Büyük Veri Dünyasında Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunmasına Dair Rehber İlkeler

www.coe.int/data-protection

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strazburg, 23 Ocak 2017 T-PD(2017)01

KİŞİSEL VERİLERİN OTOMATİK İŞLEME TUTULMASI KARŞISINDA BİREYLERİN KORUNMASI SÖZLEŞMESİ İSTİŞARE KOMİTESİ

BÜYÜK VERİ DÜNYASINDA KİŞİSEL VERİLERİN İŞLENMESİ KARŞISINDA BİREYLERİN KORUNMASINA DAİR REHBER İLKELER[1]

İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü

[1] Oy kullanan 50 üyeden yazılı usulle görüş alınmıştır: Danimarka, Lihtenştayn ve Lüksemburg çekimser kalmış, Almanya ve İrlanda ise itiraz etmiştir.

[2] İlk taslak ve sonraki sürümler Politecnico di Torino'da (İtalya) çalışan Profesör Alessandro Mantelero tarafından hazırlanmıştır.

I. Giriş

Büyük Veri, bilginin toplanması, birleştirilmesi ve analiz edilmesinde yeni bir paradigmayı temsil etmektedir. Nesnelerin interneti ve bulut bilişim gibi diğer teknolojik ortamlarla etkileşimden yararlanan Büyük Veri, toplum için önemli bir değer ve yenilik kaynağı olabilir; üretkenliği, kamu sektörü performansını ve toplumsal katılımı artırabilir.

Büyük Veri tarafından sağlanan değerli içgörüler, toplumun anlaşılma ve örgütlenme biçimini değiştirmektedir. Büyük veri bağlamında işlenen tüm veriler kişisel veriler ve insan etkileşimi ile ilgili değildir, ancak büyük bir kısmı, bireyleri ve kişisel verilerin işlenmesine ilişkin haklarını doğrudan etkiler.

Ayrıca, Büyük Veri, grupların ve toplulukların tutum örüntülerini belirlemek ve davranışlarını tahmin etmek için büyük miktarda veri toplamayı ve analiz etmeyi mümkün kıldığından, verilerin kullanımıyla ilgili risklerin kolektif boyutu da dikkate alınmalıdır.

Bu durum, Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması Sözleşmesi (CETS 108, bundan böyle "108 sayılı Sözleşme" olarak anılacaktır) Komitesini, Tarafların 108 sayılı Sözleşmenin ilke ve hükümlerini Büyük Veri bağlamında etkili kılmak üzere uygun politika ve tedbirleri uygulamaları için genel bir çerçeve sunan bu Rehber İlkeleri hazırlamaya yöneltmiştir.

Bu Rehber İlkeler, 108 sayılı Sözleşmenin ilkeleri temelinde ve devam etmekte olan modernizasyon süreci ışığında hazırlanmış olup, öncelikle Bölüm III'te tanımlandığı üzere kural koyuculara, kontrolörlere ve işleyicilere yöneliktir.

Bir kişinin kişisel verilerini ve bu verilerin işlenmesini kontrol etme hakkına dair kişisel özerkliğin korunmasının güvence altına alınması gerektiği düşünüldüğünde, bu kontrol hakkının niteliği Büyük Veri bağlamında dikkatle ele alınmalıdır.

Kontrol, kişisel verilerin kullanımı konusunda farkındalık ve gerçek bir seçim özgürlüğü gerektirir. Başta kişisel verilerin korunması temel hakkı olmak üzere temel hakların korunması için elzem olan bu koşullar farklı hukuki çözümlerle sağlanabilir. Bu çözümler, bireylerin bilgi eksikliği göz önünde bulundurularak, söz konusu sosyal ve teknolojik bağlama göre uyarlanmalıdır.

Bu nedenle, Büyük Veri uygulamalarının karmaşıklığı ve belirsizliği, kural koyucuları kontrol kavramını yalnızca bireysel kontrolle sınırlandırmayarak düşünmeye sevk etmelidir. Verilerin kullanımı üzerinde daha geniş bir kontrol fikrini benimsemeleri gerekir; buna göre bireysel kontrol, verilerin kullanımıyla ilgili risklerin çoklu etki değerlendirmesinin yapıldığı daha karmaşık bir süreçte gelişir.

II. Kapsam

Bu Rehber İlkeler, Tarafların, kontrolörlerin ve işleyicilerin, Büyük Veri kullanımının insan onuru, insan hakları ve temel bireysel ve kolektif özgürlükler üzerindeki olası olumsuz etkilerini önlemek için, özellikle kişisel verilerin korunmasına ilişkin olarak almaları gereken tedbirleri tavsiye etmektedir.

Büyük Verinin doğası ve kullanımları göz önüne alındığında, geleneksel veri işleme ilkelerinden bazılarının (örneğin, veri minimizasyonu, amaç sınırlaması, adillik ve şeffaflık ile özgür, belirli bir konuya özgü ve aydınlatılmış onam ilkesi) uygulanması bu teknolojik senaryoda zor olabilir. Bu nedenle bu Rehber İlkeler, Büyük Veri bağlamında uygulamada daha etkili olabilmeleri için 108 sayılı Sözleşme ilkelerinin özel bir biçimde uygulamasını önermektedir.

Bu Rehber İlkelerin amacı, veri sahiplerinin haklarına yönelik riskleri sınırlandırmak amacıyla geçerli veri koruma ilkelerini ve ilgili uygulamaları ortaya koyarak Büyük Veri bağlamında kişisel verilerin işlenmesine dair veri sahiplerinin korunmasına katkıda bulunmaktır. Bu riskler temel olarak veri analizinin olası yanlılığı, karar alma süreçlerinde Büyük Veri kullanımının yasal, toplumsal ve etik sonuçlarının hafife alınması ve bireylerin bu süreçlere etkin ve bilinçli katılımının marjinalleştirilmesi ile ilgilidir.

Çeşitli sektörlere özgü uygulamalarda Büyük Verinin yaygınlaşması göz önüne alındığında, mevcut Rehber İlkeler, Büyük Verinin belirli uygulama alanlarında (örneğin sağlık sektörü, finans sektörü, kolluk kuvvetleri gibi kamu sektörü) bireylerin korunmasına ilişkin daha fazla yönlendirme ve özel en iyi uygulama örnekleriyle tamamlanabilecek genel bir rehberlik sağlar.

Ayrıca, teknolojilerin ve kullanımlarının gelişimi ışığında, Rehber İlkelerin mevcut metni, 108 sayılı Sözleşme Komitesi tarafından gerekli görüldüğü takdirde gelecekte yeniden gözden geçirilebilir.

Bu Rehber İlkelerde yer alan hiçbir unsur 108 sayılı Sözleşme ve Avrupa İnsan Hakları Sözleşmesi hükümlerini engelleyici veya sınırlayıcı olarak yorumlanamaz.

III. Rehber ilkeler içinde kullanılan terminoloji

a) **Büyük Veri**: Büyük Verinin, söz konusu disipline bağlı olarak farklılık gösteren birçok tanımı vardır. Bunların çoğu, büyük hacimli, hızlı ve çeşitli verilerden yeni ve tahmine dayalı bilgi toplama ve çıkarma konusunda artan teknolojik beceriye odaklanmaktadır.[3] Veri koruma açısından, ana konular yalnızca işlenen verilerin hacmi, hızı ve çeşitliliği ile ilgili değil, aynı zamanda bireyler ve gruplarla ilgili karar verme amacıyla yeni ve tahmine dayalı bilgi çıkarmak için verilerin yazılım kullanılarak analiz edilmesiyle de ilgilidir. Bu Rehberin amaçları doğrultusunda, Büyük Veri tanımı hem Büyük Veriyi hem de Büyük Veri analitiğini kapsamaktadır.[4]

b) **Dosya Yöneticisi (Kontrolör)**: Tek başına veya başkalarıyla birlikte veri işleme konusunda karar verme yetkisine sahip olan gerçek veya tüzel kişi, kamu otoritesi, kamu görevlisi, ajans veya diğer herhangi bir organ.

c) **İşleyici**: Kontrolör adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu otoritesi, hizmet, ajans veya diğer herhangi bir organ.

d) **İşleme**: Kişisel verilerin toplanması, depolanması, saklanması, değiştirilmesi, geri alınması, ifşa edilmesi, kullanıma sunulması, silinmesi veya imha edilmesi ya da bu veriler üzerinde mantıksal ve/veya aritmetiksel işlemlerin gerçekleştirilmesi gibi kişisel veriler üzerinde gerçekleştirilen herhangi bir işlem veya işlemler dizisi.

e) **Takma ad verme (Psödonim)**: Kişisel verilerin, söz konusu ek bilgilerin ayrı tutulması ve kişisel verilerin kimliği belirli veya belirlenebilir bir gerçek kişiye atfedilmemesini sağlamak için teknik ve organizasyonel önlemlere tabi olması sayesinde, ek bilgiler kullanılmadan artık belirli bir veri sahibiyle ilişkilendirilemeyeceği şekilde işlenmesi anlamına gelir.

f) **Açık veri**: Açık lisansların koşullarına göre herhangi bir amaç için herkes tarafından serbestçe kullanılabilen, değiştirilebilen, paylaşılabilen ve yeniden kullanılabilen kamuya açık her türlü bilgi.

g) **Taraflar**: 108 sayılı Sözleşme ile yasal olarak bağlı olan taraflar.

h) **Kişisel veri**: Tanımlanmış veya tanımlanabilir bir bireyle (veri sahibi) ilgili her türlü bilgi.[5]

i) **Hassas veriler**: 108 sayılı Sözleşme'nin 6. Maddesi kapsamına giren ve işlendiklerinde tamamlayıcı uygun güvenceler gerektiren özel veri kategorileri.[6]

j) **Denetim makamı**: Bir Tarafça kurulan ve 108 sayılı Sözleşme hükümlerine uyulmasını sağlamaktan sorumlu makam.

[3] "Büyük Veri" terimi genellikle veri örüntüleri, eğilimleri ve korelasyonları hakkında çıkarımlar elde etmek için hesaplamayla analiz edilebilen son derece büyük veri setlerini tanımlar. Uluslararası Telekomünikasyon Birliği'ne (ITU) göre Büyük Veri, "heterojen özellikler gösteren kapsamlı veri kümelerinin potansiyel olarak gerçek zamanlı kısıtlamalar altında toplanmasını, depolanmasını, yönetilmesini, analiz edilmesini ve görselleştirilmesini sağlayan bir paradigmadır" (ITU. 2015. Recommendation Y.3600. (Tavsiye) Big data – Cloud computing based requirements and capabilities).

[4] Bu terim, gizli örüntüleri, eğilimleri ve korelasyonları ortaya çıkarmak için büyük miktarda veriyi analiz eden hesaplama teknolojilerini tanımlamak için kullanılır. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'na (ENISA) göre, Büyük Veri analitiği terimi "örüntüleri keşfetmek, durumları ortaya çıkarmak, davranışları tahmin etmek ve anlamak için verilerin toplanması, düzenlenmesi ve analiz edilmesine yönelik tüm veri yönetimi yaşam döngüsünü ifade eder" (ENISA. 2015. Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics).

[5] Bu tanıma göre, kişisel veriler aynı zamanda kişileri veri setlerinden ayırmak, grup profilleme bilgilerine dayanarak onları etkileyen kararlar almak için kullanılan her türlü bilgidir.

[6] Büyük veri bağlamında, bu durum özellikle daha fazla işlenen veya diğer verilerle birleştirilen kişisel veriler üzerinden ortaya çıkarılan ırk veya etnik köken, siyasi görüşler, sendika üyeliği, dini veya diğer inançlar, sağlık veya cinsel yaşamla ilgili bilgiler için geçerlidir.

IV. İlkeler ve Rehber İlkeler

1. Verilerin etik ve sosyal farkındalık içinde kullanımı

1.1 Kişisel verilerin işlenmesinde ilgili tüm çıkarların dengelenmesi ihtiyacına göre ve özellikle bilgilerin karar alma süreçlerinde tahmin amaçlı kullanıldığı durumlarda, kontrolörler ve işlemciler, insan haklarını ve temel özgürlükleri korumak ve 108 sayılı Sözleşmede belirtilen veri koruma yükümlülüklerine uyulmasını sağlamak için, hedeflenen Büyük Veri işlemenin olası etkisini ve bunun daha geniş etik ve sosyal sonuçlarını yeterince dikkate almalıdır.

1.2 Kişisel verilerin işlenmesi, ilgili topluluk veya topluluklarda yaygın olarak kabul edilen etik değerlerle çelişmemeli ve insan haklarının korunması da dahil olmak üzere toplumsal çıkarlara, değerlere ve normlara halel getirmemelidir. Bağlamsal unsurların etkisi nedeniyle katı kurallara dayalı bir etik rehberlikten söz etmek sorunlu olsa da, ortak yol gösterici etik değerler Avrupa İnsan Hakları Sözleşmesi benzeri uluslararası insan hakları ve temel özgürlükler sözleşmelerinde bulunabilir.

1.3 Bölüm IV.2'de açıklandığı gibi bir veri işlemenin olası etkisinin değerlendirilmesi, Büyük Veri kullanımının etik değerler üzerindeki etkisinin yüksek olduğunu gösteriyorsa, kontrolörler, verilerin kullanımında korunması gereken belirli etik değerleri belirlemek için geçici bir etik komitesi kurabilir veya mevcut etik değerlerden yararlanabilir. Etik kurul, yetkinlik, deneyim ve mesleki niteliklerine göre seçilen ve görevlerini tarafsız ve objektif bir şekilde yerine getiren üyelerden oluşan bağımsız bir organ olmalıdır.

2. Önleyici politikalar ve risk değerlendirmesi

2.1 Veri işlemenin artan karmaşıklığı ve Büyük Verinin dönüştürücü kullanımı göz önünde bulundurulduğunda, Taraflar bu alanda veri korumasını düzenlerken ihtiyati bir yaklaşım benimsemelidir.

2.2 Kontrolörler, kişisel verilerin işlenmesine ilişkin olarak kişilerin korunmasını sağlamak için Büyük Veri kullanımının riskleri ve bunun bireyler ve toplum üzerindeki etkilerine ilişkin önleyici politikalar benimsemelidir.

2.3 Büyük Verinin kullanımı sadece bireysel gizlilik ve veri korumasını değil, aynı zamanda bu hakların kolektif boyutunu da etkileyebileceğinden, önleyici politikalar ve risk değerlendirmesi, eşit muamele ve ayrımcılık yapmama hakkı da dahil olmak üzere Büyük Veri kullanımının yasal, sosyal ve etik etkilerini dikkate almalıdır.

2.4 Sözleşme 108 sayılı Sözleşmede yer alan veri işlemenin meşruiyeti ve veri kalitesi ilkelerine ve veri işlemenin veri sahiplerinin hakları ve temel özgürlükleri üzerindeki etkisini önleme veya en aza indirme yükümlülüğüne uygun olarak, veri işlemenin temel hak ve özgürlükler üzerindeki olası etkisinin bir risk değerlendirmesinin yapılması, bu hak ve özgürlüklerin korunmasını Büyük Veri kullanımından etkilenen farklı çıkarlarla dengelemek için gereklidir.

2.5 Kontrolörler, istenen veri işleme etkinliğinin veri sahiplerinin hakları ve temel özgürlükleri üzerindeki olası etkilerini aşağıdaki amaçlarla incelemelidir:

1) Büyük Veri içeren her bir işleme etkinliğinin risklerini ve bireylerin hakları ve temel özgürlükleri, özellikle de kişisel verilerin korunması hakkı ve ayrımcılık yapmama hakkı üzerindeki olası olumsuz sonuçlarını, sosyal ve etik etkileri de dikkate alarak belirlemek ve değerlendirmek.
2) Bu riskleri azaltmak için "tasarım gereği (by-design)" ve "varsayılan ayarlarla (by-default)"[7] çözümler gibi uygun önlemler geliştirmek ve sağlamak.
3) Sunulan çözümlerin benimsenmesini ve etkinliğini izlemek.

2.6 Bu değerlendirme süreci, yasal, sosyal, etik ve teknik boyutlar da dahil olmak üzere farklı etkileri değerlendirmek için yeterli mesleki niteliklere ve bilgiye sahip kişiler tarafından yürütülmelidir.

[7] Veri koruma bağlamında, "tasarım gereği" ve "varsayılan" terimleri, yasal ilkeleri etkili bir şekilde uygulamak ve veri koruma önlemlerini ürün ve hizmetlere yerleştirmek için en erken tasarım aşamalarından itibaren tüm veri yönetimi süreci boyunca dikkate alınan uygun teknik ve organizasyonel önlemleri ifade eder. Veri korumaya yönelik "varsayılan ayarlarla" yaklaşımına göre, veri koruma haklarını koruyan önlemler varsayılan ayarlar içindedir ve özellikle yalnızca belirli bir işleme için gerekli olan kişisel bilgilerin işlenmesini sağlarlar.

2.7 Temel hakları etkileyebilecek Büyük Veri kullanımı ile ilgili olarak Taraflar, farklı paydaşların (örneğin Büyük Veri kullanımından etkilenmesi olası bireyler veya gruplar) bu değerlendirme sürecine ve veri işleme tasarımına katılımını teşvik etmelidir.

2.8 Büyük Veri kullanımının veri sahiplerinin haklarını ve temel özgürlüklerini önemli ölçüde etkileyebileceği durumlarda, kontrolörler 2.5 paragrafında atıfta bulunulan risklerin azaltılması için tavsiye almak üzere denetim makamlarına danışmalı ve bu makamların yönlendirmesinden yararlanmalıdır.

2.9 Kontrolörler, değerlendirme sürecinin sonuçlarını düzenli olarak gözden geçirmelidir.

2.10 Kontrolörler değerlendirmeyi ve paragraf 2.5'te atıfta bulunulan çözümleri belgelendirmelidir.

2.11 Kontrolörler tarafından paragraf 2.5'te atıfta bulunulan riskleri azaltmak için alınan tedbirler, olası idari yaptırımların değerlendirilmesinde dikkate alınmalıdır.

3. Amaç sınırlaması ve şeffaflık

3.1 Kişisel veriler belirli ve meşru amaçlar için işlenmeli ve bu amaçlarla bağdaşmayacak şekilde kullanılmamalıdır. Kişisel veriler, veri sahibinin beklenmedik, uygunsuz veya başka bir şekilde sakıncalı olarak değerlendirebileceği bir şekilde işlenmemelidir. Veri sahiplerinin başlangıçtaki amaçların öngördüğünden farklı veya daha büyük risklere maruz bırakılması, verilerin beklenmedik bir şekilde daha fazla işlenmesi durumu olarak değerlendirilebilir.

3.2 Büyük Veri kullanımının dönüştürücü niteliği göz önüne alındığında ve özgür, belirli, aydınlatılmış ve açık onam gerekliliği ile amaç sınırlaması, adillik ve şeffaflık ilkelerine uymak için, kontrolörler ayrıca verilerin farklı kullanımlarının bireyler üzerindeki olası etkisini belirlemeli ve veri sahiplerini bu etki hakkında bilgilendirmelidir.

3.3 Veri işlemenin şeffaflığı ilkesi uyarınca, Bölüm IV.2'de açıklanan değerlendirme sürecinin sonuçları, kanunla korunan gizlilik saklı kalmak kaydıyla kamuya açık hale getirilmelidir. Bu tür bir gizliliğin varlığı halinde, kontrolörler gizli bilgileri değerlendirme raporunun ayrı bir ekinde sunarlar. Bu ek kamuya açık olmayacaktır ancak denetim makamları tarafından erişilebilir.

4. Tasarım gereği çözüm (By-design) yaklaşımı

4.1 Bölüm IV.2'de açıklanan değerlendirme süreci temelinde, kontrolörler ve uygulanabilir olduğu hallerde işleyiciler Büyük Verilerin işlenmesinin farklı aşamalarında uygun tasarım gereği mevcut çözümlerini benimseyecektir.

4.2 Kontrolörler ve uygun olduğu hallerde işleyiciler hem toplama hem de analiz aşamalarında, gereksiz veya marjinal verilerin varlığını en aza indirmek, olası gizli veri yanlılığından ve ayrımcılık veya veri sahiplerinin hakları ve temel özgürlükleri üzerinde olumsuz etki riskinden kaçınmak için veri işleme tasarımlarını dikkatlice değerlendirmelidir.

4.3 Teknik olarak mümkün olduğunda, kontrolörler ve uygulanabilir olduğu durumlarda işlemciler, daha büyük ölçekte kullanılmadan önce simülasyonlar yoluyla sınırlı miktarda veri üzerinde benimsenen tasarım gereği mevcut çözümlerinin yeterliliğini test etmelidir. Bu, verilerin analizinde farklı parametrelerin kullanımının olası yanlılığını değerlendirmeyi ve bilgi kullanımını en aza indirmeyi olanaklı hale getirecek ve Bölüm IV.2'de açıklanan risk değerlendirme sürecinde belirlenen olası olumsuz sonuçları azaltmak için kanıt sağlayacaktır.

4.4 Hassas verilerin kullanımıyla ilgili olarak, hassas olmayan verilerin hassas bilgileri çıkarmak için kullanılmasını mümkün olduğunca önlemek ve bunların kullanılmaları halinde, hassas veriler için benimsenen aynı güvenceleri bu verilere de uygulamak için tasarım gereği mevcut çözümler benimsenmelidir.

4.5 İlgili veri koruma ilkelerinin uygulanmasından muaf tutmayan takma isimlendirme tedbirleri, veri sahiplerine yönelik riskleri azaltabilir.

5. Onam

5.1 Özgür, belirli, aydınlatılmış ve açık onam, veri işlemenin şeffaflığı ilkesine göre veri sahibine sağlanan bilgilere dayanacaktır. Büyük Veri kullanımının karmaşıklığı göz önüne alındığında,

bu bilgiler Bölüm IV.2'de açıklanan değerlendirme sürecinin sonuçlarını kapsayacak ve deneyimden öğrenme yaklaşımıyla veri kullanımının sonuçlarını ve veri sahibi üzerindeki olası etkisini simüle eden bir arayüz aracılığıyla da sağlanabilecektir.

5.2 Veriler, veri sahibinin onamına dayalı olarak toplandığında, kontrolörler ve uygun olduğu hallerde işleyiciler, veri sahiplerinin başlangıçtaki amaçlarla uyumlu olmayan veri işlemeye tepki göstermeleri ve onamlarını geri çekmeleri için kolay ve kullanıcı dostu teknik yollar sağlamalıdır.

5.3 Veri sahibi ile kontrolör arasında veri sahibinin işleme faaliyetine ilişkin kararlarını etkileyen açık bir güç dengesizliği varsa onam özgürce verilmiş sayılmaz. Veri sorumlusu bu dengesizliğin mevcut olmadığını veya veri sahibi tarafından verilen onamı etkilemediğini göstermelidir.

6. Anonimleştirme

6.1 Veriler, bireylerin tanımlanmasına veya yeniden tanımlanmasına olanak sağladığı sürece, veri koruma ilkeleri uygulanmalıdır.

6.2 Kontrolör verilerin niteliği, kullanım bağlamı, mevcut yeniden kimlik belirleme teknolojileri ve ilgili maliyetler ışığında gereken zaman, çaba veya kaynakları dikkate alarak yeniden kimlik belirleme riskini değerlendirmelidir. Veri sorumluları, verileri anonim hale getirmek ve anonimleştirmenin etkin hale getirilmesini sağlamak için benimsenen önlemlerin yeterliliğini göstermelidir.

6.3 Teknik önlemler, ilgili kişilerin olası yeniden tanımlanmasını önlemek için yasal veya sözleşmesel yükümlülüklerle birleştirilebilir.

6.4 Kontrolörler, anonimleştirme tekniklerine ilişkin teknolojik gelişmeler ışığında yeniden kimlik belirleme riskinin değerlendirmesini düzenli olarak gözden geçirmelidir.

7. Büyük Veri destekli kararlarda insan müdahalesinin rolü

7.1 Büyük Veri kullanımı, karar alma sürecinde insan müdahalesinin özerkliğini korumalıdır.

7.2 Büyük Veri analitiği tarafından sağlanan sonuçlara dayanan kararlar, veriyle ilgili tüm koşulları dikkate almalı ve tek başına bağlamından koparılmış bilgilere veya veri işleme sonuçlarına dayanmamalıdır.

7.3 Büyük Veriye dayalı kararların bireysel hakları önemli ölçüde etkileyebileceği veya yasal etkiler doğurabileceği durumlarda, insan karar verici, veri sahibinin talebi üzerine, bu gerekçenin veri sahibi için sonuçları da dahil olmak üzere, veri işlemenin altında yatan gerekçeyi kendisine sunmalıdır.

7.4 Makul argümanlar temelinde, insan karar vericiye Büyük Veri kullanılarak elde edilen tavsiyelerin sonucuna güvenmeme özgürlüğü tanınmalıdır.

7.5 Büyük Veri analizine dayalı olarak doğrudan veya dolaylı ayrımcılık yapıldığının varsayılabileceği belirtilerin olduğu durumlarda, kontrolörler ve işleyiciler ayrımcılık yapılmadığını göstermelidir.

7.6 Büyük Veriye dayalı bir karardan etkilenen kişiler, bu karara yetkili bir makam önünde itiraz etme hakkına sahiptir.

8. Açık veri

8.1 Büyük Veri analitiğinin kullanılabilirliği göz önüne alındığında, açık veri verileri bireyler ve gruplar hakkında çıkarımlar elde etmek için kullanılabileceğinden, kamu ve özel kuruluşlar kişisel verilerle ilgili açık veri politikalarını dikkatle değerlendirmelidir.

8.2 Veri Sorumluları açık veri politikalarını benimsediklerinde, bölüm IV.2'de açıklanan değerlendirme süreci, 6. paragrafta atıfta bulunulan hükümler ışığında, farklı açık veri setlerine ait farklı verilerin birleştirilmesi ve madenciliğinin yapılmasının etkilerini de dikkate almalıdır.

9. Eğitim

Bireylerin Büyük Veri bağlamında bilgi ve Kişisel Veri kullanımının sonuçlarını anlamalarına yardımcı olmak için Taraflar bilgi ve dijital okuryazarlığı temel bir eğitim becerisi olarak değerlendirmelidir.

Büyük Veri, toplumun anlaşılma biçimini değiştiriyor. Değerli içgörüler sunuyor; üretkenliği ve toplumsal katılımı artırarak yenilikçilik için fırsatlar sağlıyor.

Rehber İlkeler, kişisel verilerin işlenmesini içeren Büyük Veri üzerine hazırlanmıştır ve kişilerin dijital ekonomilerimizin merkezine yerleştirilmesi ile temel hak ve özgürlüklerinin korunmasını sağlamak için politika yapıcılara ve bu tür verileri işleyen kuruluşlara yardımcı olmayı amaçlamaktadır.

Büyük Verinin doğası, amaç sınırlaması veya veri minimizasyonu gibi geleneksel kişisel veri koruma ilkelerinin uygulanmasını etkileyebilir, bu nedenle Rehber İlkeler ilgili kişiler için güvence sağlamayı amaçlar. Örneğin, kişisel özerkliğin ve kişisel verileri kontrol etme hakkının teminat altına alınması ve Büyük Veri bağlamında bireyler tarafından kullanılabilmesinin sağlanması büyük önem taşımaktadır.

TR

www.coe.int

Avrupa Konseyi kıtanın önde gelen insan hakları örgütüdür. 28'i Avrupa Birliği üyesi olmak üzere 47 üye ülkeden oluşmaktadır. Tüm Avrupa Konseyi üye devletleri, insan hakları, demokrasi ve hukukun üstünlüğünü korumak üzere tasarlanmış bir antlaşma olan Avrupa İnsan Hakları Sözleşmesini imzalamışlardır. Avrupa İnsan Hakları Mahkemesi Sözleşmenin üye devletlerde uygulanmasını denetler.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE