

Sendika ve Sivil Toplum Kuruluşları için Veri Güvenliği Protokolü

Son Güncelleme: 22 Ocak 2026

Sendika/STK Veri Güvenliği Protokolü, Open Supply Hub'ın mevcut yönetim ve hesap verebilirlik çerçeveleriyle birlikte uygulanır ([Safeguarding Policy](#) ve [Whistleblower Policy](#)). Bu politikalar birlikte, risklerin belirlenmesi, endişelerin dile getirilmesi, zararların raporlanması ve uygun durumlarda telafi yollarının aranması için birbirini tamamlayan ve güçlendiren mekanizmalar oluşturur.

I. Amaç

Bu protokol, Open Supply Hub'ın (OS Hub), platformda veri paylaşımı konusunda sendika ve sivil toplum kuruluşları (STK) ile nasıl çalışmayı amaçladığını özetlemektedir.

Bu politika, OS Hub'ın 2025 tarihli [Beyond Transparency](#) raporuna dayanır. (Raporun Türkçe özetine [buradan](#) ulaşılabilir). Söz konusu rapor, sendika ve STK'lardan alınan temel görüşleri yansıtarak, OS Hub gibi dijital tedarik zinciri hesap verebilirlik araçlarının bu aktörlerden gelen verileri nasıl ele alması gerektiğine – özellikle güven, güvenlik, rıza ve karşılıklılığı sağlayacak biçimde – ışık tutmuştur.

Bu politika, OS Hub'ın [Kullanım Koşulları ve Veri Kullanım Politikalarını](#) tamamlar; ancak onların yerine geçmez. Bu tarihten önce sendika ve STK'lar tarafından yüklenen veriler bu süreç kapsamında incelenmiş veya incelenmemiş olabilir. Bundan sonraki tüm veri katkıları ise bu politikaya tabi olacaktır.

OS Hub, geri bildirimlere dayanarak bu politikayı geliştirmeye ve güncellemeye devam edecektir. Yorum veya önerilerinizi bu [geri bildirim formu](#) aracılığıyla paylaşabilirsiniz.

II. Roller

Veri Katkısında Bulunan/Katkı Sağlayıcı (Contributor - Sendika/STK):

Katkı sağlayıcılar, OS Hub'a sundukları verilerin birincil kaynağıdır. Gönderilen bilgilerin doğru, paylaşımı güvenli ve gerekli kurumsal rıza alınarak sunulduğundan emin olmaktan sorumludurlar. Veri katkısında bulunma konusundaki nihai karar tamamen katkı sağlayıcıya aittir.

Open Supply Hub (OS Hub)

OS Hub süreci şu yollarla kolaylaştırır:

- Personeli ve danışma komitesi aracılığıyla olası güvenlik, hukuki ve itibara ilişkin riskler konusunda rehberlik sağlar;
- Yayın öncesinde, olası zararları tespit etmek ve azaltmak amacıyla Güvenlik İnceleme Aşamasını uygular (aşağıya bakınız);
- Riskleri en aza indirmek ve veri kalitesini artırmak için katkı sağlayıcılara geri bildirim, anonimleştirme seçenekleri ve pratik destek sunar.

Veri Kullanıcıları

Veri kullanıcıları, yayımlanan verilere OS Hub'ın [Hizmet Şartlarına](#) uygun olarak erişebilir ve bu verileri kullanabilir.

Sahiplik ve Lisans

OS Hub üzerinde yayımlanan tüm veriler [Creative Commons Atıf 4.0 Uluslararası \(CC BY 4.0\) lisansı](#) kapsamında paylaşılır. Bu, katkı sağlayıcıların verilerinin kaynağı olarak tanınmaya devam ettiği, OS Hub'ın ise bu verileri söz konusu lisansa uygun biçimde barındırdığı, düzenlediği ve açık kullanıma sunduğu anlamına gelir.

III. Veri Türleri & Rıza

Güvenliği sağlamak amacıyla OS Hub verileri iki ana kategoriye ayırır: kurumsal veriler ve kişisel/hassas veriler.

Kurumsal Veriler

Bireylere değil; kurumlara, işyerlerine veya kolektif yapılara ilişkin bilgileri ifade eder.

Örnekler (tam liste değildir):

- Bölgeye göre fabrika veya tedarikçi listeleri
- Toplu iş sözleşmelerinin (TİS) veya şikayet mekanizmalarının varlığı
- Bir araştırma çalışması kapsamında yer alan fabrikalar veya işyerleri
- Sendika veya STK öncülüğündeki girişimler, kampanyalar ya da izleme faaliyetleri

Kişisel veya Hassas Veriler

Bir kişiyi tanımlayabilecek, ifşa edebilecek veya tehlikeye atabilecek bilgileri ifade eder.

Örnekler (tam liste değildir):

- İşçilerin, emek örgütleyicilerinin veya ihbarcılarının isimleri, iletişim bilgileri ya da fotoğrafları
- Kimliği belirlenebilir ayrıntılar içeren bireysel vaka anlatımları veya tanıklıklar
- Konum, görev unvanı veya olay açıklaması üzerinden bir kişiye kadar izlenebilecek her türlü veri

Protokol: Bu tür bilgiler kamuya açık hale geldiğinde güvenliği garanti edilemeyeceği için OS Hub kişisel veya hassas verilerin yüklenmesini kabul etmez.

Geri Çekme Hakkı

Katkı sağlayıcılar, istedikleri zaman verilerinin kaldırılmasını talep edebilir. Acil talepler (örneğin güvenlik veya hukuki tehditlerle ilgili olanlar) mümkün olduğunda iki iş günü içinde işleme alınır.

Atıf

Güvenli olduğu durumlarda OS Hub, katkı sağlayan kuruluşun adını açıkça belirtir.

Katkı sağlayıcılar isimlerinin görünmesini istemezse, kayıt şu şekilde gösterilir: “Bir Sivil Toplum Kuruluşu veya Bir Sendika tarafından katkı sağlanmıştır.”

IV. Güvenlik İnceleme Aşaması

Sendika veya STK tarafından yapılan hiçbir veri katkısı, OS Hub’da yayımlanmadan önce Güvenlik İnceleme Aşamasından geçmeden yayınlanmaz. Bu süreç, veriler kamuya açık hale gelmeden önce katkı sağlayıcılar, işçiler ve topluluklar açısından doğabilecek riskleri belirlemeye ve azaltmaya yardımcı olur. Her gönderim, yayımlanmadan önce hem OS Hub ekibi hem de “Sendika ve STK Katılımı Danışma Komitesi”nden en az bir üye tarafından incelenir.

İncelemeyi Kim Yürütür

Danışma Komitesi, sendikalar ve sivil toplum kuruluşlarıyla çalışan veya bu kurumlarla yakın çalışmış; farklı bölgelerde karşılaşılan siyasi ve sivil riskleri anlayan kişilerden oluşur.

Danışma Komitesi üyelerinin tümü, gönderimleri sıkı gizlilik ve özenle ele almakla yükümlüdür. Bilgileri yalnızca olası güvenlik, hukuki veya gizlilik risklerini değerlendirmek amacıyla incelerler ve inceleme süreci dışında verileri paylaşmaları veya tartışmaları yasaktır.

Danışma Komitesi, belirli bir gönderim için gerekli sektörel veya bölgesel uzmanlığa sahip olmadığına karar verirse, OS Hub komite ve gönderimi yapan kuruluşla istişare ederek incelemeyi desteklemek üzere güvenilir bir dış uzman davet edebilir. Sürece dahil edilen her dış uzman da aynı gizlilik yükümlülüklerine ve sınırlı kullanım amacına uymak zorundadır.

Şeffaflığı sağlamak amacıyla katkı sağlayıcılar, gönderimlerini inceleyen Danışma Komitesi üyesinin adını ve bilgilerini talep edebilir. Katkı sağlayıcılar ayrıca, nihai karar verilmeden önce bağlamı açıklamak veya olası risk azaltma seçeneklerini görüşmek için ilgili üye ile kısa bir açıklama görüşmesi talep edebilir.

İncelemenin Odak Alanları

Şu anda OS Hub'ın Güvenlik İnceleme Aşaması üç risk kategorisine odaklanmaktadır.

Bu kategoriler, yeni bağlamları ve edinilen deneyimleri yansıtacak şekilde zaman içinde güncellenebilir.

a. Örgütlenme Özgürlüğü ve Sivil Alan Riskleri

Temel sorular şunları içerir:

- Yayınlama, işçileri, örgütleyicileri veya sendikaları misilleme ya da taciz riskine maruz bırakabilir mi?
- Veri, sendika veya STK faaliyetlerinin suç sayıldığı ya da ciddi biçimde kısıtlandığı bir bağlamla mı ilgilidir?

OS Hub şu anda bir sendika veya kuruluşun “meşru” ya da “sarı sendika” olup olmadığını değerlendirmez. Bu tür yargılar mevcut yetki alanımızın dışındadır. Gelecekte OS Hub, kullanıcıların farklı türde sendika ve STK’ları ayırt edebilmesine yardımcı olmak amacıyla (örneğin platform üzerinde simgeler veya işaretler aracılığıyla) farklı kategoriler veya tanımlayıcılar geliştirebilir.

b. Hukuki ve Uyumluluk Riskleri

Temel sorular şunları içerir:

- Gönderim, karalayıcı, yanıltıcı veya hatalı olduğu iddiasıyla itiraza konu olabilir mi?

- OS Hub'a veya katkı sağlayıcılara karşı dava, sorumluluk veya başka hukuki işlem riskleri öngörülebilir mi?
- Yayınlama, ulusal mevzuatın veya mevcut veri paylaşım anlaşmalarının ihlal edilmesi riskini taşıyor mu?

c. Veri Hassasiyeti ve Gizlilik Riskleri

Temel sorular şunları içerir:

- Gönderim, isimler çıkarılmış olsa bile kişisel veya kimliği belirlenebilir bilgiler içeriyor mu?
- Kişiler, görev unvanları, olaylar veya coğrafi ayrıntılar üzerinden yeniden tanımlanabilir mi?
- Veri; gözetleme, kimlik ifşası (doxxing) veya yıldırma amacıyla kötüye kullanılabilir mi?
- Veri, kamuya açık hale gelmesi durumunda mağdurları yeniden travmatize edebilecek şiddet veya taciz anlatımları içeriyor mu?

Zaman Çizelgesi

Normal koşullar altında OS Hub, eksiksiz bir gönderim alındıktan sonra Güvenlik İnceleme Aşamasını 10 iş günü içinde tamamlamayı hedefler.

Acil gönderimlerde – örneğin yayın zaman açısından kritikse veya aktif bir kampanyayla bağlantılıysa – inceleme ve yayın sürecinin, inceleyicilerin müsaitliği ve risk koşullarına bağlı olarak, 5 iş günü içinde tamamlanması için azami çaba gösterilir.

Sınırlamalar

Yukarıdaki kategoriler ve zaman çizelgeleri her olası durumu kapsamaz. OS Hub bunları, çok ülkeli ekibinin, Danışma Komitesinin ve uzmanlarının mevcut en iyi değerlendirmesine dayanarak uygular. Ancak tam koruma garanti edilemez; bu nedenle katkı sağlayıcıların, veri göndermeden önce olası riskleri dikkatle değerlendirmeleri teşvik edilir.

Güvenlik İnceleme Aşamasının Olası Sonuçları

Sonuç	Açıklama
Yayınlama	Veri OS Hub'a dahil edilmek üzere onaylanır. Anonimleştirme veya sınırlı atıf gibi koruyucu önlemler uygulanabilir.
Erteleme	Katkı sağlayıcıdan ek açıklama beklenirken veya ek güvenlik önlemleri alınırken yayın geçici olarak ertelenir.
Karantina / Red	Gönderimi yapan kuruluşla istişare edilerek, güvenli biçimde yayımlanamayacak kadar riskli olduğu değerlendirilirse veri yayınlanmaz. OS Hub, katkı sağlayıcıyla birlikte sansürleme, anonimleştirme veya gecikmeli yayın gibi seçenekleri değerlendirir; veri güvenli biçimde saklanır ve koşullar iyileştiğinde yeniden gözden geçirilir.

Karar Yetkisi & Şeffaflık

Sendika/STK Danışma Komitesi, bir veri setine ilişkin güvenlikle ilgili tüm kararlarda nihai yetkiye sahiptir. Komitenin görevi, katkı sağlayıcıları ve hak sahiplerini korumak; bireyleri veya grupları makul biçimde zarar, misilleme ya da hukuki riskle karşı karşıya bırakabilecek hiçbir verinin yayımlanmamasını sağlamaktır.

Güvenlikle ilgili kararlar, kontrol listesine dayalı veya otomatik eşiklere göre değil, bağlamsal bir değerlendirme yoluyla alınır. Risk sorularından birine ya da birkaçına “evet” yanıtı verilmesi tek başına bir gönderimin reddedilmesi anlamına gelmez. Bunun yerine komite, tespit edilen risklerin anonimleştirme, sansürleme, gecikmeli yayın, sınırlı atıf veya ek koruyucu önlemler gibi yöntemlerle makul biçimde azaltılıp azaltılamayacağını değerlendirir.

Komite, bir veri setinin tamamının veya bir bölümünün yönetilemez bir risk oluşturduğuna karar verirse, risk azaltılana kadar veri yayımlanmaz. Bu yaklaşım, “zarar vermeme” ilkesine bağlılığı ve görünürlükten önce güvenliği önceliklendirme taahhüdünü yansıtır.

Bir gönderim güvenlik gerekçesiyle ertelendiğinde, değiştirildiğinde veya reddedildiğinde, Danışma Komitesi üyeleri katkı sağlayan kuruluşla doğrudan görüşerek endişeleri açıklamaya, kararın gerekçesini paylaşmaya ve veriyi desteklemenin veya temsil etmenin daha güvenli alternatif yollarını birlikte değerlendirmeye hazırdır.

Zaman içinde tutarlılığı, hesap verebilirliği ve kurumsal öğrenmeyi desteklemek amacıyla Open Supply Hub, Güvenlik İnceleme Aşamasına ilişkin kararların ve gerekçelerinin dahili bir kaydı tutar. Bu kayıt yönetim ve referans amaçlı kullanılır; Danışma Komitesi üyeliği değişse bile süreklilik sağlar ve kamuya açık değildir.

V. Düzeltme, Revizyon ve Yayından Kaldırma

OS Hub, veriler platformda yayımlandıktan sonra koşulların, risklerin veya olguların değişebileceğini kabul eder. “Zarar vermeme” ilkesini korumak amacıyla katkı sağlayıcılar ve etkilenen taraflar, gerektiğinde düzeltme, kaldırma veya başka telafi yolları talep edebilir.

Talep Nasıl Yapılır

Talepler şu kişiler tarafından gönderilebilir:

- Veriyi sağlayan sendika veya sivil toplum kuruluşu; veya
- Katkı sağlayıcı tarafından yetkilendirilmiş bir irtibat kişisi.
Yetkili temsilcinin adı ve iletişim bilgileri, veri gönderimi sırasında OS Hub’ın resmi sendika/STK veri gönderim formunda ([Türkçe](#) & [İngilizce](#)) ya da gönderim sürecinde kararlaştırılan alternatif yollarla belirtilmelidir.

Talepler **support@opensupplyhub.org** adresine gönderilmeli ve herhangi bir dilde yazılabilir.

Yerel veya bölgesel dillerde yapılan başvurular, zamanında ve doğru takip sağlamak amacıyla gerektiğinde kurum içinde çevrilecektir.

Uygun Talepler

OS Hub, aşağıdaki nedenlerle yapılan düzeltme, revizyon veya yayından kaldırma taleplerini kabul eder (örnekler sınırlı değildir):

- Güvenlik tehditleri: Yayın, zarar, misilleme veya hukuki risk ihtimali yaratıyor ya da artırıyorsa
- Yanlışlıklar veya hatalı atıflar: Maddi hatalar, yanlış tesis bilgileri veya yanlış kaynak gösterimi

- Rızanın geri çekilmesi: Katkı sağlayıcı veya yetkili temsilci yayın iznini geri çekmek isterse
- Yasal emirler veya kısıtlamalar: Mahkeme kararları, resmi makam talimatları veya bağlayıcı yükümlülükler.
- Diğer meşru endişeler: Yeni ortaya çıkan bağlamsal riskler, gizlilik sorunları veya topluluk düzeyinde itirazlar gibi durumlar.

Mevcut Eylemler

Talebin niteliğine ve risk düzeyine bağlı olarak OS Hub:

- İnceleme süresince kaydı geçici olarak gizleyebilir;
- Belirli alanları veya metinleri düzeltebilir ya da sansürleyebilir;
- Kaydı tamamen kamu görünümünden kaldırabilir; veya
- Doğrulanmış güncellemeler ya da bağlamsal açıklamalar ekleyebilir.

Hesap verebilirlik ve tutarlılığı sağlamak amacıyla alınan tüm kararlar OS Hub'ın dahili karar kayıt sistemine işlenir.

Zaman Çizelgesi

- Acil durumlar (örneğin güvenlik veya hukuki tehditler) mümkün olduğunda iki iş günü içinde değerlendirilir ve işleme alınır.
- Acil olmayan durumlar beş iş günü içinde incelenir. Bir talep hafta sonu veya resmi tatil gününde gelirse, işlem bir sonraki iş gününde başlatılır.

İletişim ve Takip

Katkı sağlayıcılar, talepleri işleme alındıktan sonra bilgilendirilir.

Ek açıklama gerektiğinde, OS Hub personeli veya Danışma Komitesi üyeleri, nihai karar verilmeden önce mevcut seçenekleri görüşmek üzere iletişime geçebilir.

Bir talep daha geniş veya tekrarlayan bir risk örüntüsünü ortaya koyuyorsa – örneğin yinelenen tehditler veya bölgeye özgü kısıtlamalar – OS Hub, benzer vakalarda tutarlı uygulama ve kurumsal öğrenmeyi sağlamak amacıyla Danışma Komitesine danışabilir.

VI. Katkı Sağlayıcıların Sorumlulukları

OS Hub'a veri katkısında bulunan sendikalar ve sivil toplum kuruluşları (STK), paylaşılan bilgilerin güvenilir, güvenli ve haklara saygılı kalmasında önemli bir rol oynar.

Katkı sağlayıcılar, veri göndererek aşağıdaki ilkelere uymayı kabul eder.

a. Zarar Vermeme

Katkı sağlayıcılar, verinin yayımlanmasının işçileri, örgütleyicileri veya toplulukları tehlikeye atmaması için makul tüm çabayı göstermelidir. Buna, gönderim öncesinde temel bir risk değerlendirmesi yapmak ve gerekirse hukuki, dijital güvenlik veya kurumsal uzmanlara danışmak da dahildir.

b. Güvenli Kanallar Kullanma

Veriler yalnızca güvenli ve güvenilir kanallar üzerinden aktarılmalıdır. OS Hub, sendika/STK veri gönderimleri için resmi veri gönderim formu ([Türkçe](#) & [İngilizce](#)) üzerinden veri kabul eder. Bu form, Google politikalarına uygun olarak dosyaların güvenli biçimde iletilmesini sağlayan bir Google oturumu gerektirir.

Herhangi bir nedenle bu yöntem uygun veya rahat değilse, OS Hub katkı sağlayıcılarla birlikte, bağlamlarına ve risk düzeylerine uygun alternatif aktarım yöntemleri belirleyebilir (örneğin şifreli e-posta veya karşılıklı mutabık kalınan başka bir güvenli kanal).

c. Doğru ve Adil Olma

Gönderim sırasında mevcut olan en iyi ve doğrulanabilir bilgileri sağlayın.

Bilgi eksikse, ihtilaflysa veya doğrulanmayı bekliyorsa, bunu “iddia”, “doğrulama bekleniyor” veya “yaklaşık” gibi ifadelerle açıkça belirtin.

d. Rızaya Saygı Gösterme

Gönderimden önce, ilgili tüm kuruluşların veya ağların kendileriyle ilgili verilerin dahil edilmesine onay verdiğinden emin olun. Kişisel veya kimliği belirlenebilir veriler asla dahil edilmemelidir.

e. Takip Sürecine Katılım

Katkı sağlayıcılar, mümkün olduğu ölçüde:

- OS Hub veya Danışma Komitesinin açıklama taleplerine yanıt vermeli;
- Yayın sonrası ortaya çıkabilecek güvenlik veya doğruluk sorunlarının belirlenmesine ve çözülmesine destek olmalıdır.

f. Gerektiğinde Güncelleme veya Geri Çekme

Gönderilen herhangi bir bilginin zamanla güncelliğini yitirmesi, hatalı hale gelmesi veya çevrimiçi kalmasının risk oluşturması durumunda, katkı sağlayıcıların düzeltme süreci aracılığıyla OS Hub’ı derhal bilgilendirmesi teşvik edilir (aşağıya bakınız). Bu, doğruluğun korunmasına ve sürece dahil olan herkesin güvenliğinin sağlanmasına yardımcı olur.

VII. Protokolün Gözden Geçirilmesi

Bu politika en az yılda bir kez gözden geçirilir ve sendikaları, sivil toplum kuruluşlarını, veri katkı sağlayıcılarını veya Open Supply Hub'ın kendisini etkileyen hukuki, operasyonel ya da bağlamsal değişiklikleri yansıtacak şekilde gerektiğinde güncellenir.

Yapılan her revizyon sürümlendirilir ve tek, yetkili referans noktası sağlamak amacıyla Open Supply Hub'ın [Yönetişim ve Politikalar](#) sayfasında yayımlanır.

Ek A: Veri Gönderim Formu

Katkı sağlayıcılar, kurumsal verileri OS Hub ile aşağıdaki form aracılığıyla paylaşabilir:

OS Hub Sendika/STK veri gönderim formu ([Türkçe](#) & [İngilizce](#)): Bu form üzerinden veri paylaşabilmek için bir Google hesabıyla giriş yapılması gerekmektedir. Google hesabınız yoksa veya alternatif bir yöntem kullanmanız gerekiyorsa, lütfen **support@opensupplyhub.org** adresine e-posta gönderin.

Veri gönderirken, her üretim tesisi veya işyeri için aşağıdaki temel tanımlayıcı bilgileri eklemeniz rica olunur:

- Tesis / İş Yeri Adı
- Adres (aşağıdaki rehbera bakınız)
- Sektör / Endüstri
- Ülke

Veriler herhangi bir formatta gönderilebilir (örneğin: excel dosyaları, PDF'ler, kısa raporlar veya metin dosyaları).

Gönderim Formunu kullanırken bağlantı sorunları, dil engelleri veya dijital güvenlik endişeleri gibi zorluklarla karşılaşırsanız, OS Hub Signal veya şifreli e-posta dahil olmak üzere alternatif güvenli gönderim yöntemleri önerebilir.

Adreslere İlişkin Rehber

Azami doğruluk ve kullanılabilirliği sağlamak için, mümkün olduğu ölçüde adreslerin aşağıdaki rehbera uygun olması önerilir:

Adresler mümkün olduğunca eksiksiz olmalı ve şunları içermelidir:

- Sokak numarası
- Sokak adı
- Şehir / ilçe
- İl / eyalet
- Posta kodu

Sokak adı ve/veya numarası mevcut değilse veya kullanılmıyorsa, lütfen aşağıdakilerden uygun olanları kullanın:

- Mahalle adı; ve/veya
- Köy adı; ve/veya
- Sanayi bölgesinin adı ve parsel numarası(ları); ve/veya
- Yerel olarak tanınan başka bir coğrafi tanımlayıcı.

Ek rehber:

- Latin alfabesi dışındaki karakterleri mümkün olduğunca Latin / İngilizce karşılıklarına çevirin.

- Posta Kutusu veya benzeri ifadeleri (örneğin: P.K., P.O. Box, Caixa Postal, Apartado Postal) kaldırın; bunlar coğrafi konumlandırmayı ve adres doğruluğunu olumsuz etkileyebilir.

Adresin tam ayrıntılarını paylaşmak zor veya riskliyse, katkı sağlayıcıların bunu gönderim sırasında belirtmesi teşvik edilir; böylece Open Supply Hub, Güvenlik İnceleme Aşamasında uygun koruyucu önlemleri değerlendirebilir.

Ek B – Yayından Kaldırma / Düzeltme Talep Şablonu

Bir düzeltme, sansürleme veya kaldırma talebinde bulunmak için lütfen aşağıdaki bilgileri sağlayın.

Bu formatı bir e-postaya kopyalayarak **support@opensupplyhub.org** adresine herhangi bir dilde gönderebilirsiniz.

Konu satırı: Yayından Kaldırma / Düzeltme Talebi

Talep eden kişinin adı ve rolü:

Kayıt / URL / Tesis tanımlayıcısı:

.Lütfen söz konusu veri kaydını veya veri setini açıkça belirtin.

Sorun türü:

Lütfen aşağıdakilerden hangisinin geçerli olduğunu belirtin (örnekler):

- Güvenlik riski
- Yanlışlık / hatalı bilgi
- Rızanın geri çekilmesi
- Yasal emir (varsa ekleyin)
- Diğer (lütfen açıklayın)

Talep edilen işlem:

Lütfen OS Hub'dan ne yapmasını istediğinizi belirtin (örnekler):

- Belirli ayrıntıları sansürleme
- Geçici olarak gizleme
- Tamamen kaldırma
- Diğer (lütfen açıklayın)

Gerekçe ve kanıt:

En fazla 500 kelime ile açıklayın. Varsa destekleyici belgeleri ekleyin.

Tercih edilen iletişim yöntemi:

(örneğin: Signal, WhatsApp, e-posta veya başka güvenli bir kanal)