



Uluslararası İnsan Hakları
Çerçevesine Uyumun
İzlenmesi için

ETKİNİZ
AB PROGRAMI

İnsan Hakları Veritabanları

Etkiniz İnsan Hakları İzleme Araç Kutusu E-Öğrenme
Modülü

**Bu sunum, Etkiniz Uluslararası uzmanı Veronica Yates tarafından hazırlanmış, ETAT tarafından Türkçeleştirilmiştir.*



Neden bir insan hakları veri tabanı?

İnsan hakları ihlallerine ilişkin kanıt toplamak amacıyla

- BM gibi uluslararası kuruluşlara rapor verin;
- Politika ve savunuculuğun değişimi için kampanya yürütün;
- Uluslararası kurumlara yapılan şikayetleri takip edin;
- Mahkeme süreçlerini takip edin;
- Tarihi gerçekleri korumak, hesap verebilirlik, arşivleme, hafıza ve hikaye anlatımı için.

Kimin için?

Veritabanını kimlerin kullanacağını (veya kullanabileceğini) akılda tutmak önemlidir. İlk adım bilgileri tek bir yerde depolamak olsa da, birçok kişi veritabanını bir dizi faaliyet için kullanabilir (daha önce de belirtildiği gibi). Kullanıcı örnekleri şunları içerir:

- İnsan hakları araştırmacıları
- Kampanyacılar ve aktivistler
- Avukatlar
- Politika Yapıcılar
- Akademisyenler
- Gazeteciler
- BM personeli ve uzmanları
- Hükümet personeli



2. Veritabanı için temel unsurlar

Veri tabanı için toplanacak bilgiler şunları içerir:

- ne oldu, nerede ve ne zaman;
- Hangi anlaşma veya sözleşme kapsamında hangi spesifik hakların ihlal edildiği de dahil olmak üzere, işlenen olası insan hakları ihlalleri;
- ilgili kişiler: hangi fail olduğu iddia edilen kişi hangi ihlale maruz kalan hak sahibia ne yaptı, bilgi kaynakları nelerdir ve hangi müdahaleler yapıldı?

Bilgi kaynakları

Bilgi toplarken, genellikle birincil belgelere ve ikincil belgelere sahip olursunuz.

Birincil belgeler bilgi toplama faaliyetlerinden, kişilerden ve resmi belgelerden gelebilir;

İkincil belgeler, haber raporları, olayla ilgili kitaplar gibi birincil belgelere dayanarak üretilenleri ifade eder.

Önemli.

Çalışmanız ulusal veya uluslararası düzeyde yasal ve politika değişikliği de dahil olmak üzere hesap verebilirlik ve adalet arayışındaysa, birincil bilgi kaynaklarından kanıt sağlamanız gerekecektir. İkincil bilgiler genellikle teyit edilmiş bilgiler olarak değil, takip edilmesi gereken ipuçları olarak değerlendirilir.



3. İnsan hakları izlemenin temel ilkeleri

GENEL: Çalışmalarınızdan etkilenen nüfuslar üzerinde eylemlerinizin olumsuz sonuçlarını önlemek ve hafifletmek için önlemler alınması anlamına gelen '**Zarar vermeme**' ilkesine uymalısınız.

İzleme ilkeleri şunları içerir:

- Doğruluk ve kesinlik sağlayın - ihlaller iyi belgelenmiş bilgilerle desteklenmelidir;
- Doğrulama ve kanıt standardı - raporlar doğrulanan bilgilere, yani ilk kanıtları teyit eden bilgilere dayanılarak yazılmalıdır;
- Gizliliğe saygı gösterin - bu ilkenin herhangi bir şekilde ihlal edilmesi, ilgili kişiler için çok ciddi sonuçlar doğurabilir;
- Görüşülen herkesin bilgilendirilmiş onamının alındığından emin olun;
- İlgili kişilerin Güvenlik Standartları dikkate alınmalıdır;
- Tutarlılığı takip edin - Bilgiler tutarlı bir şekilde ve çeşitli kaynaklardan toplanmalıdır. Topladığınız bilgilerin nasıl doğrulandığını da detaylandırmanız önemlidir;
- Hassasiyetle davranın - İhlale maruz kalan hak sahibilerle veya akrabalarıyla ya da ihlale maruz kalan hak sahibilere ve tanıklara yakın diğer kişilerle görüşme yapıyorsanız, bir bireyin yaşamış olabileceği acılara karşı hassas olmalısınız.



4. Veritabanını nasıl oluşturacağız / Teknik hususlar

1. Bir veritabanı yönetim sistemi seçme

Yeni bir veritabanı oluştururken izleyebileceğiniz temelde iki yol vardır: kendi veritabanınızı oluşturmak veya mevcut bir sistemi kullanmak. Kendi veritabanınızı oluşturabilir veya mevcut bir veritabanı uygulamasını kullanabilirsiniz.

2. Bilgilerin sınıflandırılması

En azından şunları eklemek isteyeceksiniz:

- Konum/coğrafya
- Etkinlik tarihi
- İhlale maruz kalan hak sahibi(lar)
- İhlal türü
- Fail(ler)
- Etkilenen haklar
- Alınan önlemler / takip

3. Kamuya açık ve gizli bilgiler: Yaptığınız izlemenin türüne ve amacına bağlı olarak, toplanan bazı bilgilerin, devam eden bir soruşturma nedeniyle, güvenlik nedenleriyle veya diğer nedenlerle kamuya açık taraftan gizli tutulması gerekebilir.



5. Siber güvenlikle ilgili endişeler

Hangi teknolojiyi seçeceğinizden, tutulduğu yerin ne kadar güvenli olduğuna ve izleme faaliyetlerinde kendi güvenliğinize kadar veritabanı çalışmasıyla ilgili tüm hususları dikkate almak isteyeceksiniz. Kendinize sormanız gereken birkaç soru şunlardır:

- Nerede barındırılıyor? Kendi sunucunuz (daimi teknik personeliniz yoksa muhtemelen olası değildir), yoksa nerede barındırılıyor? Sunucuların sahibi kim? Hangi ülkelerde bulunuyorlar? Dikkate almamız gereken gizlilik sorunları var mı?
- Sunucunun güvenlik etkileri nelerdir, verilerin gizliliği, harici bir taraf bilgileri ele geçirebilir mi, özel bir veritabanı nda barındırılıyorsa, verilerin sahibi siz misiniz?
- Veritabanının kendisi güvenli mi? Bu, açık kaynağa karşı özel mülkiyete bağlı olabilir, eğer özel mülkiyet ise, şirketin veriler üzerinde herhangi bir erişimi var mı, sahibi mi, alabilir mi?
- Erişim: veritabanının arka ucuna kimin erişimi var, erişimi kim veriyor? Her yerden, telefonlarından ve bilgisayarlarından erişebilirler mi?
- İhlale maruz kalan hak sahiplerin, tanıkların ve diğer hassas kişilerin gizli bilgilerini nasıl koruyorsunuz?
- Bir kesinti veya saldırı durumunda yedek bir sistem var mı?



Uluslararası İnsan Hakları
Çerçevesine Uyumun
İzlenmesi için

ETKİNİZ

AB PROGRAMI

www.etkiniz.eu
destek@Etkiniz.eu
Instagram: etkiniz
Twitter: etkinizab