MULTIVERSERA

Reality Engine

Güven, KVKK ve Etik Yapay Zekâ Notu

Sürüm v0.1 CANONICAL · 2026 · Gizli · Sınırlı Dağıtım

Engine today, Experience OS later · Localize · Combine · Trust

İçindekiler

1. Kısa tanım

Multiversera Reality Engine; kurumlar, şehirler, eğitim yapıları ve kültür varlıkları için yapay zekâ, dijital ikiz, XR ve güven katmanlarını birleştiren modüler çoklu gerçeklik deneyim motorudur. Bu motorun ayrılmaz bir parçası olan **Trust Layer**, güveni sonradan eklenen bir özellik değil; mimarinin temeli olarak ele alır.

Bugünkü dürüst tanım bir motordur; Experience OS ve Reality OS vizyonu 2029–2030 ufkundadır. Güven yaklaşımı ise bugünden, her senaryoda geçerlidir.

2. Neden Trust Layer merkezi?

Yapay zekâ, dijital ikiz ve XR deneyimleri; kişisel veri, kurumsal içerik, kamu bilgisi ve kullanıcı etkileşimiyle çalışır. Bu da beraberinde mahremiyet, doğruluk, temsil ve sorumluluk sorularını getirir. Çoğu projede bu konular en sona bırakılır; Multiversera'da ise tasarımın başına alınır.

Privacy-by-design (tasarımda mahremiyet) ve **ethics-by-design (tasarımda etik)** yaklaşımı, her modülün ve her demonun ilk gününden itibaren güven gereksinimlerini içermesi anlamına gelir. Trust Layer, bu gereksinimleri tek bir tutarlı katmanda toplar ve tüm modüllere uygular.

Trust Layer'ın mimari içindeki yeri

3. Trust Layer neyi yönetir?

Trust Layer, yapay zekâ ve veri içeren her senaryoda şu alanları yönetmeyi hedefler:

- kişisel veri ve KVKK uyum çerçevesi (veri minimizasyonu),
- açık rıza, izin ve amaç sınırlılığı,
- etik yapay zekâ ve izinli dijital persona,
- doğrulanmış bilgi ve kaynak güvenliği,
- yapay zekâ yanıt sınırları ve içerik sınırı,
- rol bazlı erişim ve kurumsal veri ayrımı,
- çocuk ve genç güvenliği,
- erişilebilirlik,
- denetim izi (audit trail) ve insan onayı (human-in-the-loop).

Bu liste bir kontrol listesi değil; her senaryoda gözden geçirilen bir tasarım çerçevesidir.

4. KVKK ve veri minimizasyonu yaklaşımı

Multiversera, kişisel verilerin işlenmesinde **veri minimizasyonu** ilkesini hedefler: yalnızca açık ve meşru bir amaç için gerekli olan asgari veri işlenir; amaç dışı kullanım hedeflenmez.

KVKK ve GDPR açısından her uygulama, ilgili mevzuata göre tasarlanmalı ve **hukuki inceleme gerektirir**. Multiversera "KVKK/GDPR uyumludur" gibi kesin bir hüküm vermez; bunun yerine privacy-by-design yaklaşımıyla, uyum sürecini kolaylaştıracak bir tasarım çerçevesi sunar. Nihai uyum değerlendirmesi, kurumun kendi hukuk ve uyum birimlerinin sorumluluğundadır.

5. Açık rıza, izin ve amaç sınırlılığı

Kişisel veri ve persona kullanımında üç ilke esas alınır:

Açık rıza. Kullanıcı, verisinin hangi amaçla işlendiği konusunda aydınlatılır; rıza açık ve geri alınabilir olmalıdır.

İzin ve temsil yetkisi. Bir kişinin görüntüsü, sesi veya kimliğine dayalı bir dijital persona, yalnızca o kişinin (veya yetkili temsilcisinin) açık izniyle ve sınırlı kapsamda kullanılır.

Amaç sınırlılığı. Veri, toplandığı amacın dışında kullanılmaz; her senaryoda kapsam ve süre önceden tanımlanır.

6. AI avatar / dijital persona sınırları

AvatarWorks ve ilgili senaryolarda dijital persona kullanımı, sıkı sınırlara tabidir:

- Dijital persona bir kişiyi **klonlamaz** ve gerçek bir kişiyi yetkisiz biçimde **temsil etmez**; yalnızca açık izinle ve tanımlı kapsamda kullanılır.
- Persona, onaylanmış kaynaklara dayanır; kapsam dışı konularda konuşmaz.
- Persona kullanımı süre, bağlam ve amaçla sınırlıdır; kişinin hakları sözleşmeyle korunur.
- Avatar, bilmediği konuda "bilmiyorum" der; uydurma (halüsinasyon) yerine sınır içinde kalır.

Amaç, kullanışlı ama **izinli, etik ve denetlenebilir** bir dijital personadır.

7. Doğrulanmış bilgi ve kaynak güvenliği

Avatar ve anlatımlar, onaylı kaynağa dayandırılır. Yaklaşım üç unsuru içerir: kaynak doğrulama (yanıt, güvenilir ve onaylı bir bilgi tabanına bağlanır), içerik sınırı (kapsam dışı veya onaysız içerik üretilmez), ve yanlış bilgi azaltımı (doğruluk denetimi yapılır; belirsizlikte avatar emin gibi davranmaz).

Bu yaklaşım, özellikle kamu, eğitim, kültür ve finansal bilgilendirme senaryolarında yanlış veya yetersiz bilgi riskini azaltmayı hedefler.

8. Kurumsal veri, içerik ve rol bazlı erişim

Kurumsal senaryolarda veri ve içerik, **rol bazlı erişim** ilkesiyle ele alınır: her kullanıcı yalnızca yetkili olduğu veriye ve içeriğe erişir. Kurumsal veri ile kişisel veri ayrı tutulur; hassas içerik yetkisiz görünürlükten korunur.

Üçüncü taraf servislerin (bulut, yapay zekâ, veri altyapısı) kullanımı, veri akışının ve sorumluluk sınırlarının önceden tanımlanmasını gerektirir.

9. Çocuklar, gençler ve eğitim bağlamı için ek hassasiyet

Education & Campus Transformation — Eğitim ve Kampüs Dönüşümü öncelikli giriş alanı dahil, genç kullanıcı olasılığı bulunan senaryolarda (özellikle CampusVerse ve eğitim demoları) ek güvenlik uygulanır: içerik uygunluğu, ek veri koruması, yaşa uygun etkileşim ve gerektiğinde ebeveyn/kurum onayı. Çocuk ve genç güvenliği, bu bağlamda en yüksek öncelikli tasarım gereksinimidir.

10. Kamu, belediye ve afet senaryolarında güven

Civic Resilience & Disaster Awareness — Toplumsal Dayanıklılık ve Afet Farkındalığı öncelikli giriş alanında, CivicVerse ve afet farkındalığı senaryolarında (Disaster Awareness Journey, Civic Service Navigator) güven, doğrudan kamu yararıyla ilgilidir. İlkeler:

- **Panik ve yanlış yönlendirme önlenir:** afet senaryosu eğitsel ve sakinleştirici biçimde tasarlanır; gerçek bir acil durumla karıştırılmayacak şekilde açıkça işaretlenir.
- **Doğru davranış vurgulanır:** içerik, yetkili kaynaklara ve resmî yönergelere dayandırılır.
- **Erişilebilirlik esastır:** kamu hizmeti herkes için ulaşılabilir olmalıdır.

11. Kültürel miras ve turizm deneyimlerinde saygılı temsil

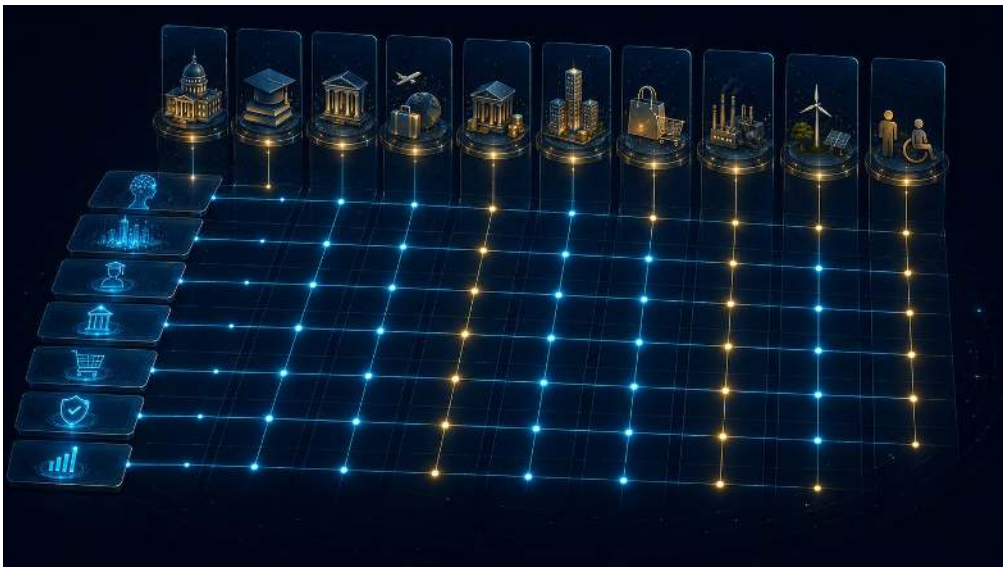
Cultural Heritage & Tourism Experience — Kültürel Miras ve Turizm Deneyimi öncelikli giriş alanında, Heritage Twin ve AI Museum Guide gibi senaryolarda kültürel temsil, **saygı ve doğruluk** ilkesiyle ele alınır: kültürel ve tarihî içerik, onaylı kaynaklara ve ilgili kurumun rehberliğine dayandırılır; hassas kültürel unsurlar saygılı biçimde sunulur; çok dilli erişimde anlam ve bağlam korunur.

12. Etik yapay zekâ ilkeleri

Multiversera'nın etik yapay zekâ yaklaşımı şu ilkelere dayanır: şeffaflık (kullanıcı, bir yapay zekâ ile etkileşimde olduğunu bilir), adalet (bias ve ayrımcılığın azaltılması hedeflenir), hesap verebilirlik (kararlar denetlenebilir ve insan onayına tabidir), sınırlılık (yapay zekâ tanımlı kapsam içinde kalır) ve insan merkezlilik (kritik kararlarda insan onayı esastır).

13. Ölçülebilir güven ve denetim izi

Güven yalnızca bir niyet değil, **ölçülebilir** bir gereksinimdir. Impact Layer ile içerik doğruluğu, erişilebilirlik kullanımı ve etkileşim anonim ve tutarlı biçimde gözlemlenir. **Denetim izi (audit trail)**, kritik işlemlerin izlenebilir olmasını hedefler; **insan onayı (human-in-the-loop)**, kritik kararlarda bir insanın devrede kalmasını sağlar.



Güvenin sektörlere yayılımı

14. Riskler ve azaltım yaklaşımı

Aşağıdaki risk başlıkları her senaryoda gözden geçirilir ve uygun azaltım tasarlanır. Bu bir tam liste veya garanti değil; bir risk farkındalığı çerçevesidir.

Risk başlığı	Azaltım yaklaşımı
Kişisel veri	Veri minimizasyonu, rıza, amaç sınırlılığı
Özel nitelikli veri	İşlemekten kaçınma; gerekiyorsa ek koruma ve hukuki inceleme
Çocuk / genç kullanıcılar	İçerik uygunluğu, ek koruma, yaşa uygun etkileşim
AI avatar / persona izni	Açık izin, temsil yetkisi, kapsam ve süre sınırı
Yatırım tavsiyesi riski	Finansal senaryolarda tavsiye değil, yalnız bilgilendirme; hukuki onay
Yanlış / yetersiz bilgi	Kaynak doğrulama, içerik sınırı, doğruluk denetimi
Kamu / afet senaryosunda panik	Eğitsel tasarım, açık işaretleme, resmî kaynak
Kültür mirası temsili	Saygılı ve onaylı kaynağa dayalı temsil
Erişilebilirlik	WCAG uyumu, altyazı, sesli rehber, klavye gezinme
Bias / ayrımcılık	Adalet ilkesi, içerik denetimi, çeşitlilik gözetimi
Veri saklama ve imha	Tanımlı saklama süresi ve imha; veri minimizasyonu
Yurt dışı veri aktarımı	Aktarım öncesi hukuki inceleme; uygun koruma mekanizmaları
Üçüncü taraf servisler	Veri akışı ve sorumluluk sınırlarının önceden tanımı
İnsan onayı	Kritik kararlarda human-in-the-loop
Denetim izi	Kritik işlemlerde izlenebilirlik

15. Ne değildir?

- Bir hukuki görüş veya hukuki danışmanlık değildir.
- Kesin bir KVKK/GDPR uyum garantisi değildir.
- Bitmiş bir uyum sertifikası veya denetim raporu değildir.
- Bir yatırım veya finansal yönlendirme dokümanı değildir.
- Hazır, canlı bir ürünün güvenlik beyanı değildir.

Bu doküman bir **tasarım ilkesi, uyum çerçevesi ve risk farkındalığı** notudur. Her uygulama, kurumun kendi hukuki ve uyum incelemesini gerektirir.

16. İlk güven değerlendirme görüşmesi (Trust Review)

Bir pilot veya iş birliği öncesinde, ilgili senaryonun güven, KVKK ve etik yapay zekâ gereksinimlerini birlikte gözden geçirdiğimiz bir **Trust Review** görüşmesi öneririz. Bu görüşmede; veri akışı, rıza ve izin yapısı, persona sınırları, kaynak doğrulama, erişilebilirlik ve denetim izi gereksinimleri ele alınır.

Trust Review / ilk görüşme

Ara bölüm / kapanış

17. İletişim

Trust Review veya güven gereksinimleri görüşmesi için: info@multiversera.com

Provenance notu (kısa): Multiversera'nın mahremiyet ve sorumlu teknoloji vizyonu 2022'de dile getirildi; bugün güven katmanı bu vizyonun olgunlaşmış hâlidir. Bu bir ürün kanıtı değil, bir vizyon sürekliliği notudur.

Bu doküman hukuki danışmanlık değildir ve kesin uyum garantisi vermez; tasarım ilkesi, uyum çerçevesi ve risk farkındalığı sunar. Her uygulama bağımsız hukuki inceleme gerektirir.