin farklı koşulları olduğu göz önüne alındığında yasal şartları takip etmek mümkün olacaktır. Örneğin, Almanya ve İtalya diğer Avrupa ülkelerine göre daha katı kural ve uygulamalara sahiptir.

3.1.1 Uzaktan Veri Toplama ve Veri Transferi

Araştırmacılar, araştırma yapılacak ülkeleri netleştirmelidirler, Özellikle başka ülkelerde araştırma yaptıkları zaman. İnternet üzerinde ve soru formunda kullanılan dil, araştırma yapılması hedeflenen ülkenin belirlenmesinde önemli rol oynar. Bu unsurlar, araştırma firmasının kurulduğu ya da bulunduğu ülkenin yönetmeliklerine uyumlu olan gizlilik politikası içinde de belirlenir. Denekler, toplanan verilerin hangi kanunlara bağlı olarak toplandığını araştırmanın ön sayfasındaki izin formunda yer alan bilgi ile öğrenebilmelidir. Bu ayrıca, denegın yaşadığı ülkenin koşullarını da ortaya çıkaracaktır, mesela dünya genelinde yapılan müşteri memnuniyeti araştırmalarında araştırmaya katılan denekler farklı ülkelerde yaşıyor olabilirler. Panellerde, katılımcıları, kayıt ve gizlilik politikalarını etkileyen kanunlara ilişkin bilgilendirmek yasal bir uygulamadır.

Avrupa Birliğinden, ESOMAR araştırmalarında toplanan verilerin (veri kontrolcü) firmanın bulunduğu ülkenin kanunlarına uyumlu olması, eğer araştırma birden fazla ülkede gerçekleştiriliyorsa, araştırmanın yapıldığı ülkelerin kurallarına uygunluğunu şart koşar. Avrupa Birliği kanunları halen oluşturulma aşamasında olduğundan, ESOMAR gelişmeleri izlemektedir.

Veriler toplandığı ülkeden 3. Ülkeye transfer edilmeden önce, araştırmacılar veri transferinin yasal olduğuna emin olmalılar. Bireylerin veri koruma haklarının sürdürülebilmesi için tüm güvenlik önlemleri alınmalı. Bu durum uzak bölgelerden veri toplama aşamasında uygulanması gerekir ya da bu uluslararası "bulut" olarak işlem görür.

Araştırmacılar bu işlemi kendi gizlilik politikalarının kapsamında belirtmeli (bakınız gizlilik politikaları için önerilen içerik ve gizlilik politikası örneği). Veri aktarımı için bireylerin izni istenmeli ve gerekli önlemler alınmalıdır.

Avrupa Birliği ülkelerinden, Avrupa Birliğine üye olmayan ülkelere veri transferi yapıldığında standart sözleşme maddelerinin kullanımı, koruma önlemlerini sağlayacağından tavsiye edilir, Örneğin Avrupa Komisyonu ve ICC tarafından geliştirilen standartlar.

3.3 Kayıt

Veri koruma yönetmeliklerinin olduğu ülkelerde , veri kontrolcülerinin yetkili makamlara kayıt olması gerekmektedir. Araştırmacıların etkinliklerini yetkili makamlara bildirmeleri ve kayıt etmeleri gerekir. Bu işlem, özellikle Almanya, İngiltere, ABD gibi veri koruma yasalarının etkili olduğu ülkeler için tavsiye edilir (bakınız bölüm 6)

3.4 Güvenlik

Araştırmacılar ve onlara bağlı organizasyonlar kişisel verileri toplarken, üst seviyede güvenliği saptalayabilmek için gerekli önlemleri almalı, özellikle veri koruma yönetmeliğine göre hassas olarak sınıflandırılan veriler için çok dikkatli olunmalıdır (bakınız bölüm 6)

Araştırmacılar müşterilerine sundukları gizli bilgilerin izinsiz erişime karşı korunduğuna emin olmak için gerekli önlemleri almalıdırlar (güvenlik duvarı, pano kontrolü gibi...)

Müşteriler, gizli bilgilerin internet araştırmaları kapsamında yayınlanmasının potansiyel riskleri konusunda uyarılmalı ve bu konuda sıkı güvenlik önlemleri uygulamaları istenmelidir. Kavram ve fikirler tek başına teknolojik araçlar ile güvenlik altına alınamaz, özellikle ifadeler yayıldıktan sonra. Ifşa edilmiş anlaşmalarla korunsun bile, kolay bir şekilde başkalarına gönderilebilir ve açığa çıkması durumunda geri dondurmeye imkansız olabilir.

3.4.1 Güvenlik Yönetimi

Araştırmacılar toplanan, web site ya da sunucuda saklanan kişisel verileri korumak için SSL (Güvenli Priz Tabakası) ya da onun denkleminde olan bir şifreleme sistemi kullanılmalıdır. İlgili ulusal yasa gerektiyorsa, "istirahat veri" -gecici modda bulunan ve ağ içerisinde her iki yöne hareket eden veri dışında, depoda tutulan tüm veriler "istirahat " olarak tanımlanır- için diğer şifrelemelere denk olacak bir düzeyde şifreleme sistemi kullanılmalıdır.

Veri güvenliđi, veri aktarımı da dahil olmak üzere yetkisiz erişim ve kişisel verilerin acıklanmasının manipule edilmesinde önemlidir.

Araştırmacı veri güvenliđini yönetmek için belirgin politika ve prosedürlere sahip olmalıdır. Verilere erişim kısıtlanmalı ve sadece ihtiyaç temelli olarak izin verilmelidir.

Araştırmacılar önemli veriler ile çalışan yöneticiler ya da kilit personelin ICC/ESOMAR koda bağlı kalacaklarını beyan ettiklerinden ve kişisel bilgileri ifşa etmeyeceklerinden emin olmalıdırlar.

Eđer taşıeron firma ya da servis sağlayıcı tarafından işletilen sunucu üzerinde geçici bir bilgi saklanıyorsa, araştırmacı veri saklanması ya da aktarımı sırasında yaşanması muhtemel izinsiz bir erişime engel olmak için, taşıeron firma sözleşmeye bağlı olarak yükümlülük almalıdır. Servis sağlayıcı tarafından tutulan kimliđi saptanabilecek veri mümkün olan en kısa zamanda silinmelidir.

4-ÇEVİRİMİÇİ KİMLİK SAPTAMA VE İZLEME TEKNOLOJİLERİN ARAŞTIRMADA KULLANIMI

Çevrimici kimlik saptama ve izleme teknolojileri hızlı bir gelişim göstermektedir. Pek çok teknoloji kullanıcının bilgisayar deneyimini geliştirmek için dizayn edilmiş, fakat bu arada, bireylerin internet üzerindeki davranış ve hareketlerinin kendi bilgileri dışında diğer bireyler ya da potansiyel organizasyonlar tarafından yakın incelemeye alınmasının yolunu da açmıştır.

Çevrimici kimlik saptama ve izleme teknolojileri pazar, sosyal ve fikir araştırmalarında panel doğruluğu, örnekleme tekniklerinde ilerlemeyi sağlamak amacıyla geliştirilmiştir. Çünkü araştırmacılar ve denekler çevrimiçi iletişim içerisindediler.

ESOMAR, CASRO ile yakın işbirliği içerisindedir. Uluslararası araştırma sektörü pazar, sosyal ve fikir araştırmalarında online teknolojilerin kullanılmasına ilişkin belirgin bir kılavuz oluşturmuştur. Bunu yaparak, profesyonel standartlar, en iyi uygulamalar ve deneklerle saygılı bir ilişki kurulmasını hedeflemektedir.

4.1 Pazar, Sosyal ve Fikir Araştırmalarında Kullanılacak Kimlik Saptama ve İzleme Teknolojileri

Kimlik belirleme ve izleme teknolojileri denekler ya da deneklerin etkinliklerini tanımlamak, doğrulamak ve izlemek için kullanılır. Bu teknolojilerin kullanımı; izleme, araştırma, kota kontrolü ve sahteciliği önlemeyi ve davranış araştırmalarını da içerir. Casus yazılım ve kötü amaçlı yazılım terimi kimlik saptama ve online izleme teknolojilerinin onaylanamaz kullanımını tanımlarken kullanılır. Pazar, sosyal ve fikir araştırmalarında casus veya kötü amaçlı yazılım olarak tanımlanan teknolojiler kullanılmaz. Bu bölüm, onaylanabilir ve onaylanamaz teknoloji kullanımı düzenlerken, aynı zamanda özel teknoloji biçimleri için de kılavuzluk eder.

4.1.1 Özel Teknolojiler

Araştırma tanıma ve izleme teknolojileri şunlardır:

Tanımlama Bilgileri

Tanımlama Bilgileri, numaralı kullanıcı ID'lerin website tarafından bilgisayarda saklandığı küçük metin dosyalarıdır ve bireylerin internet taramalarına ilişkin kesin bilgileri saklar. Tanımlama Bilgileri deneklerin geçmişteki araştırmalarda bulunma

durumunda onları tanımaya yardımcı olur. Tanımlama bilgileri içerisinde tutulan veri kişiselleştirilemez ve tarayıcı ayarlarından çıkartılıp, silinmelidir.

Araştırmacılar tanımlama bilgilerini kullanıyorlarsa, neden kullandıklarına dair kısa, belirgin ve dikkat çekici bilgiyi sunmak zorundadırlar. Tanımlama bilgilerinin kullanılması durumunda, araştırmacılar veri toplama tanımının araştırma firmasının gizlilik politikaları içerisinde tamamen ifsa edildigine emin olmalıdırlar.

2009 yılında yürürlüğe geçen Avrupa Birliği mevzuatı 2011 yılında ulusal mevzuata çevrilmiştir, bu mevzuat tanımlama bilgilerinin sadece kullanıcının onayının alındığının belirgin ve detaylı olarak gösterilmesi durumunda saklanabileceğın ya da tanımlama bilgilerine erişilebileceğini belirtmektedir.

Servisi sağlamak için tanımlama bilgilerinin kesin olarak kullanılmasını gerektiren istisna durumlar olmaktadır. Bu durumda, tanımlama bilgilerinin kendi internet sitelerinin kullanıcılarının bilgilerini depolama ve erişim amaçlı kullanılacağı açık ve kapsamlı bir açıklama ile belirtilmelidir ve son olarak bu bilgilere ulaşma ve depolama işlemlerini reddetme hakkı deneye sunulmalıdır. Avrupa Birliğine bağlı ülkelerde araştırma gerçekleştiren araştırmacılar ulusal mevzuatların izin gerekliliğı olması durumunda güncellemelere ilişkin konsultasyon yapmalıdırlar.

Panel verisi toplayan araştırmacılar ve internet ortamındaki deneklerin davranışlarını inceleyenler, bunları gizlilik politikaları içerisinde belirtmelidirler (bakınız panel data bölümü). Bununla beraber panele kayıt sırasında, bilgileri alınan deneklerin kafasında herhangi bir soru işareti kalmaması için bu etkinliğe ilişkin açıklama yapılmalıdır.

FLAŞ TANIMLAMA BİLGİLERİ

Flash tanımlama bilgileri Adobe Flash Media Player'ın kodundan örnek alınarak oluşturulan bir uygulamadır ve çoğunlukla animasyon ve videoların yer aldığı ticari sitelerin büyük bir çoğunluğu tarafından kullanılmaktadır.

Araştırma tekniğı olarak kullanılması durumunda, araştırmacıların bu bilgiyi kullanma nedenlerini ifşa etmeleri ve nasıl çıkarılacağını gizlilik politikalarında anlatmaları gerekir (bakınız gizlilik politikaları kılavuzu) ve ayrıca katılımcıların izni aranmalıdır. Bunlara ek olarak, diğer yeni teknikler geliştirilmeye devam edilmektedir, örneğın HTML5 gibi yerel depolama özellikleri olanlar kolay bir şekilde silinemez.

Makine ID (Dijital Parmakizi ya da Makine ID olarak da adlandırılır)

Bu teknolojiler çok sayıda teknik özellikleri analiz eden; alet ve makine ID'leri üreten benzeri olmayan kimlik belirleyicilerin oluşumunu ayarlayan logaritmaları yayarlar.

Aktif Ajan Teknolojileri

Aktif ajan teknolojileri araştırma için kullanılan ve deneklerin arka plan modundaki davranışlarını yakalayan donanım ve yazılımlardır. Genellikle diğer etkinliklerle eş zamanlı olarak çalışırlar, içerikleri:

- Direkt olarak kullanıcının bilgisayarına indirilen bir yazılımdır ve sadece potansiyel deneklerin araştırma içeriklerini ve araştırma sorularını sorma durumunda ikaz etme amaçlı kullanılır. Deneklerin internette gezinmesi ile ilgili veri konularını izlemez. Toplanan tüm veriler kullanıcının veri girişlerinden oluşmaktadır.
- İnternet sayfası tıklanma durumu, internet sitesi ziyaretleri, tamamlanan çevrimiçi işlemler, tamamlanan çevrimiçi formlar, reklam butonlarının oranı ve tıklanmadan görülen reklam sıklığı ve online alışverişler gibi güncel online davranışları kapsamında veri konularını yakalayabilen bir izleme yazılımıdır. Bu yazılım aynı zamanda donanım içerisinde mail ya da diğer belgelerde depolan veri konularını yakalama özelliğine de sahiptir. Bu teknolojilerden bazıları casus yazılım olarak sınıflandırılmıştır, özellikle veri konularının tam bilgisi ve sisteme girise dair izni olmadan indirme ve yükleme olduğundabu şekilde sınıflandırılır.

Arastirmacilarin casus yazilim kullanmasi kesinlikle yasaklanmistir.

4.1.2 Tanımlama ve İzleme Teknolojilerinin İfşa Edilmesi

Tanımlama ve izleme teknolojilerinin kullanımı ile ilgili açıklamalar seffaf olmalıdır ve veri toplamadan önce yapılmalıdır. Tekli projeler için bu tür açıklamalar ise araştırma davetinin bir parçasıdır ve projeye özgü bir gizlilik politikası uygulanabilir. Tekli projelerde, çoklu ve tüm projelere özel olan teknolojiler kullanılırsa; çevrimici deneklere yönelik yapılacak teknoloji açıklamaları araştırma kuruluşun genel gizlilik politikasının bir parçası olmalıdır. Projeye özgü ya da genel gizlilik politikaları hyperlink yapılarak deneklerin kolaylıkla erişebileceği şekilde hazır bir şekilde bulundurulmalıdır (Araştırma davetinde veya online araştırmanın açılış sayfasında...)

- Tanımlama bilgileri
- Flaş tanımlama bilgileri
- İzleme için tanımla bilgileri ve Yazılım uygulamaları
- Alet/Makine Kimliği Saptama'da kullanılacak ifsa edilmeye yönelik örnekler Ek 2'de temin edilmiştir.

4.2 Araştırma Organizasyonlarının Kabul Etmesi Gereken Uygulamalar

Kimlik saptama ve izleme teknolojilerini yayan araştırmacılarının kabul etmesi gereken uygulamalar aşağıdaki gibidir:

Bu uygulamaları kabul eden araştırmacılar diğer kabul edilmeyen uygulamalarla ilişki içerisinde olmamalıdır (Online Kılavuz Bölüm 4.3)

Şeffaflık çok önemlidir. Araştırmacılar tanımlama ve izleme teknolojileri ve diğer yazılımlara ilişkin bilgiyi makul bir zaman içerisinde ve veri konularını açıkça belirtilerek açıklama yapmalıdırlar. Bu iletişim, araştırmacıların veri konularının ait bilgilerin kullanılma ve paylaşılma bilgilerini temin etmelidir.

- I. Sadece veri konularından izin alındıktan sonra (ebeveynlerin veya yasal koruyucuların izinleri) araştırma donanımları bireylerin bilgisayarlarına indirilmeli
- II. Araştırmacılar tanımlama ve izleme teknolojileri tarafından toplanan ya da depolan verilere ilişkin denekler ile açık bir iletişim kurmalı.
- III. Açıklama, denegin yazılımı bilgisayar sistemlerine herhangi bir zarar vereceği kaygısı duymadan, kolayca yüklemesini sağlamalıdır.
- IV. Deneğe ait kişisel bilgiler denegin izni olmadan, ikinci bir amaç için kullanılamaz ya da 3. Kişilerle paylaşamaz.
- V. Araştırmacılar deneklerin araştırmaya katılımının gönüllü ve bilinçli olduğuna emin olmalı. Tesvikler, araştırmada kullanılacak tanımlama ve izleme teknolojilerin kabulünün gizlenme veya örtülmesi için kullanılamaz.
- VI. Araştırmacılar son kullanıcılardan sorgular almak için yöntemlerin olduğuna emin olmalıdırlar.
- VII. Rutin ve sürekli olarak, araştırma organizasyonunun açıklanmış politikaları ile tutarlı ve veri konularının katılımcı olarak kaydedildiğini açıkça belirten uyarılar gönderilmeli, böylece veri konularının gönüllü olarak araştırmaya katıldığına emin olunabilir. Araştırmacılar, panele katılan katılımcılara ve veri konularına sisteme zarar vermeden nasıl geri yükleme yapılacağını açık bir şekilde anlatmalı.
- VIII. Hataları düzeltmek, kişisel bilgilerin kapsamını arttırmayan güvenlik problemleri ve yenilikleri uygulamak için yazılım güncellemeleri yüklenirken iç , eger yapılam uyarıya makul bir süre içerisinde (30 gün) geri dönüşüm olmazsa, katılımcının bu güncellemeyi kabul ettiği varsayılır. Bu varsayım güvenlik beyanı içinde yer almalıdır. Özel araştırmalar için 30 günlük uyarı süreci, araştırmacılar tarafından internet sayfasında dikkat çekici bir açıklama olarak yer almalı.

Veri işleme sorumluluğu kritiktir. Araştırmacılar deneklerden toplanan bilgilerin korunması için gerekli önlemleri almalıdırlar.

- i. Kişisel yada hassas veri izin olmadığı sürece toplanamaz. Eğer izin alınamamışsa, veri toplamanın iptali zorunludur ve veriler hemen yok edilmelidir. Bu mümkün değilse, en yüksek düzeyde veri güvenliği önlemi alınmalıdır. Bu verilere artık erişilemez ya da başka amaçlarla kullanılamaz.
- ii. Araştırmacılar veri güvenliği ve veri konularına yönelik gizlilik tehditlerini minimize edecek güvenlik önlemlerini almalıdırlar
- iii. Araştırmacıların kullandıkları teknolojilerin son kullanıcı üzerindeki etkilerini anlamaları önemlidir; özellikle yazılım indirimleri, diğer uyumlu yazılım programları ile bir demet içerisindedir.
- iv. Araştırmacılar bu ürünlerin (ücretsiz yada değil) güvenli ve yasaya aykırı olan gizlilik veya veri güvenliği risklerinin olmaması için gerekli adımlar atılmalı.
- v. Araştırmacılar yazılımın dağıtılmasının yönetilmesinde proaktif olmalı ve dinamik bir şekilde dağıtım kanallarını izlemeli ve karmaşıklık oranı yüksek konularda tavsiye edilen işaretlere bakın.

4.3 Kabul Edilemez Uygulamalar

Araştırmacıların yapması kesinlikle yasak olan uygulamaların listesi aşağıdadır. Araştırmacıların aşağıda belirtilen uygulamaları kabul etmemeleri durumunda casus yazılım kullanıyor oldukları varsayılacaktır.

- I. Veri konularının izni olmadan yazılımın indirilmesi
- II. Veri konularından bilgi topladıklarına ve bu bilgileri nasıl kullanacaklarına ilişkin uyarı yapılmadan yazılımın indirilmesi. Bu uyarı açık, kısa ve dikkat çekici olmalı
- III. Veri konularını saptanmasını sağlayacak bilgilerin onların izni olmadan toplanması
- IV. Veri konularının sisteme giriş izinlerini almadan klavye vurus kaydedicilerini kullanmak
- V. Araştırma yapmak için gerekli olanın ötesinde, veri konularının bilgisayar ayarlarını modifiye edecek yazılımların yüklenmesi
- VI. Veri konularının bilgisayar ya da makinesindeki anti casus, anti-virus ya da anti spam programlarını kapatacak , kontrol edecek ya da gaspedecek yazılımlar yüklenmesi

- VII. Yazılımın ana operasyon sisteminde veya diğer yüklenen yazılımların beklenmeyen ya da değişken bir şekilde çalışması üzerinde zarara yol açacak önlemlerinin alınmasında başarısız olunması
- VIII. Baska yazılımlara gizlenmiş, ya da bilgisayardan kaldırılması zor olan yazılımların indirilmesi
- IX. Reklam testleri dışında, reklam içeriği gönderen yazılımların indirilmesi
- X. Kullanıcıyı ikaz etmeden ve istediği zaman sistemden çıkma teklifini sunmadan yazılım güncellemelerinin yüklenmesi
- XI. Kullanıcıyı ikna etmeden, kimlik tanımlama ve izleme teknolojilerin yapısında değişiklik yapmak
- XII. Yazılım güncellemelerine yönelik gizlilik uygulamalarındaki değişiklikleri kullanıcılara bildirilmemesi
- XIII. Veri konularının e-mail konularını izlemek
- XIV. Deneğin web tarayıcısı özel olarak ayarlanmışsa, araştırmacılar sisteme giriş izni alınmadığı sürece veri konularının internet davranışlarını izleyemez.
- XV. Denek bulunduğu güvenli bağlantı (SSL gibi...) olarak ayarlanmış internet sitesinde ise, araştırmacı denekten sisteme giriş izni almadan kişisel veri toplayamaz

4.4 İnteraktif Mobil Aletler ve Akıllı Telefonlar

İnteraktif mobil aletler ve akıllı telefonlar internet tarayıcılarının ve cep telefonlarının özelliklerini birleştirebilirler.ESOMAR online araştırma ve cep telefonu kullanılan araştırmalara yönelik kılavuzlar yayınlamışlardır.

Araştırmacıların deneklerle iletişim yöntemi olarak cep telefonunun yararlanılan fonksiyonuna bağlı olarak (deneklerin aranması / mesaj gönderim ya da mail/internet sitesi linki/yüklenen uygulamalar) uygun olan kılavuz takip edilmelidir. Eğer ikisinin kombinasyonu söz konusuysa, irtibat kurmak için cep telefonu, geri dönüşüm almak için mail kullanılması gibi., her iki kılavuzun ilgili/uygun bölümleri uygulanmalıdır.

4.4.1 İnteraktif Mobil Cihazlar

İrtibat Kurmak

Kisilerle irtibat kurmada çevrimici yöntemlerin kullanılması durumunda, ülkenin kanunları izin verse bile, araştırmacılar deneklere yönelik mail ya da diğer mesajlar vasıtasıyla istenmeyen yaklaşımlarda bulunmamalıdır. Bireylere kendileriyle araştırma kapsamında anlaşılır nedenlerden dolayı irtibata geçildiğini belirtilmelidir.

Güvenlik ve Uygulamalar

Araştırmacının mobil interaktif cihazlara apps yükledikleri zaman, kılavuzdaki bölüm 4.1.1 ve 4.1.2'ye riayet etmelidirler. Araştırmacılar deneklere gizlilik politikasını uygulayabilecekleri yer ve izin verebilecekleri uygun kanal ve mekanizma sunmalıdırlar. Bununla beraber bolum 3.4'e riayet edebilmesi için araştırmacılar bölgesel olarak saklanan herhangi bir verinin cihaz üzerinde güvenli olduğuna ve baska kullanıcılar tarafından kullanılma ya da çalınma ihtimalin mümkün olmadığına emin olmalılar. Veri şifreleme fonksiyonu bunu sağlayabilir.

Denege Maliyeti

Deneğin, araştırma sürecinde interaktif mobil cihazları kullanırken dolaşım,air-time ya da veri maliyetine maruz kalabilirler. Eğer mümkünse, araştırma deneğe hiçbir masraf yaratmayacak şekilde dizayn edilmelidir. Eğer bu mümkün değilse, deneklerin hacamaları tazmin edilmelidir. İnteraktif mobil denekler panele ya da örneklem veri tabanına eklendiğinde, maliyet ve maliyet tazminini kayıt aşamasında deneğe onaylatmalıdırlar.

Uygun Dizayn

İletişime geçilen deneklerin mobil interaktif cihazlar kullandığı zaman, araştırmacılar araştırmanın optimize edilen cihazların katılımcılar tarafından görülebileceği bir formatta sunulmasını sağlamalıdırlar. Bunun yanı sıra, deneklere araştırmadan çıkabilme imkanı sunulmalıdır. Araştırmacılar uygun çözümler geliştirmeli ve bilgiye erişmede minimum harcama ile maximum kolaylık sağlamalıdırlar. Orneğin, gizlilik politiklarına en kısa URL ile direkt link imkanı, ücretsiz telefon ve/veya posta adresi sağlanmalı.

Yer Verileri ve GPS

İnteraktif mobil cihazlardan ve akıllı telefonlardan gerçek zamanlı konum verisi gibi ek veri yakalamak artık mumkun. ESOMAR'ın kılavuzdaki Pasif Veri Toplama bölümü bu konuya işaret etmektedir. Araştırmacılar bu verileri işlemeyen önce deneğin iznini almalıdırlar.

5. YÖNTEM KONULARI

5.1 Online Örnekleme

Online örnekleme toplamanın birkaç değişik yolu vardır ve herbirinin farklı izin şartları vardır (bakınız bölüm 2.3 gizlilik politikaları). Panel üyelerinin kişisel verileri panel tedarikçileri tarafından tutulur, ama diğer **örnekleme yöntemleri kişisel verilerin servis sağlayıcılar tarafından tutulmasını gerektirmez**. Eğer bireylerin kişisel verilerinin depolanması amaçlanırsa; gerekli olan izin, uygulamanın yapıldığı zaman ya da uygulamaya başlanmadan alınmalıdır.

5.2 Erişim Paneli

Bu bölüm şu anda inceleme altındadır ve bitirildiği zaman buraya eklenecektir.
(Bu arada mevcut kılavuzdaki güncelleme sürecinde olan 26 soruya bakın)

5.3 Teknik Ayrıntılar

ICC/ESOMAR yönetme kodu araştırmacıların araştırmada kullanılan yöntemlerin teknik detaylarına ilişkin ayrıntılı bilgi sunmasını talep eder, online araştırma karmaşık method ve örnekleme stratejilerine sahip olabilirler. Bu durum tekrar edebilecek çalışmalar için teknik detayları daha önemli bir hale getirir.

ICC/ESOMAR kılavuzundaki; araştırmacılar ve müşteriler arasındaki karşılıklı hak ve sorumluluklara ilişkin bölüm ICC/ESOMAR kodu tarafından araştırma projelerinde teknik raporlama için gerekli şartları belirler.

Bu kılavuz online araştırmalar da olmak üzere tüm araştırma projelerine uygulanır.

6. TANIMLAR VE YARARLI BİLGİ KAYNAKLARI

Üç kilit kavram; araştırmacılar, kişisel veri ve rıza bu kılavuzun araçları olarak aşağıda ele alınmıştır.

Araştırmacılar: ICC/ESOMAR uluslararası kodunda araştırmacı; araştırma projesini geliştiren ya da danışmanlık yapan- müşteri organizasyonlarında çalışanlar da dahil olmak üzere- kişiler ya da organizasyonlar olarak tanımlanmıştır.

Kişisel Veri: Gerçek kişilere ilişkin belirli veya belirlenebilir; yani kurumsal varlıklara karşı özel bireylere ilişkin bilgilerdir. Tanımlanabilir kişi direkt ya da indirekt olarak özellikle bireyin fiziksel, psikolojik, akıl, ekonomik ve kültürel veya sosyal karakteristik kimlik numaralarını referans eder.

Hassas personal veriler; kimliği saptanabilir kişilere ait ırk ve etnik köken, sağlık ya da cinsel yaşam, sabıka kaydı, politik görüş, dil ya da felsefi inançlar, sendika üyeliği gibi bilgilerdir. Amerika Birleşik Devletlerinde sağlıkla ilgili bilgiler, gelir ve diğer mali bilgiler, finansal tanımlayıcılar ile devlet tarafından verilen ya da mali kimlik bilgileri de hassas veri olarak kabul edilmektedir.

Rıza: Kişisel verilerin toplanması ve işlenmesi için veri konuları tarafından serbestçe verilen bilgi sözleşmesi anlamına gelir. Pazar araştırmalarındaki rıza ise, bilgilerin hangi amaçla, kimin tarafından ve toplanan verilerin yapısına ilişkin bilgilerin net olarak sağlanması ve denek sorulara gönüllü olarak yanıt vermesi gerçeğine dayalıdır. Denek, görüşmenin ya da araştırmanın herhangi bir anında işbirliği yapmayı redderek kendi rızası ile görüşmeyi bitirebilir.

Kesin Rıza Avrupa Birliği direktifinde kişisel verilerin işlenmesi için kullanılır. Ancak kesin rıza, terim olarak Avrupa Birliği dışında tanınmaz. Bu kılavuzda “Rıza” terimi kullanılmaktadır.

Mevzuatla İlgili Kilit Noktalar

Avrupa Birliği veri koruma direktifi (resmi olarak 95/46/EC Direktifi- Kişisel verilerin işlenmesi ve serbest dolaşımı ile ilgili bireylerin korunması) Avrupa Birliği içerisinde kişisel verilerin işlenmesini düzenler. 27 Avrupa Birliği üyesi devletin tamamı, direktifi aktardılar ve kendi ulusal veri koruma mevzuatını yürürlüğe soktular.

Elektronik İletişim ve Gizliliğe İlişkin Avrupa Birliği Direktifi (resmi olarak 2009/136/EC). İstenmeyen ticari elektronik iletişim önceden izin alınmasını gerektirir ve SMS, metin mesajları ve sabit/mobil terminallerden alınan diğer mesajları da kapsar. Tanımlama bilgilerinin kullanım amaçlarına ilişkin açık ve kapsamlı bilgi

edinme sağlandıktan sonra, son kullanıcılara ait tanımlama bilgilerinin bilgisayarda depolanması için izinleri gereklidir.

Bu Direktif, mevcut e-gizlilik yönergesini güçlendirir.2002/58/EC ve onun etkileri Avrupa Komisyonu kadar, Avrupa Birliği üyelerinin 2011 yılında yapılan ulusal yasaların uygulanmasına da bağlı olacaktır.

Canada-Kişisel Bilgi Koruma ve Elektronik Belge Antlaşması

Kişisel bilgiler tanımlanabilir bireylere ait bilgiler anlamına gelir, fakat isim ve pozisyonları da dahil olmak üzere işyeri adresleri, organizasyon çalışanların telefon numaraları bilgilerini içermez.

Not: İşyerlerine ait e-posta adresi PIPEDA kuralları altında kişisel bilgi olarak kabul edilir.

Hassas kişisel bilgiler kanunda tanımlanmıştır.

Amerika Birleşik Devletleri Federal Yasaları

Amerika Birleşik Devletleri veri koruma yasaları federal düzeyde sektör spesifik, şu anda; tek, kapsamlı, ulusal gizlilik yasası yoktur. Yasa tüm özel sektör kuruluşlarına uygulanır.

İki sektöre özel gizlilik kanunları bazı finansal ve sağlık sektöründeki organizasyonlara uygulanır. The Gramm-Leach-Bliley Sözleşmesi (GLB) and Sağlık Sigortası Portatifliği ve Saymanlığı (HIPPA)

Çocuklarla araştırma yaparken, Online Çocuk Gizlilik Koruma Yasası uygulanır.

Veri Güvenliği ihlalleri ile ilgili Amerika Birleşik Devletleri Yasaları

Kaliforniya Yasa Tasarısı 1386 - ABD'de ilk güvenlik ihlali bildirim kanunu anlamında kişisel bilgileri tanımlar:

Bireylerin ilk isimleri yada aşağıdaki veri kombinasyonlardaki ilk başlangıç ya da son isimleri veya isimleri ya da veri elmanları şifre değildir.

- Sosyal güvenlik numarası
- Sürücü belgesi numarası veya Kaliforniya Kimlik Kartı numarası.
- Hesap numarası, Kredi ya da hesap kartı numarası, istenilen güvenlik kodu ile birlikte erişim kodu ve şifre bireyin hesabına erişim izni verecektir.

Yararlı Kaynaklar

Asağıdaki online arařtırmacılar için yararlı ve ilgili materyal tedarik edilmiřtir.

ACE Derneęi İşbirlięi Performansı: Bugüne kadar olan kilit internet arařtırma kavramlarına ait tanımlamalar burada geliřtirilmiştir

AMSRO Pazar ve Sosyal Arařtırmalar Gizlilik Kanunu ve Pazar ve Sosyal Arařtırmalar Gizlilik İlkeleri;

COPPA Çocukların Çevrimiçi Gizlilik Koruma Yasası;

CASRO Arařtırma Çalışmaları Standartasyon ve Ahlak Kodu, Bölüm 3. İnternet Arařtırmaları

ADM Federal Almanya Cumhuriyetinin ülkesi için ICC/ESOMAR Uluslararası Kodu ile ilgili taahhütnamesi

DMA Uygulama Kodları Çocuklar Online olarak kurulacak Ticari İletişimde uygulanacak kodlar

ADM, ASI, BVM, DGOF tarafından imzalanan **Online Anketler için rehber (Almanya);**

MRS Kodu Çocuk ve Gençlik Arařtırmaları Rehberi;

ABD-AU Güvenli Liman Çerçevesi:

ABD ve AB'nin farklı yaklaşımları arasındaki farklı gizlilik köprü kurmak için Organizasyonlar için AB'den Avrupa Birliğine veri transferi yapılırken Avrupa Birliği direktiflerine uyumu sağlar. ABD Ticaret Bakanlığı, organizasyonların değerlendirileceęi bilgiyi ve sonrasında katılımını sağlamak için Avrupa Komisyonu ile istişare halinde Güvenlik Limanını geliřtirdi.

Avrupa Komisyonu: AB kişisel veri transferi için model sözleşmeler;

ISO 26362:2009: Pazar ve kamuoyu arařtırma erişim panellerinde basın açıklaması - kelime ve hizmet gereksinimleri;

ISO 20252:2006: Pazar, görüş ve sosyal arařtırma - Kelime ve hizmet gereksinimleri.

rupa

PROJE EKİBİ

- **Jonh O'Brien**, ESOMAR Profesyonel Standartlar Komitesi Danışmanı (Proje Ekibi Başkanı)
- **REG Baker**, COO, Pazar Strateji Uzmanı
- **Diane Bowers**, ESOMAR Profesyonel Standartlar Komitesi Üyesi ve CASRO Başkanı
- **Mike Cooke**, Uluslararası Direktor, Online Geliştirme, GFK Nop
- **Jonathan Sephcott**, Genel Müdür Yardımcısı, ViewsNet, Synovate
- **Kathy Joe**, Profesyonel Standartlar ve Kamu İşleri Direktörü
- **Kees de JONG**, CEO, Uluslararası Anket Örneklemesi
- **Peter Milla**, CASRO Danışmanı
- **Adam Philips**, ESOMAR Profesyonel Standartlar ve Hukuk Kurulu Başkanı
- **Renee Smith**, Araştırma Bölümü Şefi, KANTAR
- **David Stark**, Genel Müdür, Gizlilik ve Uyum Görevlisi, GFK
- **Kevin Umeh**, Cintusa, Geçmiş Dönem CEO'su

EKLER 1- ICC / ESOMAR Kodu'nun Temel esasları

1. Kilit pazarlama arařtırmacıları ICC / ESOMAR Kanunu'nun ilgili tüm ulusal ve uluslararası kanun esaslarına uygun olmalıdır
2. Pazar arařtırmacıları etik davranmak zorundadır ve pazar arařtırması itibarına zarar verebilecek hiçbir Őey yapmamalıdır
3. Çocuklar ve gençler arasında arařtırma yaparken pazar arařtırmacıları extra dikkat göstereceklerdir.
4. Katılımcıların iřbirlięi gönüllüdür ve katılım için izin elde edildięinde ve tüm açıklamaların onurlandırılması arařtırmanın amacı ve yapısına iliřkin yanıltıcı olmayan ve yeterli bilgiye dayalı olmalıdır.
5. Özel bireyler olarak katılımcıların hakları piyasa arařtırmacıları tarafından saygıyla karsılanmalı ve bir pazar arařtırması projesinde iřbirlięinin doęrudan bir sonucu olarak zarar görmemeli veya olumsuz etkilenmemelidir.
6. Pazar arařtırmacılar, toplanan kisisel verilerin pazar arařtırması dıřında herhangi bir amaç için kullanılmasına asla izin vermemelidirler.
7. Pazar arařtırmacıları bütün hazırlanan ve geręekleřtirilen projelerin Őeffaf, doęru ve objektif olarak raporlandıęına emin olmalıdırlar.
8. Pazar arařtırmacıları adil rekabetin ilkelerine riayet etmelidirler.

EK 2- Gizlilik Politikası Örneęi

Ařaęıda verilen örnek, gizlilik politikası için bir çerçeve sunmaktadır. Bu metin kapsamlı ya da ulusal veya bölgesel yasaların güncellenmiř hali olarak kabul edilmemelidir. Arařtırma organizasyonların gizlilik politikalarının çalıřma yürüttüęü ülkelerin yürürlükteki yasal gereksinimlere uygunluęunu saęlamak arařtırmacıların sorumluluęundadır. Bu politika üç seviyeden oluřan ana bölümlere bölünmüřtür, ilk seviye veri kullanımının ve gizlilik politikalarının nasıl kullanılacağına yönelik kısa açıklamayı içerir;ikinci ařama genel ilkelerin amaçlarına iliřkin genel bilgi; 3. Ařama, arařtırmacıların kisisel verileri nasıl deęerlendireceęine yönelik tüm yaklařımları kapsayan detaylı bölümdür.

ÖRNEK:

1.Seviye

Araştırma projemize katıldığınız için teşekkür ederiz.

- 1.Sizin mahremiyetini koruyacağımıza ve bilgilerin gizli olarak ele alınacağına söz veriyoruz.
2. Verdiğiniz bilgiler araştırma amaçlı kullanılacaktır.
3. Bilgileriniz sizin bilginiz olmadan üçüncü şahıslarla paylaşılmayacaktır.
4. Size asla bir şey satmaya çalışmayacağız, ya da sizin kişisel bilgilerinizi kimseye satmayacağız. Bu bizim işimiz değil. Biz telepazarlamacı yada doğrudan pazarlamacı değiliz. Biz pazar araştırmacılarıyız ve sadece sizin fikirleriniz ve davranışlarınızla ilgileniyoruz.
5. Çalışmaya katılım kararınız, bazı sorulara yanıt vermeme ya da görüşmeyi durdurmak sizin kararınız olacaktır ve size herhangi bir soru sorulmadan bu kararınıza saygı duyulacaktır.

Pazar araştırması hakkında daha fazla bilgi (Seviye 2) için tıklayınız
Gizlilik politikalarının kapsamlı bir açıklama (Seviye 3) için tıklayınız

2. SEVIYE

Mahremiyetiniz bizim için önemlidir

Pazar, anket ve kamuoyu araştırması toplumda önemli bir fonksiyonlar sunar. İşletmeler ve hükümetler anket ve araştırmalar sayesinde daha iyi kararlar alırlar. Ankete katılan biri olarak görüşleriniz , mevcut olanları yapmak , yeni ürünler ve müşteri hizmetlerini geliştirmek için firmalara yardımcı olacaktır. Siyasi örgütler ve hükümetler de yasa ve politikalar geliştirmek ve kamunun istek ile ihtiyaçlarını tespit etmek için anketlere başvururlar.

Firmamız tarafından yapılan araştırmaya katıldığınız zaman, gizliliğinizi koruyacağımızdan emin olabilirsiniz .Ara sıra yanıtları doğrulamak için yeniden temasa geçebiliriz. Kendimizi ya da yaptığımız işi asla yanlış bir şekilde sunmayacağımıza emin olabilirsiniz. Biz detaylı gizlilik politikalarımızın içerisinde kesin standartlar oluşturduk.

Firmamızın pek çok profesyonel üyesi ESOMAR'a bağlıdır. ESOMAR dünya genelinde pazarlama, tüketici ve toplumlar için daha iyi araştırmalar sağlayan bir dünya kuruluşudur. ESOMAR gizliliğinizi korumak için firmamızında sadık kaldığı profesyonel standartlar getirmektedir.

Herhangi bir gizlilik sorunuz veya endişeniz varsa, bize e-posta yoluyla Gizlilik Görevlisi ile mail (mail adresi yerleştir), telefon (ücretsiz telefon numarası ekle) veya posta ile (posta adresi ekleyin) iletişime geçiniz.

3. Seviye

Gizlilik Politikası

Oluşturulduğu Tarih (Tarih ekleyin)

Son revize tarihi (Tarih ekleyin)

Araştırmacılara Not: Bazı ABD eyaletlerinde yukarıdaki bilgiler de içerecek şekilde web sitesine yönelik gizlilik politikalarının olması gerekliliği vardır. Şirketlerin kendi gizlilik tablolarına önemli bir değişiklik yaptıklarında, tüketicilerin bu konuya ilişkin bilgi vermek için son revize tarihini eklemek iyi bir uygulamadır.

1. Topladığımız Bilgiler

Firmamız online araştırma yürüttüğünde, araştırma davetimiz ve soru formumuz acik bir şekilde bizi tanıtır ve sizinle irtibata geçme amacımızı açıklar.

Sizinle genellikle aşağıdaki amaçlardan biri için sizinle irtibat kurarız

1. Sizi araştırmaya katılmaya davet etmek için
2. Sizinle anket görüşmesi yapmak için
3. Ankette verdiğiniz cevapları doğrulamak için
4. Kayıtlarımızda bulunan kişisel bilgilerinizi güncelleştirmek ve kişisel bilgilerinizin doğruluğundan emin olmak için (sadece paneller için geçerlidir)

Zaman zaman başka nedenlerden dolayı da sizinle irtibata geçebiliriz.

- 1.Sponsorluğu olan bir çekiliş kazanmışsanız ya da ilgili bir teşvik varsa bunu bildirmek için
2. Bilgilerinizi, sizinle yaptığımız ilk görüşmede belirtmediğimiz bir amaç dahilinde kullanma durumumuzda izninizi almak için

Araştırmamıza katıldığınız zaman yaşıyorsunuz, ev halkı birleşimi gibi demografik bilgilerinizin yanı sıra, sizin kişisel görüşlerinizi de sorabiliriz. Anketteki belirli soruları cevaplamamayı ya da görüşmenin herhangi bir anında ankete devam etmeyi reddedebilirsiniz. Eğer internet araştırma paneline katılırsanız, devredışı bırakma talimatlarını takip ederek , gönderdiğimiz e-postalar da dahil olmak üzere herhangi bir zamanda üyeliğinizi iptal edebilirsiniz.

Asla bilinçli bir şekilde yaş sınırının altında olan çocukları (ulusal yaş kodunda ve ilgili yasada belirtilen yaş sınırını ekleyin) ebeveynlerin izni olmadan araştırmaya katılmaya davet etmeyeceğiz.

Anket Yanıtları ve İletişim Bilgilerinin Gizliliği

Sizin verdiğiniz yanıtlar ile diğer katılımcıların verdiği yanıtları birleştirip müşterilerimize raporlayacağız. Aşağıda belirtilen nedenlerin dışında kasti olarak sizin kişisel cevaplarınızı raporlamıyacağız. Sizin ankete verdiğiniz cevaplar bize bağlı olan veya bağlı olmayan servis sağlayıcılar tarafından firma içinde veya dışında toplanabilir, depolanabilir yada işlenebilir (firmanın bulunduğu ülkeyi ekleyin). Onlar topladıkları veya tuttıkları herhangi bir bilgiyi bize ifşa etmek zorundadırlar. Biz bu bilgileri toplar ve gizli bir bilgi olduğunu açıklarız ve bizim değerlerimize eş değer olan güvenlik standartlarıyla koruruz.

Sizin ankete verdiğiniz cevapların gizliliğini korumak için, onları asla satmayacağız, paylaşmayacağız, kiralamayacağız; ya da sizin bilgilerinizi kasıtlı olarak isim, adres, telefon numarası veya mail adresi gibi bilgilerinizi müşterilerimize yada başka birilerine yönlendirmeyeceğiz.

Asağıdaki istisnalar dışında sizin bilgilerinizi 3. Sahıslara ifşa etmeyeceğiz.

1.Sizin isteğiniz ve rızanız olursa, kimlik bilgileriniz ve bireysel yanıtlarınız özel amaçlar doğrultusunda paylaşılabilir.

2.ESOMAR Kuralları doğrultusunda, sizin cevaplarınız sözleşmeye bağlı olarak tutulmak ve bilgilerinizin gizli bildiği olduğu açıklanmak kaydıyla 3. partilere temin edilecek ama bu bilgiler sadece araştırma ya da istatistik amaçlı kullanılacak.

3. Adli merci ve hükümet uyarınca celp, emir ya da benzeri yasal mevzuatlar doğrultusunda bilgiler ifsa edilmeye maruz kalabilir. Bu duruma sıklıkla rastlanmaz ama olması mümkündür.

Web Sitemizde Tanımlama Bilgileri, Log Dosyaları ve Diğer Teknolojilerin Kullanımı

Tanımlama bilgileri, online tarayıcınıza ilişkin bazı bilgileri depolayan ve sayısal kullanıcı ID'sini belirleyen bilgisayarınızda kayıtlı küçük metin dosyalarıdır.

(Paneller için geçerli olabilir) sizi önemli bir panel üyesi olarak tanımlamak, profilinize ve hesap bilgilerinize erişimi engellemek için sitemizde kullandığımız bazı tanımlama bilgileri gereklidir. Web tarayıcınızın gizlilik ayarları tanımlama bilgilerini kabul edecek şekilde (web site URL ekle) düzenlenmiş olmalıdır, yoksa panele kaydınız (website URL ekle) ya da Üye Bölümüne erişiminiz mümkün olmayacaktır. Eğer isterseniz, internet sitesinden çıkarken ya da tarayıcınızı kapattığınızda tarayıcının ayarını tanımlama bilgilerini silecek şekilde ayarlayabilirsiniz.

Bu site sizin tercihlerinizi kayıt etmek için Flash Local Shared Objects (LSO) -"Flash Tanımlama Bilgileri" olarak da bilinir- sizin internette gördüklerinizi tespit etmek, ziyaretlerinizi özel kullanıma ayırmak, araştırma kalitesini tehlikeye atacak sahtecilikle mücadele etmek , ya da birden fazla kullanıcıya sahip olan sitelerde sizin davranışlarınızı izlemek için kullanılıyor, fakat Flaş tanımlama bilgilerini kesinlikle sadece araştırma amaçlı kullanılıyor.

Flash tanımlama bilgileri ile tarayıcı tanımlama bilgileri, veri toplanma sayısındaki ve toplanma biçimindeki değişiklikten dolayı farklıdırlar. Popüler tarayıcıların son versiyonları internet kullanıcıların tarayıcı gizlilik ayarlarını kullanarak yada ekleme bilgi indirerek Flash tanımlama bilgilerini yönetebilirler.

Tarayıcınız bu özellikleri desteklemiyorsa, o zaman Flash Tanımlama Bilgilerini gizlilik ve depolama ayarlarını Macromedia web sitesini ya da Flash Playerinin sitesine giderek devre dışı bırakabilirsiniz.Link:

[Adobe - Flash Player: Settings Manager:](http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html)

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

Not: AB'deki araştırmacılar, tanımlama bilgilerinin servisin sağlanması için çok gerekli olmaması durumunda, tanımlama bilgilerin yerleştirilmesinde AB mevzuatı ve diğer koşullara ilişkin danışmanlık almak için bölüm 4.1.1'e bakılması tavsiye edilir.

(Davranış İzleme Araştırmaları İçin Geçerlidir.)

Biz reklam ve internet araştırmaları için hem tarayıcı hem de Flas temelli (yazılım uygulamalarını ekleyiniz) seçmeli tanımlama bilgilerini kullanırız. Bu tanımlama bilgileri ziyaret ettiğiniz internet siteleri ve seyrettiğiniz reklamlar da dahil olmak üzere, sizin onları ne sıklıkta ziyaret ettiğinizi ya da gördüğünüzü ölçüyoruz. Yalnızca küçük bir oranda reklam ve internet sitesi araştırma projesi kapsamında ölçülecektir ve toplanan bilgiler kesinlikle araştırma amaçlı kullanılacaktır. Araştırma projesinde yer aldığınızdan dolayı hiçbir şekilde ticari mesaja ya da iletişime yönlendirilmeyeceksiniz. İnternet sitesimize girdiğinizde bu programa ait ayrıntılı bilgiler sizin için mevcuttur. Bu bilgiler içerisinde katılımı nasıl durduracağınıza dair talimat da sitemizde mevcuttur.

Coğu web sitesi gibi , bazı bilgileri otomatik olarak toplar ve günlük olarak lod dosyalarında saklar. Bu bilgiler IP (internet Protokolü) adresi de dahil, tarayıcı türü, internet servis sağlayıcı, mevcut sayfa, işletim sistemi, zaman bandrolü ve tıklama akışı verileri. Bu bilgileri; trend analizi, sitemizin yönetiminde, kullanıcıların sitemiz içerisindeki hareketlerini izleme ve kullanıcı tabanına ilişkin demografik bilgilerinin edinilmesi için kullanırız. Sahteciliğe karşı korumak (Araştırma firmasının URL'sini ekle) ve sunulan bilgileri otomatik olarak toplamak için link yapabiliriz.

(Cihaz kimliği için geçerli)

Kimlik Bilgi teknolojileri bilgisayar kullanıcılarını belirlemek ve bilgisayarları izlemek için benzersiz bir tanımlayıcı atar. (Firma adını ekleyin) Cihaz kimliği teknolojileri (Cihaz ID'si ya da digital parmak izi olarak da bilinir) kişisel bilgileri toplar ya da bilgisayar kullanıcıların çevrimici hareketlerini izler. Biz bu teknolojileri, müşterilerimize araştırma sonuçlarımızın doğruluğunu ispat etmede bize yardımcı olması için kullanırız. Bu teknolojiler sizin bilgisayarınızdaki internet tarayıcınızdan ya da diğer kamuya açık veri noktalarından, sizin bilgisayarınızın teknik ayarları, bilgisayarınızın özellikleri ve bilgisayarınızın IP adresi de olmak üzere toplanan bilgileri analiz eder. Bu veriler, bilgisayarınıza atanacak benzersiz bir tanımlayıcı oluşturmak için kullanılır. Bu benzersiz tanımlayıcı, bizim koruduğumuz alfa sayısal ID'dir. Biz bu benzersiz tanımlayıcı oluşturmak için teknolojinin analizi ettiği bilgiyi tutmayız. Ayrıca bu teknoloji bilgisayarlarınızın fonksiyonlarında yada ayarlarında herhangi bir modifiye ya da değişiklik yapmaz.

Bizim performansımızın da ötesinde, müşterilerimize araştırma sonuçlarımızın korunması ve doğrulanması konularında asiste etmek için:

- a. Bize verdiğiniz bilgilerin herhangi biri ile benzersiz tanımlayıcıları birleştirmek için link kurulabilir

- b. Sizin benzersiz tanımlayıcınızı müşterilerimizle ya da diğer örneklem ya da panel tedarikçileriyle paylaşabiliriz.
- c. 3.Partilerden, panel tedarikçilerden ya da örneklemden ya da müşterilerimizden limitsiz benzersiz tanımlayıcı alınabilir ya da elde edilebilir.

Herhangi bir benzersiz tanımlayıcıyla link kurulan belirli kişiler bu gizlilik politikasına uygun olarak korunacaktır. Biz bu teknolojileri profesyonel ve etik bir tarzda firmamız tarafından yapılan açıklamalara , ifşalara, endüstri kodları ve kanunlara uygun olarak kullanabilir ve yayabiliriz .

Bu teknolojilerin kullanımında herhangi bir etik olmayan davranış olduğunu keşfetmemiz ya da öğrenmemiz durumunda, ya da bu teknolojilerin bizim deneklere açıkladığımız açıklamalarla ya da yürürlükteki kanun ve yasalara uyumsuzluk bulunduğu, etik olmayan bu davranışı yasaklamak için derhal harekete geçeceğiz.

4. Kişisel Bilgilerin Güvenliği

Biz çalışanlarımızı gizlilik, güvenlik ve mahremiyet politikaları ve işlemleri hakkında ve bunlara uyulmasının önemi konusunda bilgilendiririz.

Biz belki kişisel verilerinizi bize bağlı olan ya da olmayan firmalarla veri işleme, ödül çekilişleri ve diğer teşvikler gibi araştırma amaçlı etkinlikler için paylaşabiliriz. Biz bu firmalardan, firmamızın standartları ve mevzuattaki kanunlara uygunluğuna engel olacak durumlar için güvenlik onlemlerini alma şartı koyarız. Bu aktarım sırasında ve teslim alınma aşamasında, kişisel bilgilerinizi korumak için kabul edilen gelen endüstri standartlarını takip ederiz.

5. Kişisel Bilgilerin Doğruluğu

(Firma adını ekleyin) Kişisel bilgilerin kontrol pozisyonunda tutulması için doğru, tam, güncel, ilgili ve bizde mevcut olan son bilgilere dayanarak tüm gerekli çabalar gösterilmeli. Bizim sorularımızı dürüstçe yanıtlayan verdiğiniz kişisel bilgilerinizi doğru, tam ve güncel tutmak için sizin yardımınıza güveniyoruz.

6.Kişisel Belgelere Erişim

Araştırmacılar İçin Not:

Geniş kapsamlı gizlilik kanunları olan Avrupa, Avusturalya, Kanada, Yeni Zellanda ve diğer yargı mercilerlerinde bireylerin belirli koşullarda kuruluşlar tarafından düzenlenen kişisel bilgilere ulaşmak için yasal hakları var. Bireylerin erişim hakları ABD-AB Güvenli Liman Çerçevesinde bulunan ABD şirketleri için de geçerlidir. Bizim tarafımızdan tutulan kişisel bilgilerinize erişim istemek için, aşağıda bulunan (Bize ulaşmak için yazılacak) adres ve ya email adresine isteğinizi yazılı olarak belirtmeniz

gerekmektedir. Aşağıda belirtilen durumlar hariç, bir yanlışlık olması durumunda, kişisel bilgilerinizi düzeltmek, değiştirmek ve silmek için erişim mümkün olabilir.

1.Kişisel bilgilerinize erişim imkanı sağlamamız , kişisel bilgilerinizin ortaya çıkmasını muhtemel kılacaktır.

2.Bilgilerin ifşa edilmesi gizli ticari bilgilerin ya da müşterilerin bilgilerini (firma adını ekleyin) ortaya çıkartabilir.

3.Erişim sağlama mesuliyeti ve maliyeti sizin cevaplarınızın gizliliğini koruma ihtimaline karşı gereksiz bir risk oluşturabilir.

Biz erişim talebini aldıktan sonra, 30 gün içerisinde istenen kişisel bilgileri sunmak için gayret göstereceğiz. İsteğinizi yerine getiremediğimiz takdirde, erişim isteğinizi reddetme nedeni yazılı bir açıklama ile size bildirilecektir.

7. Bu Politikalardaki Maddelerin Değişiminin Bildirilmesi

Bu politikalarda ya da gizlilik uygulamalarında herhangi bir madde değişikliği yapmamız durumunda; madde değişikliğin uygulamaya geçirilmesinden 30 gün önce, bu değişiklik sitemizde belirgin bir şekilde yayınlanacaktır. Bununla beraber bireylerin bu uygulanabilir seçimleri nasıl uygulayacakları tarif edilecektir. Madde değişikliklerindeki uygulama takibi olarak, bu politikaların en son gözden geçirilmiş halini kayıt edeceğiz.

8. Bize Ulaşmak İçin

Bu politikalarla ilgili sorular, uygulamalara ilişkin şikayeter ya da erişim isteği direkt bir biçimde e-mail aracılığıyla Gizlilik Görevlisine yöneltilmelidir. Biz tüm bu şikayetleri sorgulayıp, gerekçeli olarak sizlere açıklayacağız.

ESOMAR pazar arařtırmalarını dünya genelinde teřvik eden, ilerleten ve yükselten bir dünya kuruluřudur.