ENERGO-PRO GROUP

Zásady používání umělé inteligence

2025

Zásady používání umělé inteligence

Verze: 1.0 | **Účinnost od:** 1. října 2025 | **Vlastník:** Výbor pro řízení umělé inteligence (AIGC)

1. Cíl a oblast působnosti

1.1. Tyto Zásady používání umělé inteligence (dále jen „**Zásady**“) stanovují závazná pravidla pro bezpečné, efektivní a odpovědné používání nástrojů umělé inteligence (dále jen „**AI**“) v rámci společnosti ENERGO – PRO a.s. (dále jen „**Společnost**“) a jejích přidružených společností (dále jen „**Skupina**“). Pro účely těchto Zásad zahrnuje Skupina společnost DK Holding Investments, s.r.o., která je jediným akcionářem Společnosti, a všechny její přímé i nepřímé dceřiné společnosti.

1.2. Naším cílem je podpořit inovace a produktivitu prostřednictvím zavádění moderních technologií a zároveň zajistit nejvyšší úroveň ochrany našich dat, duševního vlastnictví, zákazníků a dobrého jména. Naše zavádění AI musí být vedeno nejen inovacemi, ale i pevným závazkem k provozní bezpečnosti, veřejné bezpečnosti a důvěře, kterou v nás společnost vkládá.

1.3. Jsme odhodláni zajistit, aby veškeré využívání AI bylo v souladu s našimi základními etickými zásadami integrity, respektu, transparentnosti a etického jednání. Zásadní je, že ve všech našich procesech s podporou AI bude i nadále prvořadý lidský dohled a odpovědnost.

1.4. Tyto Zásady se vztahují na všechny zaměstnance, externí dodavatele, konzultanty a dodavatele, kteří mají přístup k informačním systémům Skupiny nebo zpracovávají údaje Skupiny (dále společně jen jako „**Zaměstnanci**“). Zásady se vztahují na veškeré Systémy AI používané v rámci Skupiny bez ohledu na to, zda byly vyvinuty interně, pořízeny od třetích stran nebo zda k nim lze přistupovat jako k veřejné službě.

2. Definice pojmů

Pro účely těchto Zásad se použijí následující definice:

2.1. **Systém AI:** Systém AI, jak je definován v čl. 3 odst. 1 Aktu o umělé inteligenci (jak je tento pojem definován níže). Jakýkoli strojový systém, který je navržen tak, aby fungoval s různými stupni autonomie a který může po nasazení vykazovat adaptivitu, a který pro explicitní nebo implicitní cíle odvozuje ze vstupních údajů, které obdrží, jak generovat výstupy, jako jsou předpovědi, obsah, doporučení nebo rozhodnutí, které mohou ovlivňovat fyzické nebo virtuální prostředí. Tato definice platí bez ohledu na to, zda je Systém AI samostatnou aplikací nebo integrovanou funkcí v rámci většího softwarového balíku.

Podniková AI: Schválený Systém AI, který se řídí smluvním ujednáním (včetně Dodatku o zpracování údajů, jak je tento pojem definován níže), které zaručuje ochranu našich údajů. Taková ujednání musí výslovně zakazovat, aby dodavatel používal data Skupiny k trénování svých vlastních modelů nebo modelů třetích stran.

Příklady: Microsoft Copilot for M365, DeepL Pro.

Veřejná AI: Schválený Systém AI, obvykle dostupný na veřejném internetu, který nenabízí žádné smluvní záruky ochrany dat a může používat vstupy (prompty) a výstupy (odpovědi) k trénování nebo vylepšování vlastních modelů nebo modelů třetích stran.

Příklady: Standardní verze ChatGPT, Google Gemini, Google Translate.

2.2. **Klasifikace údaje:** Všechny údaje jsou klasifikovány do čtyř úrovní:

Veřejné (úroveň 1): Veškeré informace, které jsou legálně veřejně dostupné. Patří sem jak informace oficiálně zveřejněné Skupinou, tak informace z externích veřejných zdrojů.

Příklady: Zveřejněné tiskové zprávy, akademické práce, zpravodajské články, veřejné vládní databáze, informace na veřejně přístupných webových stránkách.

Interní (úroveň 2): Neveřejné informace, jejichž neoprávněné zveřejnění by představovalo nízké riziko.

Příklady: Obecné zápisy z porad týmu (neobsahující osobní údaje ani obchodní tajemství), interní příručky, návrhy projektů neobsahující citlivé údaje.

Důvěrné (úroveň 3): Citlivé údaje, jejichž zveřejnění by mohlo způsobit Skupině, jejím partnerům nebo zákazníkům střední až vážnou újmu.

Příklady: Finanční plány, obchodní strategie, neauditované finanční výsledky, anonymizované smlouvy.

Přísně důvěrné (úroveň 4): Nejcitlivější údaje chráněné zákonem nebo smlouvou, jejichž neoprávněné zveřejnění by mohlo vést k vážným právním, finančním nebo reputačním škodám.

Příklady: Osobní údaje ve smyslu nařízení GDPR (jak je tento pojem definován níže) (např. záznamy o zaměstnancích nebo zákaznících), obchodní tajemství, cenově citlivé informace, informace chráněné dohodou o mlčenlivosti (NDA), know-how, systémová přihlašovací jména a hesla, proprietární zdrojový kód, provozní údaje z kritické infrastruktury (např. systémy SCADA), podrobná posouzení zranitelnosti sítě nebo schémata jednotek pro výrobu energie.

2.3. **Dodatek o zpracování údajů (DPA):** Právně závazná smlouva uzavřená mezi správcem údajů a zpracovatelem údajů podle článku 28 nařízení GDPR. Upravuje zpracování osobních údajů zpracovatelem jménem správce. Je povinným požadavkem podle nařízení GDPR vždy, když správce zapojí zpracovatele do zpracování osobních údajů.

2.4. **Deepfake:** Jakékoli video, zvuk nebo obraz generovaný nebo manipulovaný umělou inteligencí, který se podobá existujícím osobám, objektům, místům, předmětům nebo událostem a mohl by se rozumně uvažující osobě jevit jako autentický nebo pravdivý.

2.5. **Halucinace:** Jev, kdy model umělé inteligence generuje nesmyslné, fakticky nesprávné nebo zcela vymyšlené výstupy, přestože jsou prezentovány plynule a s jistotou.

2.6. **Prompt:** Jakýkoli vstup, jako je otázka, pokyn nebo soubor dat, který uživatel zadá Systému AI za účelem získání výstupu.

3. Role, odpovědnosti a řízení

Výbor pro řízení umělé inteligence (AIGC): Mezioborový tým složený ze zástupců vrcholového vedení, právního oddělení, oddělení lidských zdrojů a dalších klíčových oddělení. Schvaluje strategii AI, tyto Zásady a odpovídá za vedení Registru.

AI Navigátor: Hlavní kontaktní místo pro poradenství a podporu v záležitostech souvisejících s AI. Tato role poskytuje proaktivní poradenství, podporuje AIGC a pomáhá Zaměstnancům s dotazy týkajícími se AI.

Vlastník Systému AI: Neurčí-li Výbor pro řízení umělé inteligence (AIGC) jinak, vystupuje AI Navigátor jako Vlastník Systému AI pro každý schválený Systém AI. Vlastník Systému AI zodpovídá za:

1. zajištění toho, aby byl Systém AI používán výhradně ke schválenému účelu a v rámci jeho schválených parametrů;
2. slouží jako hlavní obchodní kontakt pro audity a přezkumy výkonnosti;
3. řízení přístupu uživatelů v koordinaci s IT; a
4. hlášení jakýchkoli významných problémů s výkonem nebo incidentů AI Navigátorovi, který je předá AIGC.

Zaměstnanci: Každý zaměstnanec je odpovědný za pochopení a dodržování těchto Zásad.

4. Základní zásady používání AI

Veškeré používání AI v rámci Skupiny musí být v souladu s následujícími základními zásadami:

4.1. **Human-in-the-Loop (povinný lidský dohled):** AI je podpůrný nástroj, nikoliv autonomní rozhodovací orgán. Systém AI může pomáhat a podporovat lidské schopnosti, ale nenahrazuje lidský úsudek a odpovědnost. Všechny výstupy generované AI, zejména ty s potenciálními právními nebo finančními důsledky, musí být před použitím kriticky přezkoumány, ověřeny a schváleny kvalifikovanou a odpovědnou osobou. Úroveň kontroly musí být úměrná riziku rozhodnutí (např. ověření jedné skutečnosti ve zprávě vyžaduje menší kontrolu než schválení plánu údržby sítě vygenerovaného AI).

4.2. **Odpovědnost:** Konečnou odpovědnost za jakékoli rozhodnutí nebo akci založenou na výstupu vygenerovaném AI nese osoba, která jej používá, nikoli samotný Systém AI. Zaměstnanci musí zůstat ostražití vůči možnosti, že Systém AI může vytvářet „halucinace“, a musí vždy ověřovat kritické informace z nezávislého a spolehlivého zdroje.

4.3. **Transparentnost:** Pokud je Systém AI určen k přímé interakci s fyzickými osobami (například prostřednictvím chatbota), musí být tyto osoby informovány o tom, že komunikují se Systémem AI. Zaměstnanci, kteří vytváří nebo zpracovává obrazový, zvukový nebo video obsah, který se jeví jako autentický (od ilustrací generovaných AI pro marketingové materiály až po Deepfakes), musí jasně a zřetelně informovat o tom, že byl obsah uměle vytvořen nebo zpracován, jak je podrobněji popsáno v článku 6.3 písm. iii).

4.4. **Zákaz diskriminace a nestrannost:** Systémy AI musí být používány tak, aby nedocházelo k vytváření nebo posilování neférové předpojatosti nebo diskriminace jednotlivců nebo skupin na základě chráněných charakteristik (např. věku, pohlaví, etnického původu).

4.5. **Bezpečnost a ochrana soukromí „by design“:** Ochrana a bezpečnost údajů jsou zásadní. Všechny projekty AI, od jejich pořízení až po nasazení a případné vyřazení z provozu, musí od počátku respektovat zásady ochrany soukromí a bezpečnosti.

5. Platné právní předpisy a zásady

5.1. Právní a regulační rámec

5.2. Vývoj, pořizování a používání Systémů AI ve Skupině se řídí rámcem platných právních předpisů. Všichni zaměstnanci jsou povinni dodržovat nejnovější verze zejména následujících předpisů:

Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci („**Akt o umělé inteligenci**“).

Nařízení Evropského parlamentu a Rady (EU) 2023/2854 ze dne 13. prosince 2023 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání („**Nařízení o datech**“).

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii („**směrnice NIS 2**“).

Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu („**směrnice o autorském právu**“).

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů („**GDPR**“).

ISO/IEC 42001:2023 – Informační technologie – Umělá inteligence – Systém řízení.

Veškeré platné vnitrostátní právní předpisy v zemích, kde Skupina působí, včetně zákonů upravujících pracovní právo, duševní vlastnictví a občanskoprávní odpovědnost.

5.3. Vztah k ostatním interním zásadám

5.4. Tyto Zásady doplňují ostatní závazné interní předpisy Skupiny a je třeba je číst ve spojení s nimi. Zaměstnanci jsou rovněž povinni zajistit, aby to, jak používají Systémy AI, bylo rovněž v souladu se všemi ostatními příslušnými interními předpisy, včetně zejména:

- Etického kodexu
- Politika lidských práv
- Politika lidských zdrojů
- Bezpečnostní politika
- Politika ochrany osobních údajů (interní a externí)
- Plánu řízení dodavatelů a subdodavatelů

5.5. V případě rozporu mezi těmito Zásadami a jinými interními zásadami se použije přísnější ustanovení. Záležitost by měla být neprodleně postoupena AI Navigátorovi k vyjasnění ze strany AIGC.

6. Přijatelné a zakázané použití Systémů AI

6.1. Zlaté pravidlo: Přiřazení údajů k odpovídajícímu Systému AI.

Nejdůležitější zásadou je zajistit, aby údaje zpracovával pouze Systém AI s odpovídající úrovní zabezpečení. Nedodržení této zásady představuje závažné porušení těchto Zásad.

Klasifikace údajů	**Veřejná AI**	**Podniková AI**
Úroveň 1: Veřejné	Povoleno	Povoleno
Úroveň 2: Interní	Povoleno	Povoleno
Úroveň 3: Důvěrné	Povoleno s omezením	Povoleno
Úroveň 4: Přísně důvěrné	Zakázáno	Povoleno pouze se souhlasem AIGC, s výhradou povinného posouzení dopadu na ochranu osobních údajů (DPIA) a posouzení rizik v oblasti bezpečnosti IT.

6.2. Schválené Systémy AI

Obecné pravidlo

Zaměstnanci smí používat pouze ty Systémy AI, které jsou uvedeny v oficiálním „Registru schválených Systémů AI" (dále jen „**Registr**"). Používání jakéhokoli Systému AI, který není uveden v Registru, je přísně zakázáno.

Seznam Systémů AI schválených k datu účinnosti těchto Zásad je pro přehlednost připojen jako příloha A. Směrodatnou, živou verzi Registru udržuje a pravidelně aktualizuje AIGC a je k dispozici na serveru M365 SharePoint Skupiny.

Používání Systémů AI s minimálním rizikem

Bez ohledu na předchozí ustanovení je Zaměstnancům povoleno používat Systém AI, který není uveden v Registru, za předpokladu, že takový systém splňuje podmínky „Systému AI s minimálním rizikem" podle klasifikace uvedené v článku 8 těchto Zásad. Osoba, která hodlá systém používat, nese výhradní odpovědnost za jeho správné posouzení a klasifikaci jako Systému AI s minimálním rizikem.

Osoba, která využije této výjimky, oznámí použití takového systému umělé inteligence bez zbytečného odkladu e-mailem Navigátorovi AI. Používání každého takového systému musí být vždy v plném souladu s těmito Zásadami a všemi ostatními interními předpisy Skupiny, včetně zejména zásad týkajících se ochrany údajů (GDPR), bezpečnosti informací a bezpečnosti IT.

Používání veřejných Systémů AI pro údaje úrovně 3 (důvěrné)

Zpracování údajů úrovně 3 (důvěrné) pomocí veřejných Systémů AI je přísně zakázáno, s výjimkou případů, kdy jsou splněny všechny následující podmínky:

(i) Použitý veřejný Systém AI musí být pro tento účel schválen v Registru a používán v souladu s podmínkami v něm uvedenými. K poslední revizi těchto Zásad jsou požadované metody následující:

- **Pro Adobe Acrobat AI Assistant:** Schváleno pro použití bez požadavku na další nastavení ochrany soukromí. Jeho architektura privacy-by-design (ochrana soukromí již od návrhu) zajišťuje, že jsou údaje uživatelů izolované a nepoužívají se k trénování modelů.
- **Pro ChatGPT:** Je nutné použít funkci ‚Temporary Chat'.
- **Pro Google Gemini:** Je nutné vypnout nastavení ‚Gemini Apps Activity'.
- **Pro NotebookLM:** Schváleno pro použití bez požadavku na další nastavení ochrany soukromí. Jeho architektura privacy-by-design (ochrana soukromí již od návrhu) zajišťuje, že jsou údaje uživatelů izolované a nepoužívají se k trénování modelů.

(ii) Podmínky používání veřejného Systému AI zaručují, že uživatelské vstupy (prompty) a systémové výstupy (odpovědi) nebudou použity pro účely trénování nebo vylepšování modelů AI poskytovatele nebo třetích stran.

(iii) Žádné vstupy a výstupy z relace nesmí být uchovávány v trvalé historii konverzací uživatele a musí podléhat automatickému výmazu poskytovatelem. Uživatelé musí vzít na vědomí dobu uchovávání údajů poskytovatele pro bezpečnostní a provozní účely, která v současné době činí:

- až 30 dní pro ChatGPT ‚Temporary Chat'.
- až 72 hodin (3 dny) pro Google Gemini s vypnutou funkcí ‚Aktivity'.

Uživatel zodpovídá za výběr správné funkce a pochopení příslušné doby uchovávání údajů před odesláním jakýchkoli údajů úrovně 3 (důvěrné) do veřejného Systému AI.

6.3. Zakázané činnosti

Používání AI k následujícím účelům je přísně zakázáno:

(i) Jakákoli činnost, která je v rozporu s platnými právními předpisy, zejména se zakázanými praktikami definovanými v článku 5 Aktu o umělé inteligenci, nebo porušuje Etický kodex Skupiny či jiné platné interní předpisy.

(ii) Zadávání jakýchkoli údajů 4. úrovně do jakéhokoli veřejného Systému AI nebo zadávání jakýchkoli údajů 3. úrovně do jakéhokoli veřejného Systému AI bez dodržení omezení uvedených v článku 6.2.

(iii) Vytváření nebo šíření Deepfakes a jiných syntetických médií generovaných umělou inteligencí za zlomyslným, podvodným nebo klamavým účelem – nebo jakýmkoli způsobem, který má nebo může uvést jakoukoli osobu v omyl, že obsah je autentický – je zakázáno.

Vytváření a používání obrázků, zvukových výstupů, video výstupů nebo srovnatelných výstupů generovaných nebo zpracovaných umělou inteligencí je jinak povoleno pro legitimní ilustrační, vzdělávací, designové, školicí nebo jiné obchodní účely za předpokladu, že:

a. bude zamýšlenému publiku jasně sděleno, že obsah byl vytvořen / zpracován umělou inteligencí (například štítkem na snímku, popiskem, vodoznakem, poznámkou k metadatům, poznámkou pod čarou ke snímku nebo jinou doprovodnou informací viditelnou v místě použití); a

b. obsah není prezentován jako faktický záznam skutečných osob, objektů, míst, subjektů nebo událostí.

(iv) Vytváření a používání realistických avatarů v lidské podobě za účelem vydávání se za zaměstnance, zákazníky nebo členy veřejnosti nebo klamavé interakce s nimi.

(v) Přijímání konečných automatizovaných rozhodnutí o jednotlivcích (např. při náboru, hodnocení výkonnosti nebo ukončení pracovního poměru) bez smysluplného lidského dohledu a kontroly.

(vi) Jakýkoli pokus o obcházení bezpečnostních opatření nebo omezení používání schváleného Systému AI.

6.4. **Doporučené činnosti**

Vítáme a podporujeme používání schválených Systémů AI. Následující seznam je ilustrativní, nikoliv vyčerpávající, a uvádí příklady prospěšných aplikací:

(i) Pomoc při návrhu e-mailů, zpráv nebo prezentací.

(ii) Překládání dokumentů (s výhradou pravidel klasifikace údajů).

(iii) Shrnutí dokumentů a analýza dat za účelem zjištění nových poznatků.

(iv) Brainstorming a vytváření koncepčních návrhů.

(v) Automatizace opakujících se úloh (např. generování vzorců v tabulkovém procesoru).

(vi) Prvotní návrhy technických zpráv o trendech na trhu s energií na základě veřejných údajů, přičemž všechna fakta a čísla následně ověřuje odborník na danou problematiku.

U všech potenciálních případů použití, které nejsou uvedeny výše, musí Zaměstnanci postupovat s náležitou opatrností a zajistit, aby navrhované použití bylo plně v souladu se základními principy těchto Zásad a všemi dalšími platnými právními a interními předpisy. Je třeba vždy zachovávat zdravý odborný úsudek. Existuje-li jakákoli nejistota ohledně přípustnosti nebo souladu navrhovaného použití, je před pokračováním povinná konzultace s Navigátorem AI.

7. Pořizování a schvalování Systémů AI

7.1. Každý nový Systém AI musí před svým použitím projít následujícím schvalovacím procesem:

(i) **Podání žádosti:** Osoba podá žádost na oficiálním formuláři (viz Příloha B).

(ii) **Prvotní posouzení:** Navigátor AI posoudí žádost podle základních kritérií.

(iii) **Posouzení rizik:** AIGC provede podrobné posouzení rizik (viz článek 8).

(iv) **Rozhodnutí:** AIGC schválí, zamítne nebo schválí Systém AI se stanovenými omezeními.

(v) **Registrace:** Schválený Systém AI se zapíše do Registru.

8. Posouzení rizik a klasifikace systému

8.1. Každý Systém AI se klasifikuje podle čtyřstupňového modelu rizik Aktu o umělé inteligenci:

Nepřijatelné riziko: Systémy AI, které jsou zakázány zákonem a těmito Zásadami (např. hodnocení sociálního kreditu).

Vysoké riziko: Systém AI, který splňuje kritéria stanovená v článku 6 Aktu o umělé inteligenci, včetně zejména Systémů AI, které by mohly významně ovlivnit zdraví, bezpečnost nebo základní práva osob (např. Systém AI používaný při řízení kritické infrastruktury nebo Systém AI používaný pro filtrování žádostí o zaměstnání). Takové systémy podléhají přísnějším pravidlům, včetně povinné registrace, přísného testování a průběžného monitorování.

Omezené riziko: Tato kategorie zahrnuje Systémy AI, které představují specifické riziko manipulace nebo podvodu, a proto podléhají specifickým povinnostem z hlediska transparentnosti. Tyto povinnosti se liší v závislosti na typu Systému AI a jeho použití:

- **Systémy přímé interakce (např. chatboti):** Při používání systémů určených k přímé interakci s jednotlivci, jako jsou chatboti pro interní podporu lidských zdrojů nebo externí zákaznický servis, musí být uživatelé jasně informováni o tom, že komunikují s umělou inteligencí.
- **Syntetická média (obrázky, zvuk, video):** Systémy AI používané k vytváření nebo manipulaci s realistickým obrazovým, zvukovým nebo video obsahem (např. Deepfakes) musí mít své výstupy jasně označeny jako „Vytvořeno umělou inteligencí“ nebo „Uměle manipulováno“, pakliže se nejedná o zjevně umělecký nebo kreativní obsah, který nemá představovat realitu.
- **Všeobecná umělá inteligence (GPAI) pro generování textu:** Základní modely nástrojů, jako jsou ChatGPT, Gemini a Copilot, jsou považovány za všeobecnou umělou inteligenci (GPAI) a podléhají požadavkům na transparentnost ze strany jejich poskytovatelů. Pro naše účely jakožto uživatelů, pokud jsou tyto nástroje používány pro asistenční funkce, jako je shrnutí textu, návrhy e-mailů nebo brainstorming, není třeba generovaný text označovat jako generovaný umělou inteligencí za předpokladu, že je před použitím podroben smysluplné lidské revizi a redakční kontrole. V těchto případech funguje umělá inteligence jako asistent a konečnou odpovědnost za obsah nese výhradně Zaměstnanec.

Minimální riziko: Tato kategorie se vztahuje na Systémy AI, které představují zanedbatelné riziko pro práva, svobody nebo bezpečnost osob. Systém je klasifikován jako systém s minimálním rizikem pouze tehdy, pokud splňuje všechny následující podmínky:

- Nečiní rozhodnutí nebo určení, která by měla vliv na zákonná práva fyzických osob;
- nezpracovává citlivé osobní údaje a
- jeho případné selhání nebo chybný výstup by neměly významný dopad na bezpečnost.

Systém AI může být přeřazen do vyšší kategorie rizika (omezené nebo vysoké riziko), pokud je jeho zamýšlený účel změněn tak, aby zahrnoval zpracování osobních, biometrických nebo bezpečnostně kritických údajů. Ačkoli to Akt o umělé inteligenci výslovně neupravuje, musí používání jakéhokoli Systému AI s minimálním rizikem dodržovat obecné principy stanovené v těchto Zásadách.

Příklady Systémů AI s minimálním rizikem: Filtry nevyžádané pošty využívající umělou inteligenci, modely předpovědi počasí, systémy řízení zásob využívající jednoduchou umělou inteligenci pro předpovídání poptávky, gramatické a pravopisné kontroly zabudované do textových editorů nebo e-mailových klientů, nástroje pro strojový překlad (např. automatický překlad webových stránek) používané pro rychlé porozumění (překlad veřejně dostupného textu představuje zanedbatelné riziko pouze tehdy, nejedná-li se o citlivá data)

9. Ochrana dat, duševní vlastnictví a bezpečnost

Ochrana soukromí „by design“: Zásada ochrany údajů „by design“ a ve výchozím nastavení musí být integrována do každého projektu AI od samého počátku.

Posouzení vlivu na ochranu osobních údajů (DPIA): Posouzení vlivu na ochranu osobních údajů (viz Příloha C) je povinné pro každý Systém AI, který může mít za následek vysoké riziko pro práva a svobody fyzických osob.

Duševní vlastnictví obsahu vytvořeného pomocí AI: Zaměstnanec si musí být vědom toho, že právní status obsahu vytvořeného pomocí AI je složitý a stále se vyvíjí. Není-li v podmínkách schváleného Systému AI výslovně uvedeno jinak, nemusí výstupy generované AI podléhat ochraně autorských práv nebo mohou být předmětem práv třetích stran. Veškerý obsah vytvořený pomocí AI v průběhu pracovního poměru je považován za pracovní produkt Skupiny, ale Zaměstnanec by neměl předpokládat, že Skupina vlastní výhradní autorská práva. Použití obsahu vytvořeného pomocí AI ve veřejně přístupných materiálech nebo komerčních produktech vyžaduje předchozí konzultaci s Navigátorem AI.

Ochrana důvěrných informací a duševního vlastnictví: Zaměstnanec musí dbát zvýšené opatrnosti při ochraně citlivých informací Skupiny. To zahrnuje zejména obchodní tajemství, citlivé cenové informace, know-how, informace chráněné dohodou o mlčenlivosti (NDA), autorská práva a práva průmyslového vlastnictví. Jak je uvedeno v článku 6, takové informace nesmí být nikdy vkládány do veřejného Systému AI.

Bezpečnost: Všechny Systémy AI musí splňovat naše zavedené standardy kybernetické bezpečnosti.

10. Monitorování, podávání zpráv a metriky

Budeme monitorovat výkonnost, přesnost a bezpečnost našich Systémů AI.

U vysoce rizikových Systémů AI jsou povinné pravidelné zprávy o výkonnosti pro AIGC.

Budeme měřit nejen technické parametry, ale také vytvořenou obchodní hodnotu (např. úsporu času, zlepšení procesů).

11. Reakce na incidenty a řízení změn

Incidenty: Jakýkoli incident týkající se Systému AI (např. narušení bezpečnosti údajů, chybný výstup s významným dopadem, podezření na diskriminaci) musí být neprodleně nahlášen Navigátorovi AI.

Změny: Jakákoli významná změna Systému AI (např. nová verze, změna jeho zamýšleného použití) vyžaduje nové posouzení rizik ze strany AIGC. Významná změna zahrnuje mimo jiné:

změnu zamýšleného účelu systému, nasazení nové hlavní verze jeho základního modelu nebo podstatnou změnu jeho datových vstupů nebo výstupů.

12. Školení Zaměstnanců a gramotnost v oblasti umělé inteligence

Povinná školení: Všichni zaměstnanci jsou povinni absolvovat úvodní školení o využívání umělé inteligence, které zahrnuje tuto politiku, bezpečnost dat, povědomí o rizicích (včetně diskriminace a tzv. halucinací) a správné používání schválených AI systémů. Další školení bude probíhat podle potřeby, například po zásadních změnách právních předpisů nebo našich AI systémů.

Pokročilá školení: Jsou poskytována zaměstnancům, kteří intenzivně pracují s AI, se zaměřením na efektivní formulaci promptů a pokročilé funkce schválených Systémů AI.

Portál AI: Interní stránka SharePoint sloužící jako centrální centrum zdrojů pro všechny záležitosti týkající se AI. Obsahuje Registr, uživatelské příručky, školicí materiály, dokumenty se zásadami a kontaktní informace.

13. Řízení třetích stran a dodavatelů

Před pořízením jakéhokoli podnikového Systému AI musí být dodavatel podroben důkladnému procesu hloubkové kontroly. V rámci tohoto posouzení se vyhodnotí bezpečnostní pozice dodavatele, certifikace shody, pověst a transparentnost týkající se jeho modelů AI.

Bezpodmínečný požadavek: S každým dodavatelem, jehož Systém AI bude zpracovávat naše neveřejné údaje (úrovně 2-4), musíme mít podepsaný Dodatek o zpracování údajů (DPA). Tento Dodatek musí zakazovat dodavateli používat naše údaje k trénování jeho modelů.

14. Přezkum a audit Zásad

Tyto Zásady jsou živým dokumentem. AIGC ji přezkoumává a aktualizuje nejméně jednou ročně nebo i častěji v reakci na významné technologické nebo legislativní změny. Interní audit pravidelně ověřuje dodržování těchto Zásad.

15. Sankce za nedodržení

Porušení těchto Zásad se považuje za závažné porušení pracovních povinností a může být předmětem disciplinárního opatření v souladu s interními předpisy a platnými právními předpisy, a to včetně ukončení pracovněprávního vztahu.

16. Přílohy (k dispozici na Portálu AI)

- **Příloha A:** Registr schválených Systémů AI
- **Příloha B:** Formulář žádosti o schválení nového Systému AI
- **Příloha C:** Šablona pro posouzení vlivu na ochranu osobních údajů (DPIA)
- **Příloha D:** Kontaktní údaje

Příloha A: Registr schválených Systémů AI

Poslední aktualizace: 1. října 2025 | **Spravuje:** Navigátor AI

Tento registr obsahuje konečný seznam Systémů AI, které byly posouzeny a schváleny pro použití v rámci Skupiny. Jakýkoli Systém AI, který není uveden v tomto seznamu, je považován za zakázaný, nebyl-li výslovně schválen Výborem pro řízení umělé inteligence (AIGC).

Název Systému AI	**Kategorie**	**Klasifikace rizik**	**Příklady schválených případů použití**	**Max. povolená klasifikace údajů**	**Stav**
Adobe Acrobat AI Assistant	Veřejná AI	Omezené riziko	AI Assistant rychle analyzuje dokumenty a získává klíčové informace, identifikuje vzorce a odpovídá na složité otázky, přičemž všechny odpovědi jsou přímo propojeny se zdroji v textu.	Úroveň 3 (důvěrné) s omezeními	**Schváleno**
Celsia AI Assistant	Podniková AI	Omezené riziko	Filtrování relevantních informací z interních dokumentů Skupiny, vytváření stručných shrnutí a zodpovídání otázek souvisejících s ESG.	Úroveň 4 (přísně důvěrné)	**Schváleno**
ChatGPT (verze Free/Plus)	Veřejná AI	Omezené riziko	Návrh e-mailů, shrnutí dokumentů, brainstorming nápadů nebo překlady textu.	Úroveň 3 (důvěrné) s omezeními	**Schváleno**
DeepL Pro	Podniková AI	Omezené riziko	Překlad dokumentů, včetně dokumentů obsahujících přísně důvěrné informace.	Úroveň 4 (přísně důvěrné)	**Schváleno**
Google Gemini	Veřejná AI	Omezené riziko	Návrh e-mailů, shrnutí dokumentů, brainstorming nápadů nebo překlady textu.	Úroveň 3 (důvěrné) s omezeními	**Schváleno**
Google Translate	Veřejná AI	Omezené riziko	Překlad pouze necitlivých, veřejných informací.	Úroveň 2 (interní)	**Schváleno**
Microsoft Copilot for M365	Podniková AI	Omezené riziko	Návrh e-mailů, shrnutí dokumentů a schůzek, analýza dat v rámci aplikací Microsoft 365.	Úroveň 4 (přísně důvěrné)	**Schváleno**

NotebookLM	Veřejná AI	Omezené riziko	Přetváří konkrétní projektové dokumenty, výzkumy a poznámky z jednání do podoby interaktivního experta, kterého se můžete dotazovat na shrnutí, věcné odpovědi a nové poznatky podložené pouze vašimi soukromými zdroji.	Úroveň 3 (důvěrné)	**Schváleno**

Příloha B: Formulář žádosti o schválení nového Systému AI

Tento formulář celý vyplňte a předložte jej Navigátorovi AI pro každý nový Systém AI, který chcete používat pro účely Skupiny.

Oddíl 1: Informace o žadateli

- **Celé jméno:**
- **Oddělení:**
- **Pracovní pozice:**
- **Datum žádosti:**

Oddíl 2: Podrobnosti o Systému AI

- **Název Systému AI:**
- **Dodavatel/Poskytovatel:**
- **Odkaz na webové stránky Systému:**
- **Odkaz na Zásady ochrany osobních údajů / Podmínky poskytování služeb:**

Oddíl 3: Zamýšlené použití

- **Obchodní účel:** (Popište prosím obchodní problém, který se snažíte vyřešit, a jak vám tento Systém AI pomůže. Jaký je hlavní cíl?)
- **Konkrétní úkoly:** (Uveďte konkrétní úkoly, které hodláte s tímto Systémem AI provádět, např. „Překlad smlouvy“, „Vytvoření marketingové kopie“, „Analýza zpětné vazby od zákazníků“)

Oddíl 4: Využití údajů

- **Jakou nejvyšší úroveň klasifikace údajů hodláte pomocí tohoto Systému AI zpracovávat?** (Viz článek 2.2 Zásad používání AI)
    - [ ] Úroveň 1: Veřejné
    - [ ] Úroveň 2: Interní
    - [ ] Úroveň 3: Důvěrné
    - [ ] Úroveň 4: Přísně důvěrné
- **Bude Systém AI zpracovávat nějaké osobní údaje ve smyslu GDPR?**
    - [ ] Ano

- [ ] Ne

- **Bude Systém AI používán k rozhodování, které má významný dopad na fyzické osoby (např. nábor zaměstnanců, hodnocení výkonnosti)?**
  - [ ] Ano
  - [ ] Ne

Oddíl 5: Prvotní posouzení rizik

- **Poskytuje dodavatel Dodatek o zpracování údajů (DPA), který výslovně zakazuje použití našich údajů pro trénink jeho modelů nebo modelů třetích stran?**
  - [ ] Ano
  - [ ] Ne
  - [ ] Nevím
- **Jsou vám známy nějaké bezpečnostní zranitelnosti nebo etické obavy spojené s tímto Systémem AI?** (Pokud ano, uveďte podrobnosti.)

Pouze pro interní potřebu AIGC

- **ID žádosti:**
- **Datum přijetí:**
- **Posouzení Navigátorem AI:** Úplné / Neúplné
- **Rozhodnutí AIGC:** Schváleno / Zamítnuto / Schváleno s omezením
- **Datum rozhodnutí:**
- **Odůvodnění / Omezení:**

Příloha C: Šablona pro posouzení vlivu na ochranu údajů (DPIA) pro Systém AI

Tato šablona musí být vyplněna pro každý Systém AI klasifikovaný jako **vysoce rizikový** nebo pro každý Systém AI, který zpracovává údaje **úrovně 4 (přísně důvěrné**), zejména jsou-li osobní údaje zpracovávány ve velkém rozsahu nebo je-li pravděpodobné, že zpracování povede k vysokému riziku pro práva a svobody fyzických osob.

Značka DPIA: \Unikátní ID]

Název Systému AI: [Název Systému AI]

Vlastník Systému AI: [Název]

Datum posouzení: [Datum]

Část 1: Popis zpracování

- **Povaha a rozsah zpracování:** Popište funkce Systému AI, povahu údajů, které bude zpracovávat, objem údajů a kategorie dotčených subjektů údajů.
- **Účel zpracování:** Jaké jsou zamýšlené výsledky a přínosy pro Skupinu, zákazníky nebo zaměstnance?
- **Kontext zpracování:** Popište vztah se subjekty údajů a jejich přiměřená očekávání. Podrobně uveďte zdroje údajů a případné toky údajů ke třetím stranám.

Část 2: Posouzení nezbytnosti a přiměřenosti

- **Právní základ:** Jaký je právní základ pro zpracování osobních údajů podle článku 6 GDPR?
- **Omezení účelu:** Jsou údaje zpracovávány výhradně pro stanovené, výslovně vyjádřené a legitimní účely?
- **Minimalizace údajů:** Jsou zpracovávané údaje přiměřené, relevantní a omezené na to, co je nezbytné vzhledem k účelům, pro které jsou zpracovávány?

Část 3: Posouzení rizik

- **Rizika pro práva a svobody subjektů údajů:** Identifikujte potenciální rizika, jako např:
    - Neoprávněný přístup nebo porušení zabezpečení údajů.
    - Nepřesné výstupy vedoucí k nesprávným rozhodnutím.
    - Diskriminační předpojatost ve výstupech (např. při náboru zaměstnanců nebo hodnocení úvěruschopnosti).
    - Nedostatečná transparentnost nebo vysvětlitelnost rozhodnutí za podpory umělé inteligence.

- Opětovná identifikace anonymizovaných nebo pseudonymizovaných údajů.

- **Pravděpodobnost a závažnost:** U každého identifikovaného rizika posuďte jeho pravděpodobnost (nízká/střední/vysoká) a potenciální závažnost dopadu.

Část 4: Plánovaná opatření ke zmírnění rizik

- **Technická opatření:** Popište zavedené bezpečnostní kontroly (např. šifrování, řízení přístupu, pseudonymizace).
- **Organizační opatření:** Popište procesní kontroly (např. lidský dohled, pravidelné audity, školení zaměstnanců, DPA dodavatele).
- **Zmírňování zaujatosti:** Popište opatření přijatá k testování a zmírňování algoritmické zaujatosti.
- **Opatření pro zajištění transparentnosti:** Jak budou subjekty údajů informovány o používání Systému AI a o svých právech?

Část 5: Konzultace a schvalování

- **Konzultace s pověřencem pro ochranu osobních údajů (DPO):** Zaznamenejte konzultace poskytnuté pověřencem pro ochranu osobních údajů.
- **Rozhodnutí AIGC:**
  - [ ] Pokračovat ve zpracovávání.
  - [ ] Pokračovat ve zpracovávání s výhradou zavedení dodatečných opatření.
  - [ ] Zpracovávání neprovádět.
  - [ ] Konzultovat s orgánem dohledu.

Podpisy:

- **Vlastník Systému AI:** _____
- **Pověřenec pro ochranu osobních údajů:** _____
- **Předseda AIGC:** _____

Příloha D: Kontaktní údaje

V případě jakýchkoli dotazů týkajících se těchto Zásad nebo používání AI v rámci Skupiny kontaktujte příslušné osoby.

Hlavní kontaktní místo

- **Navigátor AI**
    - **Jméno:** Tomáš Brandejský
    - **E-mail:** t.brandejsky@energo-pro.com
    - **Zodpovídá za:** Podporu Zaměstnanců v první linii, koordinaci školení a řízení schvalovacího procesu Systému AI.

Řízení a eskalace

- **Výbor pro řízení umělé inteligence (AIGC)**
    - **Předseda:** Jakub Fajfr
    - **Vedoucí právního oddělení:** Christian Blatchford
    - **Pověřenec pro ochranu osobních údajů (DPO):** Marina Radeva
    - **Vedoucí personálního oddělení:** Nikola Šugra
    - **E-mail:** AIGC@energo-pro.com
    - **Zodpovídá za:** Strategický dohled, schvalování a pravidelné aktualizace Registru schválených Systémů AI, schvalování Zásad používání AI, řízení rizik a konečné schvalování vysoce rizikových Systémů AI.