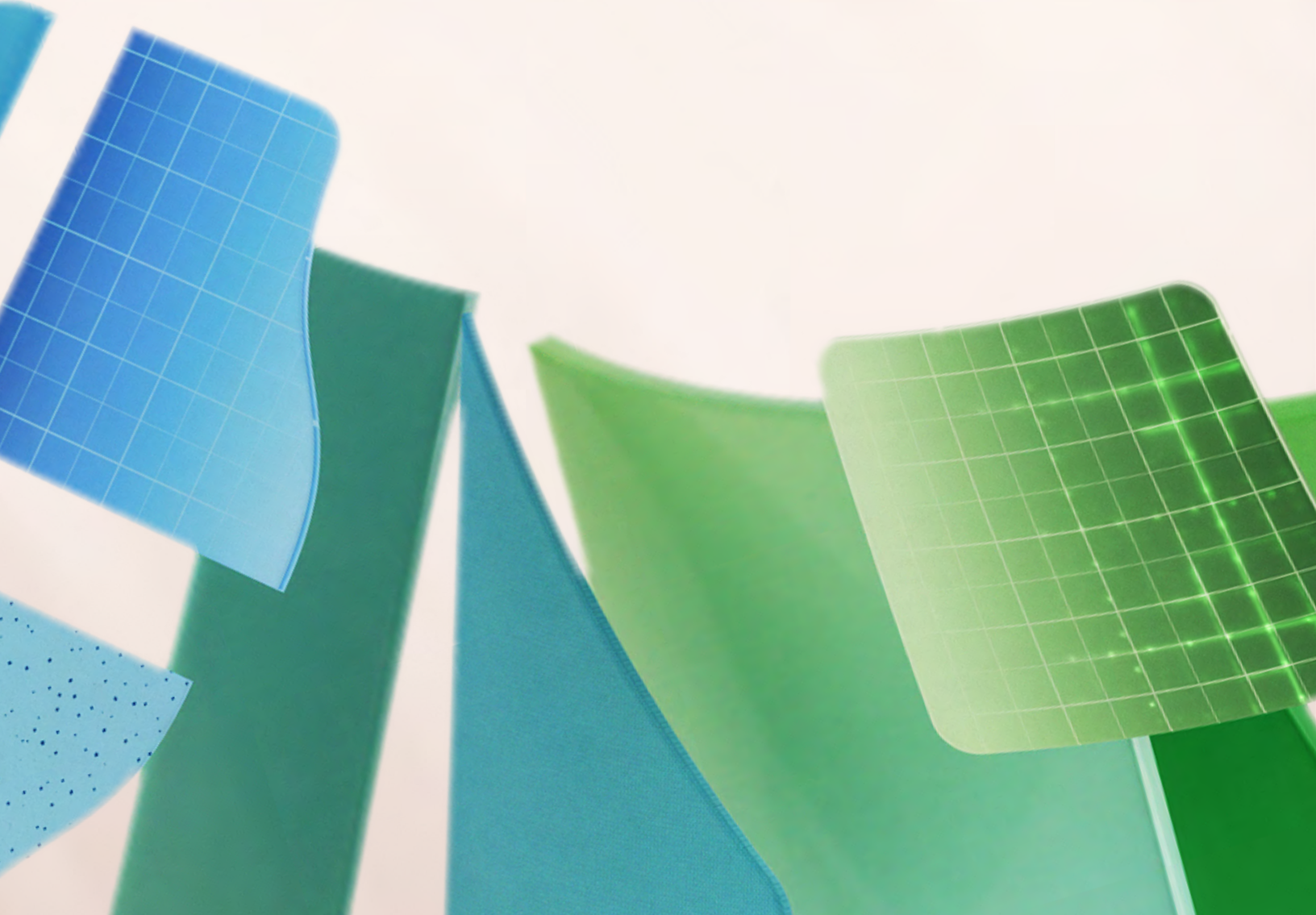


Veriler Kontrol Altında

Yapay zeka başarısı için veri yönetiminde uzmanlaşma



İçindekiler

Giriş

Veri yönetimi, güvenli yapay zekayı benimsemenin bel kemiğini oluşturur

Üretken yapay zeka, kurum dönüşümü vaatlerini yerine getirir. Ancak potansiyelin gerçekleşmesi, kurum verilerinizin kalitesine ve erişilebilirliğine bağlıdır.

Güçlü veri yönetimine öncelik veren kurumlar, yapay zeka ile rekabet avantajı elde etmeye hazırlanıyor. Veri yönetimi, yapay zeka tarafından sorgulanan ve oluşturulan verilerin doğru, güvenli, kontrollü ve uyumlu olmasını sağlamaya yardımcı olur.

Veri kalitesi ve erişilebilirliği:

Yapay zeka sistemleri, kurumunuzun benzersiz iş akışlarından uygun bağlamla mümkün olan en iyi yanıtı sağlamak amacıyla büyük, yüksek kaliteli veri kümelerini kullanır. Daha iyi veri kalitesi, daha etkili yapay zeka görüşleri ve tahminleri sağlar.

Uyumluluk: Güçlü veri yönetimi, yasal gereklilikler ve para cezaları riskini azaltarak düzenleyici gerekliliklere uyulmasını sağlar.

Güvenlik: Uygun veri etiketleme ve yönetimi, hassas bilgileri yetkisiz erişim, uygun olmayan paylaşım ve ihlallerden korur.

Güven: Güvenilir veri yönetimi, yapay zeka çıktılarında paydaş güvenini artırır ve yapay zeka girişimlerine daha fazla benimseme ve destek sağlar.

Bu e-kitapta, yapay zekaya hazır bir kurum oluşturan kritik veri yönetimi uygulamaları tanıtılmıştır. Sıkı veri kalitesi standartlarının nasıl oluşturulacağına, düzenleyici gerekliliklere uyumun nasıl sağlanacağına, veri koruma ve güvenlik önlemlerinin nasıl uygulanacağına yer verilmiştir. Hassas toplantı içeriğinin harici olarak paylaşılmasını engelleyen veya veri ihlallerine karşı korunmasını sağlayan yapay zeka sistemlerine güven oluşturmaya ve verileri eyleme geçirilebilir görüşler sağlamak için kolayca kullanılabilir hale getirmeye yönelik stratejileri öğreneceksiniz. Kurumunuz, bu uygulamaları benimseyerek sürekli yenilik ve rekabet avantajı için yapay zekanın tüm potansiyelini uygulayabilir.

Üretken yapay zeka kullanım örnekleri

İletişimi hızlandırın: Kişiselleştirilmiş içerikleri daha hızlı taslak haline getirerek ilişkiler kurmaya ve işbirliği yapmaya zaman kazanın.

Verimliliği geliştirin: Rutin görevlere harcanan zamanı azaltın, üretkenliği artırın ve maliyetleri azaltın.

Yeniliğe olanak tanıyın: Yeni ürün ve hizmetler için fikir ve tekliflerin oluşturulmasına yardımcı olun.

Müşteri deneyimini kişiselleştirin: Bağlılığı ve etkileşimi artırmak için içeriği ve önerileri özelleştirin.

Yapay zeka dönüşümü için veri yönetiminin güçlendirilmesi

Her kurumun veri kullanımını yöneten kuralları ve süreçleri vardır. Veri yönetimi çerçeveleri olgunluk ve kapsamlılık açısından farklılık gösterir ancak çok azı yapay zeka için tamamen optimize edilmiştir. Veri doğruluğunu ve tutarlılığı sağlamak gibi birçok veri yönetimi en iyi uygulaması aynı kalırken, diğer unsurların yapay zeka yatırımlarını en üst düzeye çıkarmak için güncelleştirmelere ihtiyacı vardır. Şimdi birkaç önemli alana göz atalım.

Veri görünürlüğü

Yapay zeka sistemleri içindeki ayrıntılı veri akışı bilgisi, yetkisiz veya uygun olmayan kullanımları bulmayı ve azaltmayı mümkün kılar. Bu görünürlük, yapay zeka değerini en üst düzeye çıkarmak için hassas verileri koruyarak güvenliği ve uyumluluğu desteklemeye yardımcı olur.

Geleneksel veri yönetimi, verilerin nerede olduğunu bilmeye ve erişimi denetlemeye odaklıdır. Ancak yapay zeka iş operasyonlarıyla daha tümleşik hale geldikçe, veri yönetiminin değişen güvenlik ihtiyaçlarına ayak uydurması gerekir.

Örneğin yönetimin, son derece hassas bir ürün tanıtımı ile yapay zeka tarafından oluşturulan içeriğin yönetilmesine kadar uzanması ve yapay zeka tarafından üretilen proje ile ilgili belgelerin, iletişimlerin ve görüşlerin güvenli olmasını sağlaması gerekir. Bu, yalnızca yetkili ekip üyelerinin proje bilgilerini analiz etmek veya özetlemek için yapay zekaya erişebilmesi ve kullanabilmesi için korumalar uygulamak anlamına gelir.

Ayrıca, kurumlar veri işleme ve depolama birimlerini yöneterek yapay zeka ile ilişkili operasyonel maliyetleri daha iyi kontrol edebilir.

Veri kalitesi

Kötü veri kalitesi yapay zeka sonuçlarını doğrudan etkilediğinden yapay zeka, yüksek kaliteli verilerin önemini artırır. Kurum verilerinizi sorgulamak için yapay zeka araçlarını uygularken, verilerin güncel ve güvenilir olduğundan emin olmak istersiniz. Aynı derecede önemli bir nokta da, ekiplerinizin kendi yapay zeka modellerini ve uygulamalarını oluşturmak için kullandığı verilerin kaynağını ve kalitesini anlamaktır. Düzenli veri denetimleri, sıkı doğrulama süreçleri ve proaktif yönetim, veri bütünlüğünü sağlamaya yardımcı olur. Kurumlar, bu alanlara odaklanarak daha iyi karar alma ve yenilik sağlayan güvenilir yapay zeka sonuçları elde edebilir.

Kullanıcı yönetimi

Kullanıcılar, yapay zeka ile verilerle karmaşık şekillerde etkileşime girer. Microsoft 365 Copilot gibi yapay zeka sistemleriyle doğal dil istemleri aracılığıyla iletişim kurarlar. İzin ve korumalar uygulandığında yapay zeka, bir yanıt oluşturmak üzere dosyalar, sohbetler ve e-postalar gibi verilerden gelen ilgili bağlama eklentiler aracılığıyla ek kaynaklarla erişebilir.

Yapay zekanın doğru ve temeli sağlam yanıtlar sunduğundan emin olmak için bu süreçlerde kullanılan verilerin izlenmesi oldukça önemlidir. Dipnotlar veya orijinal kaynaklara bağlantılar aracılığıyla şeffaflık sağlamak, kullanıcıların bilgileri doğrulamasına yardımcı olur, verilerin yanlış kullanımı riskini azaltır ve yönetmeliklere uyumu sağlar.

Uyumluluk ve eKeşif

Yapay zekanın yükselişi uyumluluk ve eKeşif'te (yasal durumlar için verilerin işlenmesi), özellikle yapay zeka tarafından oluşturulan verilerin yönetilmesinde ve değişen yasal gerekliliklere uyum sağlamada ortaya yeni zorluklar çıkarıyor. Veri yönetimi çerçevelerini bu zorlukları aşmak için güncellemeye, yapay zeka tarafından üretilen belgelerin veya iletişimlerin güvenli bir şekilde izlenmesini, kategorilere ayrılmasını ve depolanmasını sağlamak gibi yapay zeka tarafından oluşturulan içeriği kapsayan kurallar geliştirmek dahildir. Örneğin, yapay zeka tarafından oluşturulan e-postaların veya raporların gelecekte alınmak üzere düzgün bir şekilde etiketlendiğinden ve arşivlendiğinden emin olmak için kuralların güncellenmesi gerekebilir.

eKeşif özelliklerinin iyileştirilmesi, çeşitli platformlarda yapay zeka tarafından oluşturulan içeriği arayabilen ve tanımlayabilen yapay zeka araçlarını tümleştirmeyi içerir. Örneğin, yasal bir soruşturma sırasında eKeşif araçlarının yapay zeka tarafından oluşturulan belirli belgeleri bulup alabilmesi, ilgili iletişimleri özetleyebilmesi ve uyumluluğu kanıtlamak için açık denetim yolları sağlayabilmesi gerekir. Kurumlar bu özellikleri güncelleyerek yasal denetimler veya soruşturmalar sırasında verileri daha iyi yönetebilir ve yapay zeka tarafından oluşturulan tüm bilgilerin mahkemede erişilebilir ve savunulabilir olmasını sağlayabilir.

Veri güvenliği

Yapay zeka odaklı işlemlerin güvenliğini sağlamak için kimlik düzeyinde Sıfır Güven ilkelerini eklemek gerekir ve bu da yetkisiz erişim riskini en aza indirir. Cihazlar ve uygulamalar da dahil olmak üzere uç noktalarda yapılan düzenli güncellemeler, kötüye kullanılabilecek güvenlik açıklarını azaltır. Kurum içinde kullanımda olan üretken yapay zeka araçlarının farkında olunması, onaylanmamış veya güvenli olmayan uygulamaların engellenmesini sağlar ve bu da olası güvenlik ihlallerini önler. Kurumlar, yapay zeka araçlarına ve verilerine erişimi yalnızca güvenilir personel ile sınırlandırarak daha büyük veri bütünlüğü elde edebilir ve yapay zeka işlemlerini potansiyel tehditlere karşı koruyabilir.

Sıfır Güven nedir?

Sıfır Güven, her talebi güvenilir olmayan bir ağdan geliyormuş gibi doğrulamaya odaklanan bir güvenlik modelidir. Bu yaklaşım, kurumsal güvenlik duvarı içindeki her şeyin güvenli olduğunu varsaymak yerine "asla güvenme, her zaman doğrula" ilkesini benimser.

Sıfır Güven ilkeleri

Açıkça doğrulayın: Daima mevcut tüm veri noktalarına göre kimlik doğrulaması yapın ve yetkilendirin.

En az ayrıcalıklı erişimi kullanın: Kullanıcı erişimini Tam Zamanında ve Yalnızca Yeterli Erişim (JIT/JEA), risk tabanlı uyarlanabilir kuralları ve veri korumasıyla sınırlayın.

İhlal olduğunu varsayın: Tehditleri tespit etmek ve savunmaları güçlendirmek için hasarı sınırlayın, erişimi kontrol edin, şifreleme sağlayın ve verileri kullanın.

Yapay zeka dönüşümünde veri yönetiminin rolü: Köken, kalite ve güvenilirlik

Kurumlar, kurumsal kararlara yardımcı olması için yapay zekayı benimsediğinden, bu sistemlerin doğru ve güvenilir sonuçlar sunabilmesinin sağlanması gerekir. Veriyi temel alan yapay zeka yanıtlarının erişilebilir, tutarlı ve iyi belgelenmiş olması gerekir.

Veri yönetimi, verilerin nereden geldiğini takip eden, kalitesini kontrol eden ve güvenilirliği ile doğruluğunu garanti eden yönetim kuralları uygulayarak güvenilir yapay zekayı destekler. Bu uygulamalar, güvenilir görüşler sunan, bilinçli ve kendinden emin bir şekilde karar almayı sağlayan yapay zeka sistemlerinin temelini oluşturur.

Veri kökeni: Kökenleri ve bilgi değişikliklerini anlama

Veri kökeni, bir kurumdaki verilerin yolculuğunu izler. Verilerin kökenlerini, dönüşümlerini ve hedeflerini belgeler. Yapay zeka destekli kurumlar için veri kökenini anlamak birkaç nedenden dolayı hayati öneme sahiptir:

- **Şeffaflık:** Verilerin nereden geldiğini ve nasıl değiştiğini bilmek, yapay zeka tarafından oluşturulan çıktıların doğruluğunu onaylamaya yardımcı olur ve verilerin geçmişini net bir şekilde anlayarak düzenleyici uyumluluk sağlar.
- **İzlenebilirlik:** Veri kökeni, kurumların hataların veya tutarsızlıkların kaynağına dönüp izlemesini sağlayarak sorun giderme ve veri düzeltmeyi basitleştirir.
- **Etki analizi:** Verilerin üretken yapay zeka araçları tarafından nasıl kullanıldığını anlamak, veri kaynaklarındaki veya işleme yöntemlerindeki değişikliklerin çıktı doğruluğu ve iş sonuçları üzerindeki potansiyel etkisinin değerlendirilmesine yardımcı olur.

Veri kalitesi:

Kalite, yapay zeka yanıtlarının değerini artırır

Veri kalitesi, yapay zeka çıktılarının güvenilirliğini doğrudan etkiler. Yüksek kaliteli veriler, yapay zeka modellerinin kullanıcı girdilerine doğru ve değerli yanıtlar sunması için bağlam sağlar. Veri kalitesinin temel yönleri şunlardır:

- **Doğruluk:** Verilerin, gerçek yaşamdaki koşulları doğru şekilde temsil etmesi gerekir.
- **Eksiksizlik:** Gerekli tüm verilerin mevcut olması ve hesaba katılması gerekir.
- **Tutarlılık:** Verilerin, farklı sistemlerde ve zaman içinde tutarlı olması gerekir.
- **Güncellik:** Verilerin güncel ve gerektiğinde erişilebilir olması gerekir.

Veri güvenilirliği:

Güvenilir veriler sağlama

Veri güvenilirliği, verilerin sürekli olarak kalite standartlarını karşıladığı ve gerektiğinde erişilebilir olduğu anlamına gelir. Yapay zeka destekli kurumlarda güvenilir veriler, yapay zeka araçlarına güvenin ve bilgilendirildikleri kararların teşvik edilmesi açısından oldukça önemlidir. Veri güvenilirliğini sağlamak için aşağıdakiler gerekir:

- **Veri yedekliliği:** Kaybı önleyen ve erişilebilirliği artıran yedekleme sistemleri uygulamak.
- **Düzenli yedeklemeler:** Veri bozulması veya kaybına karşı koruma için sık sık yedekleme yapmak.
- **İzleme ve uyarılar:** Veri sorunlarını gerçek zamanlı olarak saptamak ve paydaşlara uyarmak için izleme sistemleri kurmak.
- **Olağanüstü durum kurtarma planları:** Verileri kurtarmak ve kesintilerden hemen sonra işlemleri sürdürmek için planlar geliştirmek ve test etmek.

Yönetim, güvenlik ve sorumlu yapay zeka arasındaki ilişki

Veri yönetimi ve güvenlik, birlikte sorumlu yapay zeka kullanımının bel kemiğini oluşturur. Yüksek kaliteli, güvenli veriler yapay zekanın etik ve etkili bir şekilde çalışmasını sağlar. Değerlendirilecek önemli alanlar arasında veri sınıflandırması, erişim denetimleri, şifreleme, olay yanıtı ve yasal uyumluluk bulunur.

Verileri sınıflandırma

Verileri sınıflandırma, yapay zeka araçlarının hassas bilgileri nasıl işlediğini denetlemenin önemli bir parçasıdır. Genelde veriler ve toplantılar genel, gizli veya yüksek derecede gizli olarak sınıflandırılır. Uygun sınıflandırma, yapay zekanın yalnızca uygun bilgilere erişmesini sağlayarak hassas verileri yetkisiz kullanıcılara sunma riskini azaltır.

Diğer yandan yanlış sınıflandırma, yapay zekanın kısıtlanması gereken verileri işlemesine ve güvenlik ihlallerine veya uyumluluk sorunlarına yol açabilir. Etkili veri yönetimi, ister otomatik araçlar ister son kullanıcı kuralları aracılığıyla olsun, verilerin doğru şekilde sınıflandırılmasını sağlar, hassas bilgileri korur ve yapay zekanın güvenilir ve uyumlu çıktıları sunma özelliğini destekler.

Erişim kontrolleri

Bu denetimler, yapay zeka ile ilgili verilere kimlerin erişebileceğini ve hangi uygulamaların veya kimliklerin bu verilerle etkileşim kurma iznine sahip olduğunu düzenler. Zayıf erişim kontrolleri, hassas bilgilerin izinsiz olarak açığa çıkmasına neden olarak ihlal ve yanlış kullanım riskini artırır.

Veri yönetimi, yetkili personel ile belirli uygulamalara veri erişimini kısıtlayarak ve hassas verilerin uygun şekilde işlenmesini sağlayarak bu denetimlerin uygulanmasında önemli bir rol oynar. Bu yalnızca veri bütünlüğünü korumakla kalmaz, aynı zamanda yapay zeka sistemlerinin güvenli ve güvenilir veri kümelerinde çalışmasını sağlayarak güvenilirliklerini ve uyumluluklarını artırır.

Şifreleme

Verileri ele geçirme ve şifreleme kullanarak müdahale etmekten korumak, üretken yapay zeka araçlarının yanıtlarını veri sızıntısı riski olmadan doğru bağlamda (işle ilgili veriler, dosyalar, sohbetler ve e-postalar gibi) temellendirebilmesini sağlar.

Veri yönetimi kuralları, verileri tüm yaşam döngüsü boyunca koruyarak güçlü şifreleme uygulamalarını zorunlu kılabilir. Bu yaklaşım, yapay zeka araçlarının verilerinizi güvende tutarken ve güveninizi korurken güvenilir yanıtlar verebilmesini sağlar.

Olay yanıtı

Hassas kurumsal veriler, sistemlerin yanıt oluşturmak için kullandığı dosyalara, e-postalara veya diğer kurumsal verilere yetkisiz erişim sağlayan üretken yapay zeka araçlarını içeren olaylardan kaynaklanabilir.

Bu senaryolarda proaktif bir olay müdahale planına sahip olmak oldukça önemlidir. Kurum, böyle bir plan olmadan yalnızca hassas verileri sunma riskiyle karşılaşmaz, aynı zamanda yapay zekanın güvenliği ihlal edilen çıktılarına güvenir. Veri yönetimi sağlamak için ihlallere hızlı bir şekilde müdahale etmek, etkilerini en aza indirmek ve yapay zeka sistemlerinin güvenilirliğini korumak için ayrıntılı yanıt protokollerine sahip olmak gerekir.

Yasal düzenlemelere uyumluluk

Yapay zeka uygulamalarının, veri koruma ve gizliliğini yöneten GDPR veya CCPA gibi düzenlemelere uyması gerekir. Uyum sağlanmaması önemli cezalara yol açabilir ve güveni sarsabilir. Birçok ücretsiz araç veriyi küresel olarak veya kurumunuzun normal depolama konumlarının dışında ele alabileceğinden, yapay zeka araçlarının verileri nerede işlediğini anlamak da önemlidir. Veri yönetimi, yapay zeka uygulamalarının yalnızca yasal çerçeveler dahilinde çalışmasını sağlamakla kalmaz, aynı zamanda kurumunuzun uyumluluk standartlarına uyum sağlayarak verileri doğru hizmet sınırları içinde tutmanızı da sağlar. Bu yaklaşım, etik yapay zeka kullanımını destekler ve yapay zeka teknolojisine güven oluşturulmasına yardımcı olur.



4

Veri yönetimi çerçevenizi yapay zekanın benimsenmesini desteklemek üzere güncelleme

Gelişen yapay zeka ortamında, mevcut veri yönetimi çerçevenizde fazladan dikkat gerektirebilecek belirli alanların belirlenmesi önemlidir.

Tüm çerçeveyi elden geçirmek yerine, gelişmenizin en muhtemel olduğu alanlara odaklanarak verilerinizin korunmasını ve güvende kalmasını sağlarken çabanızı yapay zekanın değerini en çok artıracığı noktalara yönlendirebilirsiniz. İşte dikkate almanız gereken birkaç önemli bilgi:

Kuralların ve prosedürlerin benimsenmesi

Yapay zeka, yeni veri toplama, işleme ve kullanım türlerini içerir. Veri kurallarını güncelleştirmek, veri gizliliği, yönetmeliklere uyum ve etik kullanım ile ilgili ihtiyaçların karşılanmasına yardımcı olabilir. Örneğin belirli durumlarda veri anonimleştirmenin gerekmesi, kişisel bilgileri koruyarak yapay zeka yaşam döngüsü boyunca kullanımını daha güvenli hale getirebilir.

Roller ve sorumluluklar

Yapay zeka hazırlığının veri yönetimiyle ilgili rollere dahil edilmesi gerekir. Yapay zeka veri gereksinimlerini bilen çalışanlar, veri kalitesini ve uyumluluğu desteklemek üzere destek görevi görebilir. Hukuk, BT ve veri bilimi ekipleri arasındaki departmanlar arası işbirliği, yapay zekaya özgü zorlukların daha etkili bir şekilde çözülmesine yardımcı olabilir.

Veri standartlarını ve tanımlarını benimseme

Veri biçimlerinin, tanımların ve kalite ölçümlerinin standartlaştırılması, bir kurum içinde yapay zeka aracı kullanımını yöneten kuralların uygulanmasını basitleştirir. Net veri standartları, yapay zeka araçlarının hangi veri kümelerinin iş bağlamı sağlamak için akıl yürütebileceğine ve kullanıcıların analiz için hangi verileri yükleyebileceğine karar vermeyi kolaylaştırır. Bu, yapay zeka uygulamalarının en ilgili ve en güvenilir verileri kullanmasını sağlar ve kurumsal kurallara uyumluluğu desteklerken etkinliklerini artırır.

Sürekli iyileştirme

Veri yönetimi, özellikle yapay zeka ile devam eden bir süreçtir. Düzenli denetimler ve yönetim çerçevenizdeki güncellemeler, veri yönetiminin yeni yapay zeka gelişmelerinde ve düzenleyici değişikliklerde benimsenmesine yardımcı olabilir. Yapay zeka, yönetim uygulamalarını kontrol etmek ve geliştirmek, potansiyel olarak boşluklar bulmak ve iyileştirmeler önermek amacıyla kullanılabilir. Bu proaktif yaklaşım, yapay zeka teknolojileri geliştikçe uyumluluğu ve verimliliği artırır.

Etkili veri yönetimine yönelik araçlar ve teknikler

Kurumsal hedeflerle uyumlu hale getirin:

Veri yönetimi stratejinizin, karar verme sürecini ve verimliliği artırmak için kurumsal hedefleri desteklediğinden emin olun.

Rutin görevleri otomatikleştirin:

Manuel hataları azaltmak ve güvenliği iyileştirmek için veri sınıflandırması ve erişim yönetimi gibi tekrarlayan görevler için otomasyonu kullanın.

Yüksek doğruluk standartları sağlayın:

Zaman içinde veri bütünlüğünü desteklemek için doğrulama ve temizleme araçlarını kullanın.

Kullanıcılara eğitim verin:

Yanlış yönetimi önlemek ve kurallara uygunluğu sağlamak için veri yönetim araçları ve prosedürleri konusunda eğitim verin.

Düzenli denetimler yapın:

Düzenleyici ve kurumsal değişikliğe ayak uydurduğundan emin olmak için veri uygulamalarını düzenli olarak gözden geçirin.

Sonuç

Microsoft 365 ile yapay zeka olanakları sağlamak için etkili veri yönetimi

Yapay zekayı sorumlu bir şekilde kullanmak için sağlam veri yönetimi gerekir. Etkili veri yönetimi, veri erişilebilirliği, doğruluk ve güvenlik sağlayarak yapay zekanın güvenilir görüşler sunmasını ve yeniliği teşvik etmesini sağlar. Veri kalitesi, uyumluluk ve güvenliğe öncelik vermek, daha iyi kararlar almayı ve rekabet avantajını sürdürmeyi sağlar.

Microsoft 365: Yapay zekaya hazırlığı güçlendirme

Microsoft 365; veri sınıflandırma, kontrol ve korumaya yönelik yerleşik araçlarla sınıfının en iyisi üretkenlik uygulamaları sunar. Bu özellikler, hazır olduğunuzda güvenli yapay zekayı benimsemeyi kolaylaştırarak veri yönetimi çerçevenizi destekler. Microsoft 365 size şunları sağlamanıza yardımcı olur:

- **Veri kalitesi:** Yapay zeka çıktıları için doğruluk ve güvenilirliği destekleyin.
- **Uyumluluk:** Yasal riskleri azaltarak yasal gerekliliklere uyun.
- **Sıfır Güven güvenliği:** Hassas bilgileri yetkisiz erişim, ihlal ve siber tehditlere karşı koruyun.

Kurumunuzun verimli ve güvenli bir şekilde çalışmasına yardımcı olmak için yapay zeka seçenekleri ve sağlam koruma ile geliştirilmiş kapsamlı üretkenlik araçlarını keşfedin.



Microsoft 365'i keşfedin