Dünya Araştırma Yasaları ve Yönetmelikleri

ESOMAR VERİ KORUMA KONTROL LİSTESİ

ESOMAR, Toplumsal, Kamuoyu ve Pazar Araştırmaları Dünya Birliği 130'dan fazla ülkeden 4900 üyeyi bir araya getirir ve teşvik edici, gelişen ve yükselen pazar araştırmasında önemli bir kuruluştur. Yasalar ve yönetmelikler www.esomar.org adresinde mevcuttur.

İÇİNDEKİLER

1 GİRİŞ

Uluslar arası bağlamda çalışan araştırmacılar bireylerin mahremiyetine saygı gösterildiğinden emin olunması ve kişisel verilerin korunması için tasarlanmış bir dizi ulusal yasayla gün geçtikçe daha fazla yüzleşmektedir. Sadece faaliyet gösterdikleri ülkedeki yasal şartlara değil, aynı zamanda araştırma yaptıkları ve/veya veri işledikleri tüm ülkelerdeki veri koruma koşullarına uyma ve bunları değerlendirme yükümlülükleri vardır.

Aynı zamanda; yeni teknolojilerin hayatımızın tüm yönlerinde amansızca genişlemesi araştırmacıların ulaşabileceği kişisel veri hacmini sadece artırmakla kalmadı, aynı zamanda korunması gereken yeni tip kişisel bilgilerle bizi tanıştırdı.

Değişmeyen tek şey, araştırmacıların katılımcıların ve müşterilerin şeffaflığını sağlayan, sağladıkları bilgilerin güvenilirliğini koruyan ve araştırma katılımcıları için değerlendirme sergileyen çalışmalarında pazar, toplumsal ve kamuoyu araştırmalarının itibarını koruma ihtiyacıdır.

2 KAPSAM

Bu belgenin amacı araştırmacılara, özellikle daha küçük kuruluşlarda çalışan ve veri koruma koşulları hakkında kapsamlı kaynaklara ve tecrübeye sahip olmayan araştırmacılara araştırma katılımcılarının kişisel bilgileri hakkında kontrollerini muhafaza etmek için uluslar arası veri koruma çerçevesinde yükümlülükleri hakkında genel rehberlik sağlamaktır. Kullanılan sistem İktisadi Kalkınma ve İşbirliği Örgütü (OECD) tarafından geliştirilmiştir. Bu sistem kişisel verinin korunması ve gizliliğinin sağlanması için planlama programlarında kullanmak için sekiz prensip içerir:

- Toplama Kısıtlaması
- Veri kalitesi
- Amacın belirlenmesi
- Kullanım kısıtlaması
- Güvenlik önlemleri
- Aleniyet
- Bireysel katılım
- Sorumluluk

Bu kapsamlı prensipler dünya çapındaki çoğu mevcut ve gelişen gizlilik ve veri koruma yasalarına yansıtılmıştır.

Ancak araştırmacılar OECD prensiplerinin AB'nin veri koruma gereksinimlerine bağlı olduğunu göz önünde bulundurmalıdır. Ve bu yüzden diğer bölgelerde çalışan araştırmacılar uygulanabilir olan diğer kapsamlara danışmaları konusunda teşvik edilmektedir. Bunlara Asya-Pasifik Birliği (APEC) Gizlilik Kapsamı, ABD Güvenli Liman Gizlilik Prensipleri ve Amerikan Kurum CPA (AICPA) ve Kanada Yeminli Mali Müşavirler Kurumu tarafından geliştirilmiş Genel Kabul Görmüş Gizlilik Prensipleri (GAPP) dahildir. Bu kapsamlar genel olarak yasal hükme sahip olmamasına rağmen, yine de araştırmacıların uygun bölgelerde çalışırken benimsemesi gereken temel prensipleri ifade ederler.

Buna ek olarak araştırmacılar, o ülkede temel prensiplerin uyarlanmasında farklılıklar olabileceğinden, saha çalışması veya veri işlemeyi planladıkları her ülkedeki ulusal veri koruma ve pazar araştırması hakkındaki düzenleyici gereksinimleri gözden geçirmeli ve bunlara uymalıdır. Bu belgede sağlanan yönetmelikler minimum standartlardır ve bunların belirli araştırma projeleri bağlamında ek hususlarla desteklenmesi gerekebilir. Araştırmacılar, tam uygunluğu sağlamak için araştırmanın gerçekleştirileceği yetki bölgesindeki yerel yasal

müşavirlere danışmayı gerekli görebilirler. Ayrıca DLA Piper tarafından sunulan ve yıllık olarak güncellenen The Data Protection Laws of the World adresindeki online kaynağa başvurmak yararlı bulunabilir.

Son olarak sağlık hizmeti araştırması gibi uzmanlaştıkları alanlarda araştırma yapan araştırmacılar daha fazla yardım için EphMRA Adverse Event Reporting Guidelines 2014 gibi belli kılavuzlara başvurabilirler.

3 "-MALI"'NIN ZORUNLULUK VE ÖNERİ ŞEKLİNDE KULLANIMI

Bu belge içerisinde "-malı" eki zorunlu gereksinimleri tanımlamak için kullanılmıştır. "-malı" ekini araştırmacıların ICC/ESOMAR International Code on Market and Social Research uymak için takip etmekle yükümlü oldukları prensipleri veya işlemleri tanımlamak için kullanıyoruz. Bir prensibin veya işlemin tatbiki hususunda önerilir/tavsiye edilir kelimeleri kullanılmıştır. Bu kullanımda, araştırmacıların bir prensibi veya işlemi uygulamayı araştırmanın doğasına göre farklı şekillerde uygulamayı seçebileceği ifade edilmiştir.

4 TANIMLAR

İşletmeler arası araştırma (B2B) işletmeler, okullar, kar amacı gütmeyen kurumlar vb yasal kurumlar hakkında veri toplanması manasına gelir.

Firmadan tüketiciye araştırma (B2C) bireylerden veri toplanması manasına gelir.

İzin bir kişi tarafından kişisel bilgilerinin toplanması ve işlenmesi hakkında özgürce verdiği ve bilgisi dahilindeki anlaşma manasına gelir. Pazar, toplumsal ve kamuoyu araştırmalarında bu izin araştırma katılımcısının toplanan verinin doğası hakkında, bu verinin hangi amaçla kullanılacağı hakkında ve kişisel veriyi saklayan kişinin veya kurumun kimliği hakkında açık şekilde bilgilendirilmesine dayanmaktadır. Araştırma katılımcısı bu iznini istediği zaman iptal edebilir.

Veri denetçisi kişisel bilgini nasıl işleneceği belirlemekle sorumlu kişi veya kurum manasına gelir. Örneğin bir araştırma müşterisi, müşterileri hakkındaki verinin denetçisi olabilir; bir devlet sosyal yardım derneği kendisinden yardım alan kişiler hakkında toplanan verilerde veri denetçisi olabilir; bir araştırma paneli sağlayıcı, online panel üyelerinde toplanan verinin veri denetçisi olabilir ve bir araştırma firması, bir omnibus anketindeki katılımcılardan toplanan verilerde veri denetçisi olabilir.

Veri işleyici veri denetçisi adına ve onun yönergeleri doğrultusunda kişisel veriyi toplayan, kaydeden, saklayan veya işlemleri gerçekleştiren (analiz dahil) taraf manasına gelir. Yukarıda belirtildiği gibi bir araştırma firması bir omnibus çalışma için hem veri denetçisi hem de veri işleyen olabilir.

Gizliliği koruyan yasalar uygulanması bu belgede belirtilen prensiplere ilişkin kişisel verileri koruma etkisi olan ulusal yasaları veya düzenlemeler manasına gelir.

Pazar araştırması –toplumsal ve kamuoyu araştırmalarını da içerir- içyüzünü kavramak ve karar vermeyi desteklemek için bireyler ve kurumlar hakkındaki bilgilerin istatistik ve analitik yöntemler ve uygulanan sosyal bilimler teknikleri kullanılarak sistematik olarak toplanması ve yorumlanması manasına gelir. Araştırmada yer alan bir kişinin kimliği, o kişinin açık izni olmadan bilgiyi kullanan kişiye açıklanmayacaktır ve sağlanan bilginin doğrudan bir sonucu olarak o kişiye bir pazarlama yaklaşımında bulunmayacaktır.

Pasif veri toplama geleneksel soru ve cevap yöntemi kullanılmadan toplanan veri manasına gelir.

Kişisel veri kimliği belirli veya belirlenebilir bir gerçek kişiye (örn: bir şirketin veya diğer karşılaştırılabilir bir kurumun aksine bir gizli kişi) ilişkin bilgi manasına gelir. Kimliği belirlenebilir kişi, özellikle bir kimlik numarası veya kişinin fiziksel, fizyolojik, akli, ekonomik, kültürel veya sosyal karakteristikleri aracılığıyla doğrudan veya dolaylı olarak kimliği belirlenebilen biridir. Bazı araştırma türlerinde böyle bir veri kaydı fotoğraflar, videolar ve ses kayıtları veya araştırma

sırasında toplanan diğer kişisel bilgiler yüzünden bireylerin kimliği belirlenebildiği durumları içerebilir.

Kişisel verinin işlenmesi bunlarla sınırlı olmamakla birlikte verilerin -otomatik veya diğer şekillerde- toplanmasını, kaydedilmesini, düzenlenmesini, saklanmasını, adaptasyonunu veya değiştirilmesini, geri kazanılmasını, istişaresini, kullanımını, iletilerek, dağıtılarak veya diğer şekillerde ulaşıma sunularak açıklanmasını, sıralanmasını veya kombinasyonunu, engellenmesini, silinmesini veya imha edilmesini içerir.

Araştırma katılımcısı bir araştırma projesinde aktif bir anket veya pasif şekillerde kişisel verisi toplanan herhangi bir kişi manasına gelir.

Araştırmacı müşteri organizasyonlarında çalışanlar ve teknoloji sağlayıcıları gibi alt yükleniciler dahil olmak üzere bir pazar araştırmasını gerçekleştiren veya araştırmada danışman olarak hareket eden bir birey veya kuruluş manasına gelir.

Araştırma müşterisi veya veri kullanıcısı araştırma projesinin tümünü veya bir kısmını talep eden, görevlendiren, sponsorluk eden veya katkıda bulunan birey veya kuruluş manasına gelir.

Hassas veri kimliği belirlenebilir bireyin ırksal veya etnik kökeni, sağlığı veya cinsel yaşamı, sabıka kaydı, politik görüşü, dini veya felsefi inanışları veya ticaret birliği üyeliği hakkındaki bilgiler manasına gelir. Farklı yetki alanlarında hassas olarak tanımlanmış ek bilgi türleri olabilir. Örneğin ABD'de kişisel sağlığa ilişkin bilgi, gelir veya diğer finansal bilgi, finansal tanımlayıcılar ve devlet tarafından sunulan veya finansal kimliğe sahip belgeler de hassas olarak tabir edilir.

Transfer veriye ilişkin olarak herhangi bir açıklama, iletişim, kopyalama veya verinin vasıta ne olursa olsun bir taraftan diğerine aktarılmasıdır. Bunlara bunlarla sınırlı olmamakla birlikte bir ağ içerisinde veya fiziksel transferler, bir medya veya cihazdan diğerine transferler veya veriye uzaktan erişim dahildir.

Kişisel verinin sınırlar arası (transborder) transferi kişisel verinin ulusal sınırlar ötesi transferi manasına gelir. Buna veriye verinin toplandığı ülke dışından ulaşım, bulut teknolojilerinin veri için kullanımı dahildir.

5 VERİ KORUMA POLİTİKALARI VE PROSEDÜRLERİ ÜZERİNE KİŞİSEL KONTROL LİSTESİ

Aşağıdaki kontrol listesini kullanıcıları başlıkların ve maddelerin sırasının OECD'nin kullandıklarıyla aynı olmadığına dikkat edebilirler. Buradaki amaç prensipleri araştırmacıların daha aşina oldukları dil ve sıralamada ifade etmektir. Kullanıcılar aynı zamanda maddelerin birbiriyle ilişkili olduğunu ve bazen birbiriyle iç içe geçtiğini fark edebilirler. **Yine de kontrol listesinin bir bütün olarak görülmesi ve bağımsız maddelerin münhasır olmaktan çok bütünleyici olarak görülmesi önemlidir ve farklılıkların kuruluşun veri denetçisi veya veri işleyici olarak hareket etmesine bağlı olduğuna özel dikkat gösterilmesi önemlidir. Cevabı "evet" olmayan herhangi bir soru gizlilik koruma programında potansiyel bir açığa işaret eder ve bu da bir veya daha çok veri koruma yasasının ihlali riskini ortaya çıkarır.**

5. 1 Minimum etki

1. *Bir araştırma projesi tasarlarken kişisel veri toplanmasını sadece araştırmanın amacı için gerekli maddelerle mi sınırlıyorsunuz ve bu bilgilerin bu amaçlara uymayan şekillerde kullanılmadığından emin oluyor musunuz?*

Araştırmacılar sadece anketin o belirli kişiyle gerçekleştirildiğine dair ve/veya kalite kontrol örneklemesinin gerektirdiği ve/veya ankette analitik perspektifi sağlayacak gerekli kişisel bilgiyi toplamalı ve saklamalıdır. B2B araştırma durumunda araştırmanın amacı için gerekli olabileceğinden bu, bireysel katılımcının şirket içindeki pozisyonu veya seviyesine ilişkin kişisel veriyi içerir.

Aynı prensip kişisel verinin geleneksel soru-cevap yöntemiyle toplanmadığı pasif veri toplama yöntemleri için de geçerlidir. Bu yüzden toplanan kişisel verilerin sadece araştırma amacına yönelik gerekli olanlar olduğundan emin olmak araştırmacının sorumluluğundadır. Başka kişisel verilerin alınması durumunda bu maddeler elenmeli ve silinmelidir.

2. *Süreçleri araştırma katılımcılarının pazar araştırma projesinde yer almanın doğrudan sonucu olarak zarar görmeyeceği veya olumsuz etkilenmeyeceğinden emin olacak şekilde mi uyguluyorsunuz?*

Araştırmacı kişisel verinin izlenmediğinden veya bir bireyin kimliğinin çapraz analiz (tümden gelim ifşa), küçük örnekler veya araştırma sonuçlarındaki farklı yollar aracılığıyla anlaşılmadığından emin olmalıdır. Örnekler coğrafi alan verisi veya müşteri memnuniyet anketinde belirli bir çalışanı teşhis etme yetisi gibi yardımcı bilgilerin bir araya getirilmesini içerir.

3. *Adınıza hizmetleri gerçekleştirmesi içi alt yüklenici veya diğer üçüncü taraf tedarikçiler kullanmayı planlıyorsanız, sunmayı kabul ettikleri hizmetleri gerçekleştirmeleri için gerekli kişisel bilgiyi minimum miktarda açıklıyor musunuz? Do you have contracts in place that ensure a similar level of protection on their part?*

Bir altyüklenici kullanırken, sadece sunulması üzerine anlaşılan hizmeti gerçekleştirmeleri için gerekli minimim miktarda kişisel bilgi sağlayın. Bu bilgiler alt yüklenicinin elindeyken sorumluluklarını sözleşmeler ve talimatlarla her zaman açıkça belirtin. Tüm alt yükleniciler araştırma firması ile aynı kurallara ve yönetmeliklere tabi olmalıdır. Dahası, kişisel verinin alt yükleniciye veya diğer bir üçüncü tarafa aktarılması yalnızca araştırma firmasının müşterisinin önceden verdiği izin veya yetki ile yapılmalıdır.

Yukarıdaki husus araştırma katılımcılarının toplanan tüm verinin gizli kalacağı ve sadece kümelenmiş şekilde analiz edilip raporlanacağına dair güvence verildiğini varsaymaktadır. Eğer araştırma katılımcıları kişisel verilerine ait cevaplarının aktarılacağına dair izin verirse, bilginin nasıl paylaşılacağına ve kullanılacağına dair bilgilendirilmelidirler.

5. 2 Bildirim ve izin

4. *Kişisel verisi toplanacak her katılımcıdan izin alıyor musunuz?*

OECD Gizlilik Prensiplerine göre yasal veya adil şekillerde edinilecek kişisel bilgilerin uygun olduğunda araştırma katılımcısının izni veya bilgisi dahilinde toplanması tavsiye edilir. Genel olarak ulusal yasalar bir dizi yasal ve adil dayanak sağlar ama çoğu durumda araştırmacıların bir izne itimat etmeye mecbur olacaktır.

İzin alma sorumluluğunun diğerlerinin elinde olduğu durumlar vardır. Yaygın örneklere üçüncü taraf panellerinin kullanılması veya müşteri veri tabanının kullanılması dahildir. Bu ve benzeri durumlarda araştırmacı iznin düzgün şekilde alındığına dair güvence edinmelidir.

İzinler;

- Serbest olmalıdır (gönüllü verilmeli ve istediği zaman geri çekilebilmeli);
- Spesifik olmalıdır (bir veya birden fazla belirtilmiş amaca ilişkin); ve
- Bilgilendirilmiş olmalıdır (izin vermenin ilgili sonuçları konusunda tamamen bilinçli)

Araştırma katılımcısı tarafından sağlanan bilgiler hakkındaki izin aşağıdaki maddelerde belirtilen şekilde bir beyan veya hareket ile açıkça belirtilmiş olmalıdır. Özetle katılımcının (a) hangi kişisel verilerinin hangi kullanıma konulacağı, (b) toplanacak spesifik veri; (c) veriyi toplayan şirketin veya kuruluşun adı, adresi ve iletişim bilgisi ve eğer aynı şirket değilse veri denetçisinin bilgileri ve (d) verinin üçüncü taraflara açıklanıp açıklanmayacağı konusunda bilgilendirilmesi tavsiye edilir.

Araştırmacıların izin almakta kullanacakları mekanizmayı dikkatlice değerlendirmeleri tavsiye edilir; genellikle dahil olma, vazgeçme, ima edilmiş, bilgilendirilmiş veya aşikar olarak ifade edilir. Seçilen özel(spesifik) yöntemin belgelendirilmesi tavsiye edilir.

Genel olarak daha hassas, izinsiz veya açık olmayan veri toplaması durumlarında daha yüksek izin standartları gereklidir. Bazı yetki alanlarında tanımlanmış "hassas kişisel veri" sınıfları vardır ve bunlar hakkında veri toplanmadan önce bireylerin açık izinlerinin alınması gereklidir.

Araştırmacıların katılımcı olarak tanımlanmayan kişilerden veya istemeyerek kişisel veri topladığı veya aldığı durumlar olabilir. Örneklere katılımcıların gönüllü olarak verdikleri bilgiler; araştırmayı gerçekleştirmeye yeterli bilgiden daha fazlasını içeren müşterinin sağladığı bilgiler; ve fotoğraflara veya video kayıtlarına giren katılımcı olmayan kişiler dahildir. Araştırmacılar bu tür bilgilere diğer kişisel bilgilerle aynı şekilde davranması tavsiye edilir. Eğer verisi toplanan kişileri verilerin kullanımı, saklanması veya yeri konusunda bilgilendirme yolu yoksa bu verilerin kimlik bilgilerinin silinmesi veya hemen imha edilmesi tavsiye edilir. Bazı yetki bölgelerinde bu tür verilerin silinmesi veya istemeyerek elde edilen diğer bilgilerle aynı şekilde ele alınması zorunludur.

5. Toplanan ve elde edilen verinin amacı veya amaçları hakkında net misiniz?

Araştırma endüstrisi pazar araştırması ile pazarlama, satış promosyonu, liste geliştirme, doğrudan pazarlama ve doğrudan satış gibi diğer amaçlar arasında uzun süredir bir ayrım sağlamayı başarmıştır. Bu ayrım amacı ayırt etmek ve düzenleyicilerin ve genel kamuoyunun gözünde araştırmanın pozitif imajını desteklemek için kritik bir bileşendir. Son yıllarda yeni teknolojilerin gelişmesi kişisel bilgi toplama olasılıklarını online takip ve indirilebilir mobil uygulamalar gibi teknikler aracılığıyla artırmıştır. Tüm durumlarda veri toplamadan evvel muhtemel araştırma katılımcılarının verilerinin hangi amaçla kullanılacağı ve kalite kontrol amaçlarıyla sonradan tekrar iletişim kurmak gibi diğer potansiyel sonuçlar konusunda bilgilendirilmesi önemlidir.

Araştırmacılar bir araştırma katılımcısından bir pazar araştırmasında kullanılmak üzere kişisel veri topladığında, araştırma katılımcısının şeffaflığı kritik bir bildirim unsurudur. Araştırma katılımcısına toplanan verinin kullanım amacı ve üçüncü taraflarla paylaşılması konusunda yeterli şekilde bilgi verilmelidir. Örnek olarak; eğer kişisel verinin kullanım amacı bir müşteri profiline bir anket cevabı iletmekse bu, araştırma katılımcısına kişisel verinin toplanacağı zaman açıklanmalıdır.

Gizlilik bildirimleri toplanan verinin türünden ve kullanım amaçlarının değişmediğinden emin olmak için düzenli olarak gözden geçirilmelidir ve araştırmacılar araştırma kuruluşunda kullanılan asıl çalışma uygulamalarının ve teknolojilerinin araştırma katılımcılarına yapılan taahhütlerle ve gelişen düzenleyici gereksinimlerle uyumlu olduğundan emin olmalıdır. Her kişisel verinin önerilen kullanım alanı yerel gizlilik yasaları, ICC/ESOMAR Yasaları ve ESOMAR Yönetmelikleri ve araştırma katılımcılarına verilen gizlilik sözleriyle uyumlu olduğundan emin olmak için analiz edilmelidir.

6. Toplanacak spesifik veri hakkında net misiniz?

Belirli yetki alanlarında kişisel verinin geniş tanımlarına bakacak olursak, araştırma katılımcılarına bildirime hazırlanırken tüm toplanması olası kişisel veri unsurlarını değerlendirin. Kişisel veri isim, adres, eposta adresi, telefon numarası, cep numarası, doğum günü, mobil cihaz tanımlayıcı, IP adresi, fotoğraf, ses ve video kaydı, ulusal kimlik numaraları (ehliyet, sosyal güvenlik, ulusal sigorta numaraları) kuruluşunuz tarafından atanmış kullanıcı tanımlayıcı, sosyal medya kullanıcı adı, çerezde saklanmış bilgi veya takip etme pikseli/tagi içerebilir. Ayrıca tek bir veri maddesinin tek başına yerel yasalara göre kişisel olarak kimliği belirlenebilir sayılmadığını unutmayın ama diğer verilerle bir araya geldiğinde (örneğin alan/posta kodu, cinsiyet, işyeri veya okul, pozisyon ve maaş) bir bireyin seçilip ayrılmasına olanak verebilir.

Buna ek olarak kişisel veriyi alabilecek tüm olası kişileri değerlendirin. Araştırmacıların, araştırma ajanslarının, üçüncü taraf olarak servis sağlayıcıların ve/veya nihai müşterilerin hepsinin araştırma projesi süresince kişisel veri toplama ve/veya kullanma ehliyeti olabilir.

7. Katılımcının farkında olmayacağı pasif veri toplanması dahil olmak üzere verinin nasıl toplanacağını netleştiriyor musunuz?

Tarihte araştırma kişisel veri toplamadan ana yöntem olarak anket yapmaya güveniyordu. Yukarıda 5. maddede belirtildiği gibi yeni teknolojiler bireylerin kişisel verilerinin toplandığından

haberi olmadan daha geniş bir kapsamda kişisel veri toplamayı olası hale getirdi. Veri ister aktif şekilde anket yapılarak toplansın ister mobil uygulama veya online çerezler aracılığıyla davranış takibi şekilde pasif olarak toplansın, tüm araştırma katılımcıları toplanan belirli veri ve veriyi toplamakta kullanılan yöntem konusunda bilgilendirilmelidir.

Araştırmacılar toplanan verinin hangi unsurlarının ve/veya veri toplama yönteminin araştırma katılımcısı tarafından algılanmadığın değerlendirmesi ve toplama yöntemine ilişkin önemli seviyede açıklama sağlaması tavsiye edilir. Veri toplamayı tanımlamak ve beklenmedik veya çiğneyici olabilecek kullanımlarda daha detaylı bir gizlilik bildirimi için üzerinden geçilmiş "kısa form" bildirimlerini değerlendirin. Mobil uygulamalar, özellikle coğrafi konumu belirleyenler, "pasif dinleme", ve/veya mobil cihazın işletme sistemini ölçenler bu tür faaliyetler için araştırma katılımcısının açık izni ve detaylı bir açıklama gerektirmektedir.

5. 3 Doğruluk/Güvenlik

8. *Prosedürler toplanan tüm verinin doğru, tam ve güncel olduğundan emin olmak için uygun mu?*

Araştırma sürecinin her aşamasında kalite kontrollerinin yapılması tavsiye edilir. Anket veya araştırma uygulamaları geliştirirken, veri toplanmasında hata riskini minimuma indirmek için test etme saha çalışmasına başlamadan evvel testlere başlanması tavsiye edilir. Saha çalışması aşaması sırasında izleme ve doğrulama görüşmelerinin uygulanabilir araştırma kalite standartlarına uygun şekilde gerçekleştirilmesi tavsiye edilir. Veri işleme ve raporlama aşamaları sırasında, verinin doğru olduğundan emin olmak ve analiz, sonuç ve önerilerin veri ile tutarlı olduğundan emin olmak için ek kalite kontrollerinin yapılması tavsiye edilir.

Panel idare eden araştırmacıların panel üyelerinin profil verilerini herhangi bir zamanda güncellemesi ve gözden geçirmesi ve bunu düzenli olarak yapmalarının hatırlatılması tavsiye edilir. Panellerde çizilen örnekler güncel demografik bilgi içermesi tavsiye edilir. Bu hususta standart uygulamalar için iyi bir kaynak olarak "ISO 26362:2009 – Pazar, kamuoyu ve toplumsal araştırmalarda erişim panelleri" gösterilebilir

9. *Saklanan kişisel bilginin kullanılmak için toplandığı amaçtan öte, gerektiğinden daha fazla süre tutulmadığından veya daha ileri seviyede işlenmediğinden emin oluyor musunuz? Daha fazla gerekmediğinde tanımlayıcıları veri kayıtlarından kaldırmak veya ayrı olarak saklamak için prosedürlere sahip misiniz?*

Araştırmacıların veri saklama sürelerini mümkün olduğunca kısa belirlemesi tavsiye edilir. Fakat bu uygulanabilen yasaları temel alarak toplanan kişisel verinin kaynağına ve veri denetçisi veya veri işleyici olarak hareket etmelerine bağlıdır. İkinci durumda müşteriler sözleşmeyle veriyi tutma sürelerini düzenleyebilirler.

Kişisel verinin kaynağına bağlı olarak, uzun vadeli çalışmalara ait bilgi veya panelistler hakkında profil bilgisi tipik olarak kullanılacak ve aktif üye oldukları süre boyunca saklanacaktır. Aksine panele katılmayan geçici olarak araştırmada yer alan katılımcılar için daha kısa kişisel veri saklama süresi uygulanması tavsiye edilir. Açıkçası doğruluklarından emin olmak ve veri bütünlüğü gizlilik prensibini yerine getirmek için kalite kontrollerinin veri işleme aşamasında gerçekleştirilmesi gerektiğinden kişisel bilgiyi çok hızlı imha etmemek önemlidir.

Kişisel veri kullanıldığı zaman, araştırmacılar için en iyi uygulama takma adlı tanımlayıcılar kullanmalarıdır. Katılımcıların şirket içinde oluşturulmuş kimlik numaralarına karşılık gelen isimlerini adreslerini veya telefon numaralarına bağlayan bir ana dosya erişimin örnekleme veya panel yönetim elemanlarıyla gibi sınırlı bir kesimin erişiminde güvenli bir şekilde saklanmalıdır. Böylece katılımcı seviyesindeki veriyi işlemeye ihtiyacı olan araştırmacılar, veri işleyiciler veya kodlama personeli katılımcıların ismini, adreslerini veya telefon numaralarını görmeden de işlerini gerçekleştirilebilir.

Anket cevapları kümelenmiş şekilde işlendiğinde ve raporlandığında, cevapların katılımcılar hakkında istatiksel veri, kişisel veri, karşılık gelen takma adlı tanımlayıcılarla birlikte silinmesi tavsiye edilir. Böylelikle araştırma kuruluşu bundan böyle kişisel verileri tutmaz.

10. *Kişilerden topladığınız kişisel veriler hakkında bireylerden gelen taleplere karşılık yerinde prosedürler var mı? Prosedürleriniz kimlikleri doğrulama, taleplere makul bir sürede yanıt verme, doğru olmayan verileri düzeltmesine veya veriyi tamamen silmeye müsaade etme dahil bireylerin taleplerine erişimin idaresi için mi?*

Resmi prosedürlerin geliştirilmesi, iletilmesi ve kuruluşların haklarında tuttuğu kişisel verilere ulaşmak isteyen bireylere cevap verilmek için izlenmesi tavsiye edilir. Erişim talebinde bulunan bireylerin kimliklerinin doğrulanması, kişisel verinin diğer kişilere uygun olmayan şekillerde açıklanmasını önlemek için önemlidir.

Erişim talebinde bulunan bir bireyin -söz konusu kişisel veriye erişmek için yasal hakkı olduğunu iddia eden kişi- kimliği bir kez doğrulandığında araştırmacıların erişim talebini mümkün olduğunca hızlı şekilde karşılamak için gayret göstermesi tavsiye edilir. Örneğin yürürlükteki yasalara bağlı olarak 10 ila 30 gün içerisinde. Eğer araştırma firması talebi karşılamak için ek süreye ihtiyaç duyarsa, yasada belirtilen zaman sınırını bireye bildirimde bulunarak ve sebeplerin geçerli olduğunu belirterek uzatabilir. Örneğin istişare gerçekleştirmek veya talep edilen bilgiyi birden fazla veri tabanından toplamak için ek süre gerekebilir.

Veri koruma yasaları kuruluşların belli durumlarda bireylerin kişisel bilgiye erişimini reddetmesini gerektiren istisnalar içerebilirken, bu istisnaların pazar araştırmasına ilişkin kişisel bilginin işlenmesine etkisi büyük oranda yoktur. Örneğin eğer bilgi avukat-müvekkil imtiyazı altına giriyorsa kuruluşun yürürlükteki yasalar kuruluşun veriye erişim talebini reddetmesine olanak sağlar. Başka bir örnek belirtmek gerekirse, eğer kuruluş ulusal güvenlik veya hukuki yaptırım sebebiyle bir devlet kuruluşuna bilgi açıkladıysa, bu kurum kuruluşa verilen bilgi hakkında bilgi açıklamama veya bu bilgiye erişimi reddetme konusunda talimat verebilir.

11. *Kayıp, izinsiz erişim, imha, kullanım, değiştirilme ve açıklanma gibi risklere karşı her veri setini korumak için yerinde güvenlik protokolleri var mı?*

Bu sorumlulukları yerine getirmek kişisel bilgiyi ve diğer türlerdeki gizli bilgileri korumak için bir güvenlik politikası geliştirmek ve uygulamakla başlar. ISO 27001 üzerine kapsamlı bir güvenlik politikası temellendirilebilecek bir bilgi güvenlik standardı olarak tanınmıştır.

Gerekli korumayı sağlamak için uygun güvenlik önlemlerinin kullanımı şunları içerir:

- Fiziksel önlemler (kilitli dosya dolapları, ofislere sınırlı erişim, alarm sistemler, güvenlik kameraları)
- Teknolojik araçlar (şifreler, kriptolama, güvenlik duvarları)
- Organizasyonel kontroller (özgeçmiş kontrolleri, bilgisayarları çalışma sahasına çıkarmaya ilişkin kurallar, erişimi “bilinmesi gereken” temeliyle sınırlamak, personel eğitimi, müşteri ve alt yükleniciler ile yapılacak sözleşmeler)

Güvenlik politikasının aynı zamanda açıklanan kişisel veri içerisindeki potansiyel veri açıklarıyla ilgilenecek bir prosedür içermesi tavsiye edilir. Eğer veri, bir müşterinin veri tabanı gibi başka bir taraf tarafından toplanmış ve sağlanmışsa, o taraf derhal bilgilendirilmelidir. Verileri açıklanan katılımcılar bu açıklama kendilerine bir risk oluşturuyorsa (örn: kimlik hırsızlığı) bilgilendirilmelidirler ve bu riske karşı korumak için uygun adımlar atılmalıdır.

12. *Kişisel bilginin ne kadar tutulacağına dair açık bir ifade var mı?*

Kişisel verinin tutulma süresi bir araştırma projesinden ötekine 9. soruya daha evvel verilen yanıtlardaki durumların çeşitliliğine bağlı olarak değişebilir.

Genel veri tutma uygulamalarının gizlilik politikalarında yer alması tavsiye edilirken, farklı türlerdeki çalışmalar için kesin veri tutma süreleri belirlemek her zaman kullanışlı olmayabilir. Bu yüzden araştırmacılar veri tutma bilgisini çalışma takviye materyalleri, anket tanıtımları veya çalışmaya özel izin formlarında iletmeyi değerlendirmelidirler. Talep edilmesi durumunda verilen projede veri tutma süreleri iletmeye her zaman hazır olmaları tavsiye edilir.

5.4 Veri transferi

13. Kişisel verinin kullanımını ve açıklanmasını idare eden kuralları ve prosedürleri tanımladınız mı?

Bu kurallar ve prosedürler ülkenizdeki yerel gizlilik ve veri koruma yasalarında açıkça belirtilmiştir. Bunun açıklamasının personelin kişisel veriyi nasıl idare edeceğine dair prosedürleri uygulayabilmesi ve bu kurallara ve prosedürlere aşina olması için süreçlerle ve yazılı belgelerle açıkça belgelenmesi tavsiye edilir. Örneğin böyle bir veri müşterilere veya müşterinin şirketindeki araştırmacılara dahi açıklanmadan evvel araştırma katılımcısından izninin gerektiği prensibini içerecektir.

14. Hangi koşullar altında kişisel verinin açıklanacağı açık mı?

Araştırma katılımcıları kişisel verileriyle ne yapıldığını bilmelidirler ve bu ya sözlü olarak açıklanmalı veya yazılı şekilde veya katılımcıların onayladığı bir belgeyle sağlanmalıdır. Örneğin kendi izinleriyle kabul ettiklerini sözlü olarak ifade etmelerinin kanıt olarak kaydedilmesi.

15. Personelinizin bu kurallardan haberi var mı ve personeliniz prosedürleri nasıl kullanacağı konusunda eğitimli mi?

Gizlilik politikanız firmanızın veri toplama ve idare etme uygulamalarını tanımlar. Katılımcılara yapılan gizlilik sözlerinin tutulduğundan emin olmak için iç standart çalışma prosedürleri (SOPs) geliştirmek aynı oranda önemlidir.

Gizlilik hakkındaki personel eğitiminin yürürlükteki yasalara genel bir bakışı, mesleki davranış kurallarını, firmanızın tüketiciyi hedef alan gizlilik politikalarını ve SOP'leri içermesi tavsiye edilir. Gizlilik eğitiminin en azından yıllık olarak gerçekleşmesi ve katılım kayıtlarının saklanması tavsiye edilir.

Katılımcılarla iletişim kuran tüm ön saf personelinin şirketin politikalarını ve prosedürlerini iyi derecede açıklıyor olabilmesi tavsiye edilir. Cevap veremedikleri sorularda içeriden yardım almak için kimle iletişime geçeceklerini bilmeleri tavsiye edilir.

Prosedürlerin takip edildiğine dair bir çeşit takip dahil açık bir gözetim olması ve sorumlulukların ana hatlarıyla ifade edilmesi tavsiye edilir.

5.5 Kişisel verinin sınırlararası transferi

16. Eğer kişisel veri bir yetki alanından ötekine transfer edilecekse, bu kaynak ve hedef yetki alanlarındaki veri koruma gereksinimlerini karşılayacak şekilde mi yapılıyor?

Buna genel olarak "kişisel verinin sınırlararası transferi" olarak değinilir. Bu veri farklı ulusal sınırlar içerisinde toplandığında ve/veya veri işlemesi kıyıdan uzakta yapıldığında veya başka bir ülkeye yaptırıldığında ortaya çıkar. Örneğin bir müşteri başka bir ülkedeki bir araştırmacıdan kendi sağladığı müşteri veya hizmet kullanıcısı verisiyle bir çalışma gerçekleştirmesini istediğinde. Araştırmacıların uyması gereken, verinin nasıl idare edileceğine ve korunacağına dair her ülkenin kendi yasaları vardır. Bu karışık görünebilirken, eğer araştırmacıların karşılaştığı uygunluk sorunları üç ana soruna ayrılırsa bu kolaylık sağlar:

- Kişisel verinin sınırlararası transferinin yürürlükteki ulusal yasalara uygun şekilde gerçekleştirildiğinden emin olmak. Sınırlararası transferin uygun şekilde korunmasından emin olmak için en yaygın dayanak ya izin ya da uygun sözleşmesel maddelerin kullanılması ve yürürlükteki yasaların gerektirdiği yerlerde ulusal Veri Koruma Mercisinden veya diğer uygun gizlilik düzenleyici merciden bu sözleşmelerin kullanımı hakkında önceden onay alınmasıdır. Ek bir güvenlik önlemi olarak ve verinin sınırların dışında işlendiği durumda riski daha fazla azaltmak için uygulanabilen yerlerde tanımlayıcı kişisel verinin kaldırılması tavsiye edilir. Böylece sadece takma adlı kimlik numarası kişisel seviyedeki veriyi katılımcıların kimlikleriyle ilişkilendirebilir.

- Araştırmacıların müşterinin sağladığı örneklemi kullanarak çalışmayı gerçekleştirdiği durumlar gibi veri işleyici olarak görev aldığı ölçüde araştırmacılar sınırlararası transfer gerçekleştirebilir Araştırmacıların bu transferleri yöneten yasalara uyduğundan emin olduğu sınırlararası transferlerde bile veri kontrolcüsü adına hareket ederek veri işleyici olarak kişisel veriyi işlediklerinde veri kotrolcüsü olarak kontrol ettikleri ve projeyi nasıl gerçekleştirebileceklerini etkileyebilecek kişisel veriyi sınırlararası transfer edemeyebileceklerini akıllarında tutmaları tavsiye edilir. Yukarıdaki her iki taraf arasında yerinde bir yazılı anlaşma olması tavsiye edilir.
- Başka ülkelerdeki araştırma katılımcılarından kişisel veri toplandığı anda sınırlararası kişisel veri transferi; örneğin araştırmacının çalışmayı kontrol ettiği farklı ülkelerde yaşayan araştırma katılımcılarını hedef alan online anketler. Yürürlükteki gizlilik yasaları normal olarak araştırmacının yer aldığı ülkenin ulusal yasaları olacaktır. Ancak araştırmacı aynı zamanda çalışmanın veya panelin verinin toplandığı diğer ülkelerdeki yürürlükteki ulusal yasalara uyduğundan emin olmalıdır. Tavsiye edilen uygulamalar şunları içerir: (1) ülkesi dahil araştırmacının yasal bilgileri (şirket adı, posta kodu, vb) tüm veri toplama materyallerinde açıkça iletilmelidir; (2) kullanılan online gizlilik politikası çalışmada ve panelde yer alacak sınırlararası transferin anahatlarını ifade eden basit ve açık bir açıklama içerir; ve (3) paneldeki veri toplama izni sorusunda sınırlararası transfere değinilir.
-

5.6 Dış kaynak kullanımı ve alt yüklenici kullanma

17. *Kuruluş dışı veri işleyiciler veya diğer altyükleniciler için uygun gözetim dahil olmak üzere açık gereksinimler var mı?*

Kuruluş dılı tüm veri işleyicilerine veya altyüklenicilere herhangi bir türde veri transfer edilirken kişisel verilere ilişkin gerekli veri koruma kurallarını takip etmeleri için iletilmesi gereken açık gereksinimler olmalıdır. Kişisel veya kümelenmiş seviyede, verinin şifrelenmesi(kriptolanması) veya güvenli FTP transfer platformlarının kullanımı gibi ayrılmış IT süreçlerine herhangi bir verinin transferinde ek koruma olması tavsiye edilir. Eğer altyükleniciler veya kuruluş dışı veri işleyicileri yedek olarak herhangi bir veriyi kopyasını çıkarırsa, o zaman bu verinin saklanması süresince veriyi korumak için açık bir süreç olmalı ve daha fazla gerek olmadığında kopya veriler silinmelidir.

5.7 Gizlilik politikası

18. *Gizlilik ve kişisel veri koruma programınıza dair bilgi hazırda mevcut mu ve katılımcılar tarafından rahatça anlaşılabilecek bir formda mı?*

Birçok yetki alanı araştırma katılımcılarına hali hazırda mevcut olan gizlilik politikası bilgisi gerektirir. Gerekli içerik ve bilginin ülkeden ülkeye değişmesine rağmen araştırmacılar her zaman kendilerini araştırma katılımcılarına açıkça tanıtmalıdır ve araştırmanın amacını, kişisel verinin nasıl toplandığını, nasıl idare edileceğini (toplama, saklama, kullanma, erişim ve açıklama) ve nasıl daha fazla bilgi alabileceklerini veya bir şikayette bulunacaklarını açıkladıklarından emin olmalıdır.

Araştırmacılar politikaların rahatça anlaşıldığından, başlıkla ilişkili olduğundan, kolayca ulaşılabileceğinden, mümkün olduğunca az ve öz olduğundan ve kuruluşun faaliyetlerine göre oluşturulduğundan emin olmalıdır. Buna politikaları mümkün olduğunca çok dilde ulaşılabilir yapmak ve politikaları düzenli olarak gözden geçirmek ve uygulanabilir şekilde güncellemek dahildir.

19. *Veri kontrolcüsünün kimliği ve sorumluluğu açık mı?*

Araştırmacılar kişisel veri idaresine ilişkin kendi rollerinin ve sorumluluklarının araştırma katılımcılarına açıkça ifade edildiğinden emin olmalıdır. Buna kuruluş dışı veri işleyicilerin kullanılıp kullanılmadığı ve veri denetçisini tanımlamak da dahildir. Katılımcılar hangi kuruluşun verilerini idare konusunda tamamen güvenilir olduğu konusunda şüpheye düşürülmemelidir.

Bazı yetki bölgeleri aynı zamanda şirketin veri güvenlik uygulamaları için sorumluluğu yüklenen belirli bireyin tanımlanmasını gerektirir.

Müşterinin sağladığı örnekleri kullanan karartılmış anket durumunda katılımcılara görüşmenin başlangıcında müşterinin adının anket sonuna kadar açıklanmayacağını çünkü bu bilginin en başta açığa vurulmasının tepki yanlılığı yaratabileceği söylenmelidir. Birçok ulusal veri koruma yasası katılımcılara araştırmacının kişisel verilerini kimden elde ettiğini yasal olarak bilme hakkı verdiğinden, araştırmacılar, katılımcılardan gelecek talep üzerine müşterinin adını vermeye hazır olmalıdırlar.

20. *Verinin yeri fark etmeksizin veri denetçisinin kontrolü altındaki kişisel veri için güvenilir olduğu açık mı?*

Eğer veri işlemenin herhangi bir kısmın altyükleniciye vermeye yatkınsa veya kişisel veri kendi yetki alanı dışına transfer ediliyorsa, veri denetçisinin altyüklenicinin bilgilerini ve işleme konumlarını sağlamak için hazır olması tavsiye edilir; ve gerekli yerlerde veri denetçisinden önceden yazılı izin alınması tavsiye edilir. Araştırma ajansının veri denetçisi olduğu durumda, veri işleyicilerinin kullanımına ilişkin referans içermesi ve ilişkili olduğu yerlerde gizlilik politikalarında ülkeleri veya geniş bölgeleri listelemesi tavsiye edilir. Araştırmacılar bazı yetki alanlarının eşit seviyede veri koruma yasalarına sahip olmayan ülkelere veya bölgelere kişisel veri transfer etmesini yasakladığı konusunda dikkatli olmaları tavsiye edilir. İlgili yerel yasa tarafından şart tutulan sınırlararası transferleri yöneten kurallarla uyuma konu olarak kişisel bilgiyi çok uluslu bir grup içerisinde transfer edilmesine çoğu yetki alanında izin verilmektedir, ancak bazılarında hala verinin bulunabileceği konumlardaki veriye konu olan kişilere bildirim yapılması gereklidir.

6 Özel Durumlar

6.1 Çocuklardan veri toplanması

Ebeveyn izninin artık gerekmediğini belirleyen ulusal yaş sınırı kuralları oldukça değişkendir. Araştırmacılar ne zaman ebeveyn izninin gerektiğini veya hangi bölgelerde kültürel hassasiyetlerin bu şekilde yaklaşımı gerektirdiğini belirlemek için verinin toplanacağı yerdeki ulusal yasalara ve yetki alanlarındaki düzenleyici kurallara bakmalıdır. Ulusal yönetmeliklerin yokluğu halinde, Çocuklar ve gençlerle anket isimli ESOMAR yönetmeliğine başvurunuz.

Çocuklardan veri toplamak çocuğun yasal vasisinden doğrulanabilir izin gerektirir. Ebeveyn veya sorumlu yetişkine çocuğun katılımı hakkında bilgili bir şekilde karar vermesini sağlamak için araştırma projesi hakkında yeterli bilgi sağlanmalıdır. Araştırmacının sorumlu yetişkinin kimliğini ve çocuğun nesi olduğunu kaydetmesi tavsiye edilir.

6.2 İşletmeler arası araştırma

Önemli sayıda araştırma projesi işletmeler, okullar, kar amacı gütmeyen kuruluşlar ve benzer kuruluşlar gibi yasal kurumlardan veri toplamayı gerektirir. Bu tür araştırma genelde kuruluş hakkında çalışanların ücretleri, çalışan sayısı, sektör, konum gibi bilgilerin toplanmasını gerektirir.

Tüm bu örneklerde yer alan kuruluşların raporlamadaki kimlik açıklanmasına dair diğer türlerdeki araştırmalardaki bireylerle aynı seviyede korunması gereklidir.

Birçok ulusal veri koruma yasasının bireyin ünvanını ve işyeri iletişim bilgisini kişisel veri olarak değerlendirdiğini belirtmek kayda değerdir. Bazı veri koruma yasaları gereksinimlerini hem gerçek hem de tüzel kişilere uygulayarak daha ileri seviyeye ulaşır. (örneğin bireyler ve tüzel kişilikler)

6.3 Fotoğraflar, ses ve video kayıtları

Bir dizi yeni araştırma tekniği araştırma projesinin bir parçası olarak fotoğraf, ses ve video kaydı yaratır, saklar ve aktarır. Bu tür tekniklere iki önemli örnek etnografya ve gizli müşteridir.

Araştırmacılar fotoğrafları, ses ve video kayıtlarını kişisel veri olarak kabul etmeli ve bu şekilde idare etmelidir. Eğer araştırmacılar katılımcılardan bu formlarda bilgi sağlamalarını isterlerse, araştırmacıların aynı zamanda özellikle katılımcı olmayan kişilerden istenmeden toplanmış veri miktarını azaltmak için katılımcılara rehberlik etmesi tavsiye edilir.

Son olarak bazı gözlemsel araştırmalar kamu alanlarında araştırma katılımcısı olarak seçilmeyen kişileri içeren fotoğraflama, video ve ses kaydı almayı gerektirebilir. Bu tür durumlarda araştırmacılar bu görüntüleri paylaşabilmek için yüzleri açıkça görülen ve kimlikleri belirlenebilen bu bireylerden izin almalıdırlar. Eğer izin alınamıyorsa, bireyin görüntüsü piksellenmeli veya anonimleştirilmelidir. Buna ek olarak bölgenin gözlemlendiği konusunda bilgilendirmek için sorumlu birey veya kuruluşun iletişim bilgisiyle birlikte açık ve okunaklı işaretler konulmalıdır. Kameraların sadece gözlemlenmesi planlanan alanları görüntüleyecek şekilde yerleştirilmesi tavsiye edilir.

6.4 Bulut teknolojisiyle depolama

Kişisel veriyi bulut teknolojisiyle depolama kararının dikkatlice değerlendirilmesi tavsiye edilir. Araştırmacılar bulut teknolojisiyle depolama sağlayan hizmet sağlayıcısının güvenlik kontrollerini ve standart koşul ve şartlarını değerlendirmelidir. Birçok bulut depolama servis sağlayıcısı güvenlik ihlali ve kişisel verinin gizliliğinin ifşa olması halinde düşük tazminatlar önermektedir. Bu da araştırmacının firmasının bireylerin zarar görmesiyle sonuçlanacak ciddi güvenlik ihlallerinden doğacak ciddi finansal zarar riskiyle karşı karşıya kalacağı manasına gelir.

Bu yüzden araştırmacıların bu tür risklere karşı korunmak için telafi edici kontroller uygulaması tavsiye edilir. Örneğin hareket halindeyken (bulut alanına veya bulut alanından aktarılırken) veya saklanırken (bulut alanı sağlayıcının sunucularında saklanırken) kişisel veriyi kriptolamaları tavsiye edilir. Araştırmacıların aynı zamanda siber ortam mesuliyetine dair bir sigorta poliçesini değerlendirmeleri tavsiye edilir.

Araştırmacılar aynı zamanda bulut alanda saklamada veri aktarımının sınırlararası bir transfer olup olmadığını belirlemek için fiziksel konumları da göz önünde bulundurmalıdır. Bu konuda daha fazla bilgi için bu belgenin 5.5 nolu bölümüne başvurunuz. Bazı bulut alan hizmet sağlayıcıları bazı durumlarda uygun olabilecek ülkelere özgü saklama konumları önermektedir.

Son olarak araştırmacıların kişisel verileri halkında kullanımına açık bir bulut alan yerine özel bir bulut alanda saklamaları tavsiye edilir. Özel bulut alanlar belirli bir veri merkezinde araştırmacının firmasına adanmış özel teçhizata sahip olanlardır. Özel bulut alanın en önemli faydası araştırmacının kişisel verinin nerede olduğunu her daim bilmesidir. Aksine, halkın kullanımına açık bir bulut alan verinin iki veya daha fazla veri merkezinde ve iki veya daha fazla kıta üzerindeki sunucularda depolanmasına sebep olabilir. Böylece veri denetçilerinin kişisel verinin hangi konumda saklanması gerektiğini belirten ve yükümlü olduğu yürürlükteki veri koruma yasaları ve sözleşmelerle olası uygunluk sorunları ortaya çıkabilir.

6.5 Anonimleştirme ve takma ad kullanma

Araştırmacının veri koruma sorumluğunun anahtar noktası verinin müşteriye veya genel kamuoyuna sunulmadan evvel verideki kimliklerinin tanınmaz hale getirilmesidir. Anonimizasyon kişisel tanımlayıcıların silinmesi veya verinin bireylerin kimliklerinin teşhisine olanak vermeyecek şekilde değiştirilmesi yoluyla alınan koruyucu önlemlerden biridir.

Takma ad kullanma, kontrol amacıyla kişilerin bireysel verileri hala ayrı olarak saklanırken, kimlik numaraları kullanmak gibi verideki bireylerin hala ayırt edilmesini sağlayacak şekilde eşsiz bir tanımlayıcı kullanılmasını veya karım, algoritmayı içerir. (soru 9'a bakınız)

Bu tür teknikleri kullanırken araştırmacılar o veri için yasal anonimizasyon/takma ad kullanma yasal standartlarını yakalamakta hangi unsurların kaldırılması gerektiğini belirlemek için yerel ulusal ve düzenleyici yasalara başvurmalıdır.

7 KAYNAKLAR VE REFERANSLAR

DLA Piper, Data Protection Laws of the World (Dünya Veri Koruma Yasaları)

EphMRA Adverse Event Reporting Guidelines 2014 (EphMRA Olumsuz Durum Raporlama Yönetmelikleri 2014)

ICC/ESOMAR International Code on Market and Social Research (ICC/ESOMAR Pazar Araştırması ve Toplumsal Araştırmada Uluslar Arası Yasalar)

ESOMAR Interviewing Children and Young People Guideline (ESOMAR Çocuk ve Gençlerle Anket Kılavuzu)

ISO 26362:2009 – Access panels in market, opinion, and social research (Pazar, kamuoyu ve toplumsal araştırma erişim panelleri)

ISO 20252 – Market, Opinion and Social Research (Pazar, Kamuoyu ve Toplumsal Araştırma)

OECD Privacy Principles (OECD Gizlilik Prensipleri)

8 PROJE EKİBİ

Başkanlar:

- Reg Baker, ESOMAR Profesyonel Standartlar Komitesi ve Uluslar Arası Pazar Araştırması Enstitüsü Danışmanı
- David Stark, Doğruluk, Uygunluk ve Gizlilik, GfK, Başkan Yardımcısı
-

Proje Ekibi üyeleri:

- DebrahHarding, Yönetici, Pazar Araştırması Derneği
- Stephen Jenke, Danışman
- Kathy Joe, Uluslar Arası Standartlar ve İç işler Yöneticisi, ESOMAR
- Wander Meijer, Uluslar arası COO, MRops
- Ashlin Quirk, SSI Genel Danışmanlık
- Barry Ryan, Müdür, Uluslar arası Gizlilik - Program, Politika & Yönetim, American Express
- Jayne Van Souwe, Başkan, Wallis Danışma Grubu