

ENERGO-PRO GRUP

Yapay Zeka Kullanım Politikası 2025



Yapay Zeka Kullanım Politikası

Sürüm: 1.0 | **Yürürlük tarihi:** 1 Ekim 2025 | **Sahibi:** Yapay Zeka Yönetişim Komitesi (AIGC)

1. Amaç ve Kapsam

- 1.1. Bu Yapay Zeka (YZ-AI) Kullanım Politikası (“Politika”), ENERGO - PRO a.s. (“Şirket”) ve bağlı şirketleri (topluca ‘Grup’) bünyesinde Yapay Zeka (“AI”) araçlarının güvenli, etkili ve sorumlu kullanımına ilişkin bağlayıcı kuralları belirlemektedir. Bu Politikanın amaçları doğrultusunda, Grup, Şirketin tek hissedarı olan DK Holding Investments, s.r.o. ve tüm doğrudan ve dolaylı bağlı şirketlerinden oluşmaktadır.
- 1.2. Amacımız, modern teknolojilerin benimsenmesi yoluyla yenilikçiliği ve üretkenliği desteklerken verilerimizin, fikri mülkiyetimizin, müşterilerimizin ve itibarımızın en üst düzeyde korunmasını sağlamaktır. Yapay zekayı benimsememiz yalnızca inovasyonla değil, aynı zamanda operasyonel güvenlik, kamu güvenliği ve toplumun bize duyduğu güvene olan sıkı bağlılığımızla yönlendirilmelidir.
- 1.3. Yapay zekanın her kullanımının dürüstlük, saygı, şeffaflık ve etik davranış gibi temel etik ilkelerimizle uyumlu olmasını sağlamaya kararlıyız. En önemlisi, yapay zeka odaklı tüm süreçlerimizde insan gözetimi ve sorumluluğu her şeyden önce gelmeye devam edecektir.
- 1.4. Bu Politika, Grubun bilgi sistemlerine erişim sağlayan veya Grup verilerini işleyen tüm çalışanlar, harici yükleniciler, danışmanlar ve tedarikçiler (topluca “Personel”) için geçerlidir. Bu Politika, dahili olarak geliştirilip geliştirilmediğine, üçüncü taraflardan tedarik edilip edilmediğine veya bir kamu hizmeti olarak erişilip erişilmediğine bakılmaksızın, Grup içinde kullanılan tüm Yapay Zeka Sistemleri için geçerlidir.

2. Tanımlar

Bu Politikanın amaçları doğrultusunda, aşağıdaki tanımlar geçerli olacaktır:

- 2.1. **Yapay Zeka Sistemi:** Yapay Zeka Yasasının 3(1) maddesi ile tanımlanan bir yapay zeka sistemi (aşağıda tanımlandığı şekliyle). Farklı seviyelerde özerklikle çalışmak üzere tasarlanmış ve dağıtım sonrasında uyarlanabilirlik sergileyebilen ve açık veya örtük hedefler için, aldığı girdiden, fiziksel veya sanal ortamları etkileyebilecek tahminler, içerik, öneriler veya kararlar benzeri çıktıların nasıl üretileceğini çıkarımlayan herhangi bir makine tabanlı sistem. Bu tanım, Yapay Zeka Sisteminin bağımsız bir uygulama mı yoksa daha büyük bir yazılım paketi içinde entegre bir özellik mi olduğuna bakılmaksızın geçerlidir.

Kurumsal Yapay Zeka: Verilerimizin korunmasını garanti eden bir sözleşmeye dayalı anlaşma (aşağıda tanımlanan bir Veri İşleme Zeyilnamesi de dahil olmak üzere) ile yönetilen onaylı bir Yapay Zeka Sistemi. Böylesi anlaşmalar, satıcının Grup verilerini kendi veya herhangi bir üçüncü taraf modelini eğitmek için kullanmasını açıkça yasaklamalıdır.

Örnekler: M365 için Microsoft Copilot, DeepL Pro.

Kamuya Açık Yapay Zeka: Veri korumasına yönelik sözleşmeye dayalı garantiler sunmayan ve kendi modellerini veya üçüncü taraf modellerini eğitmek veya geliştirmek için girdileri (İstemler) ve çıktıları (Yanıt) kullanabilen, genellikle kamuya açık internette kullanılabilen onaylı bir Yapay Zeka Sistemi.

Örnekler: ChatGPT, Google Gemini, Google Translate uygulamalarının standart sürümleri.

2.2. **Veri Sınıflandırması:** Tüm veriler dört seviyede sınıflandırılmaktadır:

Kamuya Açık (Seviye 1): Yasal olarak kamuya açık olan her türlü bilgi. Bu bilgiler hem Grup tarafından resmi olarak yayınlanan bilgileri hem de harici kamu kaynaklarından alınan bilgileri içermektedir.

Örnekler: Yayınlanmış basın bültenleri, akademik makaleler, haber yazıları, halka açık devlet veri tabanları, kamuya açık web sitelerindeki bilgiler.

Kurum İçi (Seviye 2): Yetkisiz ifşanın düşük risk oluşturacağı kamuya açık olmayan bilgiler.

Örnekler: Genel ekip toplantısı tutanakları (kişisel veri veya ticari sır içermeyen), kurum içi kılavuzlar, hassas olmayan proje taslakları.

Gizli (Seviye 3): Açıklanması halinde Gruba, ortaklarına veya müşterilerine orta veya ağır derecede zarar verebilecek hassas veriler.

Örnekler: Mali planlar, iş stratejileri, denetlenmemiş mali sonuçlar, anonim sözleşmeler.

Çok Gizli (Seviye 4): Yetkisiz ifşanın ciddi yasal, mali veya itibar kaybına yol açabileceği, yasa veya sözleşme ile korunan en hassas veriler.

Örnekler: GDPR tarafından tanımlanan kişisel veriler (aşağıda tanımlanan şekilde) (örneğin, çalışan veya müşteri kayıtları), ticari sırlar, fiyata duyarlı bilgiler, Gizlilik Anlaşması (NDA) ile korunan bilgiler, know-how, sistem girişleri ve şifreleri, özel kaynak kodu, kritik altyapıdan operasyonel veriler (örneğin, SCADA sistemleri), ayrıntılı şebeke güvenlik açığı değerlendirmeleri veya enerji üretim birimlerinin şemaları.

2.3. **Veri İşleme Zeyilnamesi (DPA):** GDPR Madde 28 uyarınca bir veri denetleyicisi ile bir veri işleyici arasında yapılan yasal olarak bağlayıcı bir sözleşme. Kişisel verilerin kontrolör adına işleyici tarafından işlenmesini yönetir. Bir kontrolör kişisel verileri işlemek için bir işleyici görevlendirdiğinde GDPR kapsamında zorunlu bir gerekliliktir.

2.4. **Deepfake:** Mevcut kişilere, nesnelere, mekanlara, konulara veya olaylara benzeyen ve makul bir kişiye yanlışlıkla gerçek veya doğru gibi görünebilecek yapay zeka tarafından oluşturulan veya yapay zeka tarafından manipüle edilen video, ses veya görüntü içeriği.

2.5. **Halüsinasyon:** Bir yapay zeka modelinin, güven ve akıcılıkla sunulmasına rağmen saçma, gerçekte yanlış veya tamamen uydurma çıktılar ürettiği bir olgu.

2.6. **Bilgi İstemi:** Bir çıktıyı ortaya çıkarmak için bir kullanıcı tarafından bir Yapay Zeka Sistemine sunulan soru, talimat veya veri kümesi benzeri herhangi bir girdi.

3. **Görevler, Sorumluluklar ve Yönetişim**

Yapay Zeka Yönetişim Komitesi (AIGC): Üst yönetim, Hukuk, İK ve diğer kilit departmanlardan temsilcilerden oluşan çapraz işlevli bir ekip. Yapay zeka stratejisini, bu Politikayı onaylar ve Kaydın sürdürülmesinden sorumludur.

AI Navigator: Yapay zeka ile ilgili konularda rehberlik ve destek için birincil irtibat noktasıdır. Bu pozisyon proaktif tavsiyelerde bulunur, AIGC'yi destekler ve Personele yapay zeka ile ilgili sorularında yardımcı olur.

Yapay Zeka Sistem Sahibi: Yapay Zeka Yönetişim Komitesi (AIGC) tarafından aksi belirlenmediği sürece, AI Navigator, onaylanan her Yapay Zeka Sistemi için Yapay Zeka Sistem Sahibi olarak hareket edecektir. Yapay Zeka Sistem Sahibi:

1. Yapay Zeka Sisteminin sadece onaylanmış amacı için ve yetkilendirilmiş parametreleri dahilinde kullanılmasını sağlamaktan;
2. denetimler ve performans incelemeleri için öncelikli iş irtibat sorumlusu olarak görev yapmaktan;
3. BT ile koordinasyon içinde kullanıcı erişimini yönetmekten ve
4. Önemli performans sorunlarını veya olayları AIGC'ye iletmek üzere AI Navigator'a bildirmekten sorumludur.

Personel: Personelin her üyesi bu Politikanın anlaşılmasından ve bu Politikaya uyulmasından sorumludur.

4. Yapay Zeka Kullanımının Temel Prensipleri

Grup bünyesinde yapay zekanın her türlü kullanımı aşağıdaki temel ilkelere uygun olmalıdır:

- 4.1. **Human-in-the-Loop (Döngü İçindeki İnsan) (Zorunlu İnsan Gözetimi):** Yapay zeka destekleyici bir araçtır, otonom bir karar verici değildir. Bir Yapay Zeka Sistemi insan yeteneklerine yardımcı olabilir ve bu yetenekleri destekleyebilir, ancak insan yargısının ve hesap verebilirliğinin yerini alamaz. Yapay zeka tarafından üretilen tüm çıktılar, özellikle de potansiyel yasal veya mali sonuçları taşıyanlar, kullanılmadan önce nitelikli ve sorumlu bir kişi tarafından eleştirel bir şekilde incelenmeli, doğrulanmalı ve onaylanmalıdır. İnceleme seviyesi, kararın riskiyle orantılı olmalıdır (örneğin, bir rapordaki tek bir gerçeği doğrulamak, yapay zeka tarafından oluşturulan bir ağ bakım programını onaylamaktan daha az inceleme gerektirmektedir).
- 4.2. **Hesap Verebilirlik:** Yapay zeka tarafından üretilen çıktılara dayalı herhangi bir karar veya eylem için nihai sorumluluk, yapay zeka sistemine değil, bu sistemi kullanan kişiye aittir. Personel, bir Yapay Zeka Sisteminin “halüsinasyon” üretme olasılığına karşı tetikte olmalı ve kritik bilgileri her zaman bağımsız ve güvenilir bir kaynaktan doğrulamalıdır.
- 4.3. **Şeffaflık:** Bir yapay zeka sisteminin gerçek kişilerle (örneğin bir sohbet robotu (chatbot) aracılığıyla) doğrudan etkileşim kurmak üzere tasarlandığı durumlarda, bu kişiler bir yapay zeka sistemiyle etkileşim kurdukları konusunda bilgilendirilmelidir. Gerçek olduğu iddia edilen görüntü, ses veya video içeriği üreten veya manipüle eden personel (pazarlama materyalleri için yapay zeka tarafından üretilen illüstrasyonlardan Deepfake'lere kadar), Bölüm 6.3(iii)'de daha ayrıntılı olarak açıklandığı üzere, içeriğin yapay olarak üretildiğini veya manipüle edildiğini açıkça ve dikkat çekici bir şekilde açıklamalıdır.
- 4.4. **Ayrımcılık Yapmama ve Adalet:** Yapay Zeka Sistemleri, korunan özelliklere (örneğin yaş, cinsiyet, etnik köken) dayalı olarak bireylere veya gruplara karşı haksız önyargı veya ayrımcılık yaratmaktan veya bunları güçlendirmekten kaçınacak şekilde kullanılmalıdır.
- 4.5. **Tasarım Yoluyla Güvenlik ve Gizlilik:** Veri koruma ve güvenlik temel unsurlardır. Satın almadan dağıtım ve nihai olarak hizmetten çıkarmaya kadar tüm yapay zeka projeleri, en başından itibaren gizlilik ve güvenlik ilkelerini bünyesinde barındırmalıdır.

5. Yürürlükteki Mevzuat ve Politikalar

5.1. Yasal ve Düzenleyici Çerçeve

- 5.2. Grubun Yapay Zeka Sistemlerini geliştirmesi, satın alması ve kullanması, yürürlükteki yasalar ve uluslararası standartlar çerçevesine tabidir. Tüm Personelin, bunlarla sınırlı olmamak üzere, aşağıda belirtilen yönetmeliklerin en son sürümlerine uyması gerekmektedir:

Avrupa Parlamentosu ve Konseyinin yapay zekaya ilişkin uyumlaştırılmış kurallara ilişkin 13 Haziran 2024 tarihli ve **2024/1689 (AB) sayılı Yönetmeliği (“Yapay Zeka Yasası”)**.

Avrupa Parlamentosu ve Konseyinin verilere adil erişim ve kullanımına ilişkin uyumlaştırılmış kurallara ilişkin 13 Aralık 2023 tarihli ve **2023/2854 (AB) sayılı Yönetmeliği (“Veri Yasası”)**.

Avrupa Parlamentosu ve Konseyinin Birlik genelinde yüksek bir ortak siber güvenlik seviyesi için alınacak önlemler hakkında 14 Aralık 2022 tarihli ve **2022/2555 (AB) sayılı Direktifi (“NIS 2 Direktifi”)**.

Avrupa Parlamentosu ve Konseyinin Dijital Tek Pazarda Telif Hakkı ve İlgili Haklara İlişkin 17 Nisan 2019 tarihli ve **2019/790 (AB) sayılı Direktifi (“Telif Hakkı Direktifi”)**.

Avrupa Parlamentosu ve Konseyinin kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımı konusunda gerçek kişilerin korunmasına ilişkin 27 Nisan 2016 tarihli ve **2016/679 (AB) sayılı Yönetmeliği (“GDPR”)**.

ISO/IEC 42001:2023 - Bilgi teknolojisi - Yapay zeka - Yönetim sistemi.

İş hukuku, fikri mülkiyet ve hukuki sorumluluk ile ilgili kanunlar dahil olmak üzere, ancak bunlarla sınırlı olmamak üzere, Grubun faaliyet gösterdiği yargı bölgelerinde **geçerli olan tüm ulusal mevzuat**.

5.3. Diğer İç Politikalarla İlişkisi

- 5.4. Bu Politika, diğer bağlayıcı Grup politikalarını tamamlayıcı niteliktedir ve bu politikalarla birlikte okunmalıdır. Personel ayrıca, AI Sistemlerini kullanımlarının, aşağıdakiler dahil ancak bunlarla sınırlı olmamak üzere, diğer tüm ilgili iç politikalara da uygun olmasını sağlamalıdır:

- Davranış Kuralları
- İnsan Hakları Politikası
- İnsan Kaynakları Politikası
- Güvenlik Politikası
- Veri Koruma Politikaları (Kurum İçi ve Kurum Dışı)
- Yüklenici ve Alt Yüklenici Yönetim Planı

- 5.5. Bu Politika ile bir diğer kurum içi politika arasında herhangi bir çelişki olması durumunda, daha kısıtlayıcı olan hüküm geçerli olacaktır. Konu, AIGC tarafından açıklığa kavuşturulması için derhal AI Navigator'a iletilmelidir.

6. Kabul Edilebilir ve Yasaklanmış Kullanım

- 6.1. **Altın Kural: Verilerin Uygun Yapay Zeka Sistemiyle Eşleştirilmesi.**

En önemli ilke, verilerin yalnızca uygun güvenlik düzeyine sahip bir AI Sistemi tarafından işlenmesini sağlamaktır. Bu ilkeye uyulmaması, bu Politikanın ciddi bir ihlalini teşkil etmektedir.

Veri Sınıflandırması	Kamuya Açık Yapay Zeka	Kurumsal Yapay Zeka
Seviye 1: Kamuya açık	İzin verilmektedir	İzin verilmektedir
Seviye 2: Kurum İçi	İzin verilmektedir	İzin verilmektedir
Seviye 3: Gizli	Kısıtlamalarla izin verilmektedir	İzin verilmektedir
Seviye 4: Çok Gizli	Yasak	Yalnızca AIGC onayı ile izin verilmektedir, zorunlu DPIA ve BT Güvenlik Riski Değerlendirmesine tabidir.

6.2. Onaylanmış Yapay Zeka Sistemleri

Genel Kural

Personel, yalnızca resmi “Onaylanmış AI Sistemleri Kaydında” (“Kayıt-Register”) listelenen AI Sistemlerini kullanabilir. Kayıta listelenmeyen herhangi bir AI Sisteminin kullanımı kesinlikle yasaktır.

Bu Politikanın yürürlüğe girdiği tarihte onaylanmış Yapay Zeka Sistemlerinin listesi, referans amaçlı olarak Ek A'da verilmektedir. Kayıtların resmi ve güncel versiyonu AIGC tarafından tutulmakta ve düzenli olarak güncellenmekte olup, Grubun M365 SharePoint platformunda mevcuttur.

Asgari Riskli Yapay Zeka Sistemlerinin Kullanımı

Bir önceki maddeye bakılmaksızın, Personel, bu Politikanın 8. Bölümünde verilen sınıflandırmaya göre “Asgari Riskli Yapay Zeka Sistemi” olarak nitelendirilen, Kayıta yer almayan bir Yapay Zeka Sistemini kullanabilir. Sistemi kullanmak isteyen kişi, sistemin Asgari Riskli Yapay Zeka Sistemi olarak doğru bir şekilde değerlendirilmesi ve sınıflandırılmasından tek başına sorumludur.

Bu istisnadan yararlanan kişi, AI Navigator'a böylesi bir Yapay Zeka Sisteminin kullanımını gecikmeksizin e-posta yoluyla bildirmelidir. Bu tür sistemlerin kullanımı, her zaman bu Politika ve veri koruma (GDPR), bilgi güvenliği ve BT güvenliği ile ilgili olanlar dahil ancak bunlarla sınırlı olmamak üzere tüm diğer Grup politikalarına tam olarak uygun olmalıdır.

Seviye 3 (Gizli) Veriler için Kamuya Açık Yapay Zeka Sistemlerinin Kullanımı

Aşağıda belirtilen koşulların tümü karşılanmadığı sürece, Kamuya Açık Yapay Zeka Sistemleri kullanılarak Seviye 3 (Gizli) Verilerin işlenmesi kesinlikle yasaktır:

- (i) Kullanılan Kamuya Açık Yapay Zeka Sistemi, bu amaçla Kayıttan onaylanmış olmalı ve burada belirtilen koşullara uygun olarak kullanılmalıdır. Bu Politikanın son revizyonu itibarıyla, gerekli yöntemler aşağıda belirtilen şekildedir:
 - **Adobe Acrobat AI Assistant için:** Ek gizlilik ayarları gerektirmeden kullanım için onaylanmıştır. Tasarımında gizlilik öncelikli mimarisi, kullanıcı verilerinin izole edilmesini ve model eğitimi için kullanılmamasını sağlamaktadır.
 - **ChatGPT için:** 'Geçici Sohbet' özelliği kullanılmalıdır.
 - **Google Gemini için:** 'Gemini Apps Activity' ayarı kapatılmalıdır.
 - **NotebookLM için:** Ek gizlilik ayarları gerektirmeden kullanım için onaylanmıştır. Tasarımında gizlilik öncelikli mimarisi, kullanıcı verilerinin izole edilmesini ve model eğitimi için kullanılmamasını sağlamaktadır.
- (ii) Kamuya açık AI sisteminin kullanım koşulları, kullanıcı girdilerinin (komutlar) ve sistem çıktılarının (yanıtlar) sağlayıcı veya üçüncü taraf yapay zeka modellerinin eğitimi veya iyileştirilmesi amacıyla kullanılmayacağını garanti etmektedir.
- (iii) Oturumdan gelen tüm girdiler ve çıktılar, kullanıcının kalıcı konuşma geçmişinde saklanmayacak ve sağlayıcı tarafından otomatik olarak silinecektir. Kullanıcılar, güvenlik ve operasyonel amaçlarla sağlayıcının halihazırda:
 - ChatGPT 'Geçici Sohbet' için en fazla 30 gün ve
 - "Etkinlik" özelliği kapalıyken Google Gemini için 72 saate kadar (3 gün) olan saklama süresini kabul etmelidir.

Kullanıcı, herhangi bir Seviye 3 (Gizli) Veriyi Kamu Yapay Zeka Sistemine göndermeden önce doğru özelliği seçmekten ve geçerli veri saklama süresini anlamaktan sorumludur.

6.3. Yasaklanmış Faaliyetler

Yapay zekanın aşağıda belirtilen amaçlarla kullanılması kesinlikle yasaktır:

- (i) Yürürlükteki yasalara, özellikle de Yapay Zeka Yasasının 5. maddesinde tanımlanan yasaklanmış uygulamalara aykırı olan veya Grubun Davranış Kuralları veya yürürlükteki diğer kurum içi politikalara aykırı olan her türlü faaliyet;
- (ii) Bölüm 6.2'de belirtilen kısıtlamalara uymadan herhangi bir Kamuya Açık Yapay Zeka Sistemine herhangi bir Seviye 4 Verisinin girilmesi veya herhangi bir Kamuya Açık Yapay Zeka Sistemine herhangi bir Seviye 3 Verisinin girilmesi;
- (iii) Deepfake'lerin ve yapay zeka tarafından üretilen diğer sentetik medyanın kötü niyetli, dolandırıcılık veya aldatma amaçlı olarak veya herhangi bir şekilde, herhangi bir kişiyi içeriğin gerçek olduğuna inandırmak amacıyla yaratılması veya yayılması yasaktır.

Meşru bir şekilde açıklayıcı, eğitici, tasarım, eğitim veya diğer ticari amaçlarla yapay zeka tarafından üretilen veya yapay zeka ile manipüle edilen görüntüler, sesler, videolar veya benzer çıktıların oluşturulmasına ve kullanılmasına:

- a. içeriğin hedef kitleye yapay zeka tarafından üretilmiş/yapay zeka tarafından manipüle edilmiş olduğunun açıkça (örneğin, varlık üzerinde bir etiket, başlık, filigran, meta veri bildirimi, slayt dipnotu veya kullanım noktasında görülebilen diğer eşlik eden bilgilerle) belirtilmesi ve
- b. içeriğin gerçek dünyadaki kişiler, nesneler, mekanlar, konular veya olayların gerçek kayıtları olarak sunulmaması

kaydıyla izin verilmektedir.

- (iv) Çalışanları, müşterileri veya kamuoyunu taklit etmek veya aldatıcı bir şekilde etkileşim kurmak amacıyla gerçekçi, insan benzeri avatarların oluşturulması ve kullanılması.
- (v) Anlamlı bir insan denetimi ve gözetimi olmaksızın bireyler hakkında nihai, otomatik kararlar alınması (örneğin, işe alım, performans değerlendirmeleri veya işten çıkarma).
- (vi) Onaylanmış bir Yapay Zeka Sisteminin güvenlik önlemlerinin veya kullanım sınırlamalarının etrafından dolaşılmasına yönelik her türlü girişim.

6.4. Teşvik Edilen Faaliyetler

Onaylanmış Yapay Zeka Sistemlerinin kullanılması memnuniyetle karşılanmakta ve teşvik edilmektedir. Aşağıda verilen liste, faydalı uygulamalara ilişkin örnekler sunan, kapsamlı olmayan bir liste niteliğindedir:

- (i) E-postaların, raporların veya sunumların hazırlanmasına yardım edilmesi.
- (ii) Belgelerin tercüme edilmesi (veri sınıflandırma kurallarına tabi olarak).
- (iii) Belgelerin özetlenmesi ve verilerin analiz edilmesi yoluyla yeni anlayışların belirlenmesi.
- (iv) Beyin fırtınası yapılması ve kavramsal taslakların oluşturulması.
- (v) Tekrarlayan görevleri otomatikleştirilmesi (örneğin, elektronik tablo formüllerinin oluşturulması).
- (vi) Kamuya açık verilere dayalı enerji piyasası eğilimleri hakkında teknik raporların ilk taslaklarının hazırlanması ve tüm olguların ve rakamların daha sonra konunun uzmanı tarafından doğrulanması.

Yukarıda belirtilmeyen olası kullanım durumlarında, Personel gerekli özeni göstermeli ve önerilen kullanımın bu Politikanın temel ilkelerine ve diğer tüm geçerli yasal ve kurum içi düzenlemelere tam olarak uygun olduğundan emin olmalıdır. Her zaman sağlam bir mesleki muhakeme sergilenmelidir. Önerilen kullanımın izin verilebilirliği veya uygunluğu konusunda herhangi bir belirsizliğin söz konusu olması halinde, devam etmeden önce AI Navigator ile istişarede bulunulması zorunludur.

7. Yapay Zeka Sistemlerinin Temini ve Onaylanması

7.1. Her yeni Yapay Zeka Sistemi, kullanılmadan önce aşağıdaki onay sürecinden geçmelidir:

- (i) **Talep Gönderimi:** Kişi, resmi formu kullanarak bir talepte bulunmalıdır (bakınız Ek B).

- (ii) **İlk Değerlendirme:** AI Navigator temel kriterlere göre talebi inceleyecektir.
- (iii) **Risk Değerlendirmesi:** AIGC ayrıntılı bir risk değerlendirmesi gerçekleştirecektir (bakınız Bölüm 8).
- (iv) **Karar:** AIGC, AI Sistemini onaylayacak, reddedecek veya belirli sınırlamalarla onaylayacaktır.
- (v) **Kayıt:** Onaylanan Yapay Zeka Sistemi, Kayda kaydedilecektir.

8. Risk Değerlendirmesi ve Sistem Sınıflandırması

8.1. Her Yapay Zeka Sistemi, Yapay Zeka Yasasının dört katmanlı risk modeline göre sınıflandırılacaktır:

Kabul Edilemez Risk: Yasa ve bu Politika tarafından yasaklanan Yapay Zeka Sistemleri (örneğin, sosyal puanlama).

Yüksek Risk: Bireylerin sağlığını, güvenliğini veya temel haklarını önemli ölçüde etkileyebilecek Yapay Zeka Sistemleri (örneğin, kritik altyapının yönetiminde kullanılan bir Yapay Zeka Sistemi veya iş başvurularını filtrelemek için kullanılan bir Yapay Zeka Sistemi) dahil olmak üzere, Yapay Zeka Yasasının 6. maddesinde belirtilen kriterleri karşılayan bir Yapay Zeka Sistemi. Bu tür sistemler, zorunlu kayıt, sıkı testler ve sürekli izleme dahil olmak üzere daha katı kurallara tabidir.

Sınırlı Risk: Bu kategori, manipülasyon veya aldatma konusunda belirli riskler taşıyan ve bu nedenle belirli şeffaflık yükümlülüklerine tabi olan Yapay Zeka Sistemlerini kapsamaktadır. Bu yükümlülükler, Yapay Zeka Sisteminin türüne ve kullanımına göre değişiklik göstermektedir:

- **Doğrudan Etkileşim Sistemleri (örneğin, Sohbet Robotları):** Kurum içi İK desteği veya dış müşteri hizmetleri için sohbet robotları gibi bireylerle doğrudan etkileşim kurmak üzere tasarlanmış sistemleri kullanırken, kullanıcılara bir yapay zeka ile iletişim kurdukları açıkça bildirilmelidir.
- **Sentetik Medya (Görseller, Ses, Video):** Gerçekçi görseller, ses veya video içerikleri (örneğin Deepfakes) oluşturmak veya manipüle etmek için kullanılan yapay zeka sistemlerinin çıktıları, içerik açıkça sanatsal veya yaratıcı nitelikte olup gerçekliği temsil etme amacı taşımadığı sürece, “yapay zeka tarafından oluşturulmuş” veya “yapay olarak manipüle edilmiş” olarak açıkça etiketlenmelidir.
- **Metin Üretimi için Genel Amaçlı Yapay Zeka (GPAI):** ChatGPT, Gemini ve Copilot benzeri araçların dayandığı modeller, Genel Amaçlı Yapay Zeka (GPAI) olarak kabul edilmektedir ve sağlayıcılarının şeffaflık gerekliliklerine tabidir. Kullanıcılar (dağıtımıcılar) olarak amaçlarımız doğrultusunda, bu araçlar metin özetleme, e-posta taslakları hazırlama veya beyin fırtınası gibi yardımcı işlevler için kullanıldığında, kullanımdan önce anlamlı bir insan incelemesi ve editoryal kontrole tabi tutulması koşuluyla, üretilen metnin yapay zeka tarafından oluşturulduğunun söylenmesi gerekli değildir. Bu durumlarda, yapay zeka bir yardımcı olarak işlev görmektedir ve içeriğin nihai sorumluluğu tamamen Personele aittir.

Minimal Risk: Bu kategori, bireylerin hakları, özgürlükleri veya güvenliği için ihmal edilebilir düzeyde risk oluşturan Yapay Zeka Sistemleri için geçerlidir. Bir sistem, yalnızca:

- Gerçek kişilerin yasal haklarını etkileyen kararlar veya tespitler yapmaması;

- Hassas kişisel verileri işlememesi ve
- Olası arızası veya hatalı çıktısı, malzeme güvenliği üzerinde herhangi bir etkiye sahip olmaması

koşulların tümünü karşıladığı takdirde Minimum Risk olarak sınıflandırılabilir.

Bir Yapay Zeka Sistemi, kullanım amacının kişisel, biyometrik veya güvenlik açısından kritik verilerin işlenmesini içerecek şekilde değiştirilmesi durumunda, daha yüksek bir risk kategorisine (Sınırlı veya Yüksek Risk) yeniden sınıflandırılabilir. Yapay Zeka Yasası tarafından özellikle düzenlenmemiş olsa da, herhangi bir Asgari Riskli Yapay Zeka Sisteminin kullanımı, bu Politikada belirtilen genel ilkelere uymak zorundadır.

Asgari Riskli Yapay Zeka Sistemlerine Örnekler: Yapay zeka destekli spam filtreleri, hava durumu tahmin modelleri, talep tahmini için basit yapay zeka kullanan envanter yönetim sistemleri, kelime işleme veya e-posta istemcilerine entegre edilmiş dilbilgisi ve yazım denetimi yardımcıları, hızlı anlama için kullanılan makine çevirisi araçları (örneğin, web sitesi otomatik çevirisi) (halka açık metinlerin çevirisi, hassas veriler söz konusu olmadığında ihmal edilebilir düzeyde risk oluşturur)

9. Veri Koruma, Fikri Mülkiyet ve Güvenlik

Tasarımda Gizlilik: Tasarım gereği ve varsayılan olarak veri koruma ilkesi, her yapay zeka projesine başlangıçtan itibaren entegre edilmelidir.

DPIA: Gerçek kişilerin hak ve özgürlükleri açısından yüksek risk oluşturması muhtemel tüm yapay zeka sistemleri için Veri Koruma Etki Değerlendirmesi (bakınız Ek C) zorunludur.

Yapay Zeka Tarafından Üretilen İçeriğin Fikri Mülkiyeti: Personel, yapay zeka tarafından üretilen içeriğin yasal statüsünün karmaşık ve sürekli değiştiğinin farkında olmalıdır. Onaylanmış bir yapay zeka sisteminin şartlarında aksi açıkça belirtilmediği sürece, yapay zeka tarafından üretilen çıktılar telif hakkı korumasına tabi olmayabilir veya üçüncü şahısların haklarına tabi olabilir. İstihdam süresince yapay zeka kullanılarak oluşturulan tüm içerikler Grubun çalışma ürünü olarak kabul edilmekle birlikte, personel Grubun münhasır telif hakkına sahip olduğunu düşünmemelidir. Yapay zeka tarafından üretilen içeriğin kamuya açık materyallerde veya ticari ürünlerde kullanılması için önceden AI Navigator ile görüşülmesi gerekmektedir.

Gizli Bilgilerin ve Fikri Mülkiyetin Korunması: Personel, Grubun hassas bilgilerini korumak konusunda son derece dikkatli davranmalıdır. Bu bilgiler arasında bunlarla sınırlı olmamak üzere ticari sırlar, fiyat açısından hassas bilgiler, teknik bilgiler, gizlilik anlaşmalarıyla korunan bilgiler, telif hakları ve sınai mülkiyet hakları sayılabilir. 6. Bölümde belirtildiği üzere, bu tür bilgiler hiçbir şekilde Kamuya Açık Yapay Zeka Sistemine girilmemelidir.

Güvenlik: Tüm Yapay Zeka Sistemleri, belirlediğimiz siber güvenlik standartlarına uymak zorundadır.

10. İzleme, Raporlama ve Ölçütler

Yapay Zeka Sistemlerimizin performansı, doğruluğu ve güvenliği izlenecektir.

Yüksek Riskli Yapay Zeka Sistemleri için, AIGC'ye düzenli performans raporları sunulması zorunludur.

Sadece teknik parametreleri değil, aynı zamanda elde edilen iş değeri de (örneğin, kazanılan zaman, proses iyileştirmeleri) ölçülecektir.

11. Olaylara Müdahale ve Değişiklik Yönetimi

Olaylar: Bir Yapay Zeka Sistemini ilgilendiren her türlü olay (örneğin, veri ihlali, önemli etkiye sahip hatalı çıktı, ayrımcılık şüphesi) derhal AI Navigator'a bildirilmelidir.

Değişiklikler: Bir Yapay Zeka Sisteminde yapılan herhangi bir önemli değişiklik (örneğin, yeni bir sürüm, kullanım amacıyla bir değişiklik), AIGC tarafından yeni bir risk değerlendirmesi yapılmasını gerektirmektedir. Önemli değişiklikler arasında, bunlarla sınırlı olmamak üzere, sistemin kullanım amacıyla bir değişiklik, temel modelinin yeni bir ana sürümünün kullanıma sunulması veya veri girişleri veya çıkışlarında önemli bir değişiklik sayılabilir.

12. Personel Eğitimi ve Yapay Zeka Okuryazarlığı

Zorunlu Eğitim: Tüm Personelin, bu Politika, veri güvenliği, risk farkındalığı (ayrımcılık ve halüsinasyonlar dahil) ve onaylanmış AI Sistemlerinin doğru kullanımı konularını kapsayan AI kullanımı konusunda ilk eğitimi alması gerekmektedir. Örneğin, yasal düzenlemelerde veya AI Sistemlerimizde önemli güncellemeler yapıldıktan sonra, ihtiyaç duyulması halinde ek eğitimler verilecektir.

İleri Seviye Eğitim: Yapay zeka ile yoğun olarak çalışan personele, onaylanmış yapay zeka sistemlerinin etkili komutları ve gelişmiş özelliklerine odaklanarak sunulmaktadır.

Yapay Zeka Portalı: Yapay zeka ile ilgili tüm hususlarda merkezi kaynak noktası olarak hizmet veren dahili bir SharePoint sitesi. Bu site, kayıt defterini, kullanıcı kılavuzlarını, eğitim materyallerini, politika belgelerini ve iletişim bilgilerini içermektedir.

13. Üçüncü Taraf ve Tedarikçi Yönetimi

Herhangi bir Kurumsal Yapay Zeka Sisteminin satın alınması öncesinde, satıcı kapsamlı bir durum tespiti sürecine tabi tutulacaktır. Bu değerlendirme, tedarikçinin güvenlik duruşunu, uyumluluk sertifikalarını, itibarını ve yapay zeka modelleriyle ilgili şeffaflığını değerlendirecektir.

Tartışmaya Açık Olmayan Gerekliklik: Yapay zeka sistemi bizim kamuya açık olmayan verilerimizi (Seviye 2-4) işleyecek olan tüm tedarikçilerle imzalı bir Veri İşleme Zeyilnamesi (DPA) imzalanmalıdır. Bu DPA, tedarikçinin modellerini eğitmek için verilerimizi kullanmasını yasaklamalıdır.

14. Politika Gözden Geçirme ve Denetim

Bu Politika, sürekli güncellenen bir belgedir. AIGC, önemli teknolojik veya yasal değişikliklere yanıt olarak, en azından yılda bir kez veya daha sık aralıklarla bu Politikayı gözden geçirecek ve güncelleyecektir. İç Denetim, bu Politikaya uygunluğu periyodik olarak doğrulayacaktır.

15. Uygunsuzluk Durumlarında Uygulanacak Yaptırımlar

Bu Politikanın ihlali, iş akdine belirtilen görevlerinin ciddi bir ihlali olarak değerlendirilecek olup, iç düzenlemeler ve geçerli yasalar uyarınca, iş akdinin veya sözleşmenin feshine kadar varan disiplin cezalarına tabi tutulabilir.

16. Ekler (Yapay Zeka Portalında Mevcuttur)

- **Ek A:** Onaylanmış Yapay Zeka Sistemleri Kaydı
- **Ek B:** Yeni Bir Yapay Zeka Sisteminin Onaylanması için Talep Formu
- **Ek C:** Veri Koruma Etki Değerlendirmesi (DPIA) Şablonu
- **Ek D:** İletişim Bilgileri

Ek A: Onaylanmış Yapay Zeka Sistemleri Kaydı

Son Güncelleme: 1 Ekim 2025 | Muhafaza Eden: AI Navigator

Bu kayıt, Grup içinde kullanım için değerlendirilmiş ve onaylanmış AI Sistemlerinin kesin bir listesini sunmaktadır. Bu listede yer almayan herhangi bir Yapay Zeka Sistemi, Yapay Zeka Yönetişim Komitesi (AIGC) tarafından açıkça onaylanmadığı sürece yasaklanmış olarak kabul edilmektedir.

Yapay Zeka Sisteminin Adı	Kategori	Risk Sınıflandırması	Onaylanmış Kullanım Örnekleri	İzin Verilen Maksimum Veri Sınıflandırması	Durum
Adobe Acrobat AI Assistant	Hakla Açık Yapay Zeka	Sınırlı Risk	AI Assistant, belgelerinizi hızlı bir şekilde analiz ederek önemli bilgileri ayıklar, kalıpları belirler ve tüm yanıtları metin içindeki kaynaklara doğrudan bağlayarak karmaşık soruları yanıtlar.	Kısıtlamalarla birlikte Seviye 3 (Gizli)	Onaylı
Celsia AI Assistant	Kurumsal Yapay Zeka	Sınırlı Risk	Kurum içi Grup belgelerinden ilgili bilgilerin filtrelenmesi, kısa özetlerin hazırlanması ve ESG ile ilgili soruların yanıtlanması.	Seviye 4 (Çok Gizli)	Onaylı
ChatGPT (Ücretsiz/Plus sürümleri)	Hakla Açık Yapay Zeka	Sınırlı Risk	E- postaların yazılması, belgelerin özetlenmesi, fikirlerin beyin fırtınası veya metinlerin çevirisi.	Kısıtlamalarla birlikte Seviye 3 (Gizli)	Onaylı
DeepL Pro	Kurumsal Yapay Zeka	Sınırlı Risk	“Çok Gizli” ibaresi bulunanlar dahil olmak üzere belgelerin tercümesi.	Seviye 4 (Çok Gizli)	Onaylı
Google Gemini	Hakla Açık Yapay Zeka	Sınırlı Risk	E- postaların yazılması, belgelerin özetlenmesi, fikirlerin beyin fırtınası veya metinlerin çevirisi.	Kısıtlamalarla birlikte Seviye 3 (Gizli)	Onaylı
Google Translate	Hakla Açık Yapay Zeka	Sınırlı Risk	Sadece hassas olmayan, kamuya açık bilgilerin tercümesi.	Seviye 2 (Kurum İçi)	Onaylı

M365 için Microsoft Copilot	Kurumsal Yapay Zeka	Sınırlı Risk	E-postaların yazılması, belgelerin ve toplantıların özetlenmesi, Microsoft 365 uygulamaları içinde veri analizi.	Seviye 4 (Çok Gizli)	Onaylı
NotebookLM	Hakla Açık Yapay Zeka	Sınırlı Risk	Belirli proje belgelerinin, araştırmaların ve toplantı notlarının özetlerini, gerçeklere dayalı cevapları ve yalnızca özel kaynaklarınıza dayanan yeni kavrayışlar için sorgulayabileceğiniz etkileşimli bir uzmana dönüştürülmesi.	Seviye 3 (Gizli)	Onaylı

Ek B: Yeni Bir Yapay Zeka Sisteminin Onaylanması için Talep Formu

Grup amaçları için kullanmak istediğiniz yeni Yapay Zeka Sistemleri için lütfen bu formu eksiksiz olarak doldurun ve AI Navigator'a gönderin.

1. Bölüm: Talep Eden Bilgileri

- **Adı Soyadı:**
- **Departmanı:**
- **İş Unvanı:**
- **Talep Tarihi:**

2. Bölüm: Yapay Zeka Sistemi Bilgileri

- **Yapay Zeka Sisteminin Adı:**
- **Tedarikçi/Sağlayıcı:**
- **Sistemin Web Sitesi Bağlantısı:**
- **Gizlilik Politikası / Hizmet Şartları bağlantısı:**

3. Bölüm: Kullanım Amacı

- **Ticari Amaç:** (Çözmeye çalıştığınız iş sorununu ve bu Yapay Zeka Sisteminin nasıl yardımcı olacağını açıklayın. Başlıca hedef nedir?)
- **Belirli Görevler:** (Bu Yapay Zeka Sistemi ile gerçekleştirmek istediğiniz belirli görevleri listeleyin, örneğin, “Hukuki sözleşmelerin tercümesi”, “Pazarlama metinlerinin oluşturulması”, “Müşteri geri bildirimlerinin analizi”.)

4. Bölüm: Veri Kullanımı

- **Bu Yapay Zeka Sistemi ile işlemek istediğiniz en yüksek veri sınıflandırma seviyesi nedir?** (Yapay Zeka Politikası 2.2 bölümüne bakınız)
 - ☐ Seviye 1: Kamuya Açık
 - ☐ Seviye 2: Kurum İçi
 - ☐ Seviye 3: Gizli
 - ☐ Seviye 4: Çok Gizli
- **Yapay Zeka Sistemi, GDPR'da tanımlanan Kişisel Verileri işleyecek mi?**
 - ☐ Evet

- ☐ [] Hayır
- **Yapay Zeka Sistemi, bireyler üzerinde önemli etkisi olan kararların alınmasında (örneğin, işe alım, performans değerlendirmesi) kullanılacak mı?**
 - ☐ [] Evet
 - ☐ [] Hayır

5. Bölüm: İlk Risk Değerlendirmesi

- **Tedarikçi, verilerimizin kendisinin veya herhangi bir üçüncü tarafın model eğitimi için kullanılmasını açıkça yasaklayan bir Veri İşleme Zeyilnamesi (DPA) sağlıyor mu?**
 - ☐ [] Evet
 - ☐ [] Hayır
 - ☐ [] Bilmiyorum
- **Bildiğiniz kadarıyla, bu Yapay Zeka Sistemi ile ilgili bilinen herhangi bir güvenlik açığı veya etik sorun var mı? (Varsa, lütfen ayrıntıları belirtin.)**

Sadece AIGC tarafından Kurum İçi Kullanım İçin

- **Talep No.:**
- **Alındığı Tarih:**
- **AI Navigator Değerlendirmesi:** Tamamlandı / Tamamlanmadı
- **AIGC Kararı:** Onaylandı / Reddedildi / Sınırlamalarla Onaylandı
- **Karar Tarihi:**
- **Gerekçe / Sınırlamalar:**

Ek C: Yapay Zeka Sistemi için Veri Koruma Etki Değerlendirmesi (DPIA) Şablonu

Bu şablon, özellikle de kişisel verilerin büyük ölçekte işlendiği veya işlemenin gerçek kişilerin hak ve özgürlükleri açısından yüksek risk oluşturmasının muhtemel olduğu durumlarda Yüksek Riskli olarak sınıflandırılan herhangi bir Yapay Zeka Sistemi veya Seviye 4 (Çok Gizli) verileri işleyen herhangi bir Yapay Zeka Sistemi için doldurulmalıdır.

DPIA Referansı: [Benzersiz ID]

Yapay Zeka Sisteminin Adı: [Yapay Zeka Sisteminin Adı]

Yapay Zeka Sistemi Sahibi: [İsim]

Değerlendirme Tarihi: [Tarih]

1. Kısım: İşlemenin Açıklaması

- **İşlemenin Niteliği ve Kapsamı:** Yapay zeka sisteminin işlevselliğini, işleyeceği verilerin niteliğini, veri hacmini ve ilgili veri sahiplerinin kategorilerini açıklayın.
- **İşleme Amacı:** Grup, müşteriler veya çalışanlar açısından hedeflenen sonuçlar ve faydalar neler?
- **İşleme Bağlamı:** Veri sahipleriyle olan ilişkinizi ve onların makul beklentilerini açıklayın. Veri kaynaklarını ve üçüncü taraflara yapılan veri akışlarını ayrıntılı olarak belirtin.

2. Kısım: Gerekliklik ve Orantılılık Değerlendirmesi

- **Yasal Dayanak:** GDPR 6. Madde uyarınca kişisel verilerin işlenmesinin yasal dayanağı nedir?
- **Amaç Sınırlaması:** Veriler, belirtilen, açık ve meşru amaçlar için mi işleniyor?
- **Veri Azaltma:** İşlenen veriler, işlendikleri amaçlarla ilgili olarak yeterli, ilgili ve gerekli olanla sınırlı mıdır?

3. Kısım: Risk Değerlendirmesi

- **Veri Sahiplerinin Hak ve Özgürlüklerine Yönelik Riskler:** Potansiyel riskleri belirleyin, örneğin:
 - Yetkisiz erişim veya veri ihlali.
 - Yanlış kararlara yol açan hatalı çıktılar.
 - Çıktılarda (örneğin, işe alım veya kredi puanlamasında) ayrımcı önyargı.
 - Yapay zeka destekli kararlarda şeffaflık veya açıklanabilirlik olmaması.
 - Anonimleştirilmiş veya takma adla anonimleştirilmiş verilerin yeniden tanımlanması.

- **Olasılık ve Ciddiyet:** Tanımlanan her risk için, olasılığını (Düşük/Orta/Yüksek) ve potansiyel etki şiddetini değerlendirin.

4. Kısım: Risklerin Azaltılması için Öngörülen Önlemler

- **Teknik Önlemler:** Uygulanan güvenlik kontrollerini açıklayın (örneğin, şifreleme, erişim kontrolleri, takma ad kullanımı)..
- **Organizasyonel Önlemler:** Prosedürel kontrolleri açıklayın (örneğin, insan gözetimi, düzenli denetimler, personel eğitimi, tedarikçi DPA).
- **Önyargı Azaltma:** Algoritmik önyargıyı test etmek ve azaltmak için atılan adımları açıklayın.
- **Şeffaflık Tedbirleri:** Veri sahipleri, AI Sisteminin kullanımı ve hakları konusunda nasıl bilgilendirilecek?

5. Kısım: İstişare ve Onay

- **VKG ile istişare:** Veri Koruma Görevlisi tarafından verilen tavsiyeleri kaydedin.
- **AIGC Kararı:**
 - ☐ İşlemeye başlayın.
 - ☐ Ek önlemlerin uygulanmasına bağlı olarak işlemeye başlayın.
 - ☐ İşlemeye başlamayın.
 - ☐ Denetim Makamına danışın.

İmzalar:

- **Yapay Zeka Sistemi Sahibi:** _____
- **Veri Koruma Görevlisi:** _____
- **AIGC Başkanı:** _____

Ek D: İletişim Bilgileri

Bu Politika veya Grup içinde yapay zeka kullanımı ile ilgili her türlü sorunuz için lütfen ilgili kişilerle iletişime geçiniz.

Birincil İrtibat Noktası

- **AI Navigator**
 - **İsim:** Tomáš Brandejský
 - **E-posta:** t.brandejsky@energo-pro.com
 - **Sorumluluklar:** Personel için birinci basamak destek, eğitim koordinasyonu ve Yapay Zeka Sistemi onay sürecinin yönetimi.

Yönetişim ve Eskalasyon

- **Yapay Zeka Yönetişim Komitesi (AIGC)**
 - **Başkan:** Jakub Fajfr
 - **Genel Hukuk Müşaviri:** Christian Blatchford
 - **Veri Koruma Görevlisi (VKG):** Marina Radeva
 - **İK Bölüm Başkanı:** Nikola Šugra
 - **E-posta:** AIGC@energo-pro.com
 - **Sorumluluklar:** Stratejik gözetim, Onaylı Yapay Zeka Sistemleri Kaydının onaylanması ve düzenli olarak güncellenmesi, Yapay Zeka Politikasının onaylanması, risk yönetimi ve Yüksek Riskli Yapay Zeka Sistemleri için nihai onay.