Doporučení k využívání nástrojů umělé inteligence na UP

Praktický průvodce pro výuku, vědu, výzkum, administrativu a podpůrné činnosti

Univerzita Palackého v Olomouci

Verze 4.5.2026

Jak dokument používat

Dokument slouží jako praktická navigace pro zaměstnance a studenty UP: pomáhá rychle posoudit účel použití AI, typ vkládaných dat, provozní režim nástroje a míru lidské kontroly. Není katalogem všech existujících služeb ani návodem na konkrétní komerční produkt.

Pokud potřebujete rychlé rozhodnutí, začněte těmito částmi:

1. **Rychlé minimum pro každého zaměstnance a studenta UP.**
2. **Semafor dat: zelená, žlutá a červená zóna.**
3. **Povolené, podmíněné a zakázané způsoby použití AI**.
4. **Praktické scénáře pro výuku, výzkum a administrativu.**
5. **Co dělat při incidentu nebo pochybnosti.**

Jedna věta, kterou si zapamatovat
Do AI nástroje, u něhož nejste schopni ověřit pravidla pro zpracování dat (všechny online nástroje) nevkládejte nic, co byste bez váhání nezveřejnili na webu.

Preambule

Tento dokument poskytuje praktický rámec pro bezpečné, odpovědné a kontrolovatelné využívání umělé inteligence na Univerzitě Palackého v Olomouci. Jde o doporučený minimální rámec pro celou UP; fakulty a další pracoviště jej mohou podle svých potřeb zpřesnit nebo zpřísnit.

Dokument navazuje na dřívější doporučení UP k využívání AI, na veřejně dostupné dokumenty UP k ochraně osobních údajů, etice a vědecké integritě, na související univerzitní předpisy a na evropský rámec pro používání umělé inteligence, zejména nařízení Evropského parlamentu a Rady (EU) 2024/1689, známé jako AI Act.

Závaznost v konkrétních situacích vzniká zejména prostřednictvím vnitřních předpisů, sylabů, zadání práce, publikačních pravidel, grantových podmínek, smluvních závazků a rozhodnutí příslušných pracovišť. Aktuální verze tohoto doporučení, FAQ a navazující metodické materiály budou zveřejňovány na webovém portálu AI na UP.

Dokument je technologicky i mediálně neutrální. Vztahuje se na chatboty, překladače, generátory obrázků, zvuku a videa, nástroje pro analýzu dat, asistenty v kancelářském softwaru, programovací asistenty, vyhledávací asistenty, AI agenty, AI systémy zabudované do informačních systémů, lokální modely, API služby i specializované výzkumné nebo administrativní nástroje.

Rychlé minimum pro každého zaměstnance a studenta UP

1. **Za výstup odpovídá člověk.** AI může být podpůrný nástroj, nikoli autor, rozhodovatel nebo náhrada odborného úsudku.
2. **Nejdřív posuďte data.** Před použitím AI si určete, zda pracujete s veřejnými, interními, osobními, citlivými, smluvně chráněnými nebo výzkumnými daty.
3. **Interní a neveřejná data patří jen do povoleného režimu.** Nestačí, že nástroj je dostupný, populární nebo zabudovaný v aplikaci. Rozhodující jsou smluvní, bezpečnostní a provozní podmínky.
4. **Do veřejných nástrojů nevkládejte červená data.** Patří sem zejména citlivé osobní údaje, zdravotní údaje, mzdové údaje, neveřejná zkoušková zadání, neveřejné smlouvy, nepublikovaná výzkumná data, hesla, API klíče a přístupové tokeny.
5. **Výstupy AI vždy ověřujte.** AI může halucinovat, vynechávat podstatné informace, reprodukovat zkreslení (bias), vytvářet chybné citace nebo přesvědčivě formulovat nepravdy.
6. **Použití AI přiznávejte.** Řiďte se pravidly předmětu, fakulty, vydavatele, grantové agentury nebo pracoviště.
7. **Syntetický obraz, hlas a video vyžadují zvláštní opatrnost.** Vytváření deepfakes, falešných nahrávek, nevyžádaných podobizen nebo sexuálně explicitních syntetických materiálů je na UP nepřípustné.
8. **Při chybě práci zastavte**. Pokud jste do AI omylem vložili citlivá nebo neveřejná data, nepokračujte ve zpracování, poznamenejte si základní okolnosti a kontaktujte nadřízeného nebo odpovědnou osobu pracoviště. Podrobnosti jsou v části 4.3 a 12.

1. Základní principy

1.1 AI je podpůrný nástroj, nikoli náhrada odpovědnosti

AI může pomáhat s návrhy, strukturací textů, jazykovou úpravou, překlady, sumarizací, tvorbou pracovních variant, programováním, analýzou dat, tvorbou vizuálů, přípravou výuky, rešeršní orientací nebo administrativní podporou. Nemá však nést konečné rozhodnutí v situacích, které mají právní, studijní, pracovněprávní, etický, bezpečnostní, zdravotní nebo vědecký dopad.

Uživatel AI je odpovědný zejména za:

- vhodnost zvoleného nástroje a režimu použití,
- oprávněnost vložení dat,

- věcnou správnost výstupu,
- uvedení použití AI tam, kde je to vyžadováno,
- dodržení pravidel ochrany osobních údajů, autorského práva, mlčenlivosti, akademické integrity a kybernetické bezpečnosti.

1.2 AI nesmí být uváděna jako autor

Generativní AI nemá autorství ani odpovědnost za obsah. V akademické, publikační a administrativní praxi se proto neuvádí jako autor nebo spoluautor. Může být uvedena jako použitý nástroj, zdroj asistence nebo součást metodiky, pokud to vyžadují pravidla vydavatele, grantové agentury, fakulty, předmětu nebo pracoviště.

V případě vědeckých textů je vhodné popsat zejména:

- jaký nástroj nebo model byl použit,
- k jakému účelu byl použit,
- zda ovlivnil pouze jazykovou úpravu, nebo i věcnou strukturu, analýzu, kód, vizualizaci či interpretaci,
- jak byla provedena lidská kontrola výstupu.

1.3 Rozhoduje účel použití, data a režim nástroje

Stejný nástroj může být bezpečný pro práci s veřejným textem a současně nepřijatelný pro práci s osobními údaji, neveřejným rukopisem, zkouškovým zadáním nebo interní smlouvou. Proto tento dokument nepracuje pouze s otázkou „jaký nástroj smím použít“, ale s otázkou „za jakých podmínek a s jakými daty smím nástroj použít“.

1.4 Transparentnost a akademická integrita

Použití AI je třeba přiměřeně uvést tam, kde AI ovlivnila obsah, metodu, výklad, analýzu nebo podobu výstupu. Nepřiznané vědomé využití AI může být etickým prohřeškem, porušením pravidel předmětu, porušením publikačních pravidel nebo porušením pravidel vědecké integrity.

Transparentnost neznamená uvádět každý banální překlep opravený automatickým nástrojem. Znamená však uvést významnou asistenci AI, která měla vliv na obsah, strukturu, argumentaci, překlad, výpočet, vizualizaci, kód, výzkumný postup nebo interpretaci.

1.5 AI gramotnost je minimální podmínkou odpovědného používání

Každý, kdo používá AI při práci nebo studiu na UP, by měl rozumět alespoň základním vlastnostem a limitům nástroje. Minimální AI gramotnost zahrnuje schopnost:

- rozpoznat, že AI může vytvářet nepřesné, smyšlené, zkreslené nebo neúplné výstupy,
- posoudit citlivost vkládaných dat,
- rozlišit mezi veřejným, interním, osobním a vysoce citlivým použitím,

- vědět, kdy je nutná lidská kontrola nebo konzultace,
- rozpoznat rizika syntetických médií, halucinací, biasu, prompt injection, úniku dat a automatizačního zkreslení,
- rozlišit mezi nástrojem pro prvotní návrhy, inspiraci a pomocné zpracování textu a nástrojem vhodným pro rozhodování nebo vědecký výstup.

2. Nejdřív posuďte data: semafor pro práci s AI

Před každým použitím AI si položte otázku: **Co přesně do nástroje vkládám a proč?** Pokud lze cíle dosáhnout bez vložení citlivých nebo neveřejných dat, zvolte bezpečnější variantu: anonymizaci, syntetický příklad, lokální zpracování, interní nástroj, agregovaný popis nebo konzultaci.

Zóna	Typ dat	Kam lze data zadat	Typické příklady
Zelená	Veřejné informace, vlastní nápady a pracovní návrhy bez osobních údajů, interních informací a neveřejného know-how.	Do běžných veřejných nástrojů, pokud neporušujete autorská práva, smluvní mlčenlivost ani pravidla pracoviště.	Veřejný článek, obecná osnova, veřejný abstrakt, obecný e-mail bez osobních údajů, jazyková úprava veřejného textu.
Žlutá	Interní nebo neveřejné pracovní materiály bez vysoké citlivosti; pseudonymizované nebo agregované podklady; podklady s omezeným dopadem při úniku.	Jen do univerzitou povoleného, smluvně ošetřeného nebo jinak bezpečně nastaveného režimu.	Interní metodický text, pracovní prezentace, pseudonymizovaný dataset, anonymizovaný zápis, interní návrh bez citlivých údajů.
Červená	Citlivé osobní údaje, neveřejné zkouškové materiály, neveřejné smlouvy, obchodní tajemství, nepublikovaná výzkumná data, přístupové údaje a bezpečnostní tajemství.	Nezadávat do veřejných AI nástrojů. Řešit lokálně, ve schváleném interním prostředí nebo po konzultaci s prorektorem pro vědu, tvůrčí činnost a transfer znalostí (který zapojí DPO, právní oddělení nebo CVT podle povahy věci).	Rodná čísla, zdravotní údaje, mzdové údaje, seznamy studentů, výsledky zkoušek, hesla, API klíče, access tokeny, patentovatelný nápad, recenzovaný rukopis, data z probíhajícího výzkumu.

Důležité upřesnění: To, že text neobsahuje osobní údaje, ještě neznamená, že jej lze bez dalšího vložit do veřejného nástroje. Může jít o neveřejné know-how, smluvně chráněné informace, autorsky chráněný materiál, neveřejný výzkumný výstup nebo reputačně citlivý obsah.

3. Povolené, podmíněné a zakázané způsoby použití AI

3.1 Povolený režim použití

Povolený režim použití znamená konkrétní kombinaci nástroje, účelu, typu dat, smluvních podmínek, bezpečnostního nastavení a odpovědností. Dokument proto neobsahuje statický seznam AI nástrojů: bezpečné nebo nepřípustné není jméno služby samo o sobě, ale její konkrétní použití v konkrétním režimu.

Povolený režim použití má tyto vlastnosti:

- je určen pro konkrétní typ práce a dat,
- má vyjasněné smluvní podmínky a odpovědnosti poskytovatele,
- je jasné, zda se vstupy a výstupy používají pro trénování nebo zlepšování modelu,
- má popsanou retenci dat a logování,
- má řízení přístupu a přiměřené bezpečnostní prvky,
- u osobních údajů má vyjasněn režim podle GDPR,
- je uvedeno, kdo jej schvaluje, spravuje a aktualizuje.

U veřejných chatbotů a API bez smluvních a bezpečnostních garancí vycházejte z toho, že nejsou určeny pro žlutou ani červenou zónu.

3.2 Praktický checklist pro žlutou zónu

Před použitím AI pro interní nebo neveřejná data musí být jasné alespoň toto:

- data se v továrním nastavení nepoužívají k dalšímu trénování modelu, nebo je tato možnost smluvně a technicky vypnutá (opt-out),
- je známá doba uchování vstupů, výstupů a logů,
- je jasné, kde jsou data ukládána a kdo k nim může přistupovat,
- nástroj umožňuje řídit přístupy a role,
- je vyjasněno, zda je potřeba zpracovatelská smlouva,
- je vyjasněno, zda použití nevyžaduje posouzení vlivu na ochranu osobních údajů,
- existuje postup pro nahlášení incidentu,
- uživatelé jsou poučeni, jak s nástrojem pracovat.

Opt-out nastavení v osobním nebo bezplatném účtu ani pouhá dostupnost AI funkce v e-mailu, prohlížeči či kancelářském softwaru samy o sobě nevytvářejí povolený režim pro interní nebo osobní údaje.

3.3 API, klíče, tokeny a automatizace

Při používání AI přes API vznikají další rizika. Je třeba odlišit token jako jednotku účtování nebo délky textu od API tokenu / API klíče / access tokenu jako přístupového tajného hesla, který patří do červené zóny.

Základní pravidla:

- API klíče, access tokeny a tajné konfigurační hodnoty nikdy nevkládejte do veřejného AI nástroje.
- API klíče neukládejte do zdrojového kódu, veřejných repozitářů, sdílených dokumentů ani promptů.
- Pro výuku používejte testovací účty a demonstrace bez reálných interních dat.
- Pro výzkum a administrativu používejte centrálně schválené účty, řízení přístupu a auditovatelné nastavení.
- U automatizací a AI agentů nastavte limity, lidské schvalování a logování, zejména pokud nástroj může odesílat e-maily, měnit dokumenty, zapisovat do systémů, spouštět skripty nebo přistupovat k datům.
- Při použití API musí být jasné, zda poskytovatel ukládá vstupy a výstupy, jak dlouho je uchovává a zda je využívá k trénování nebo zlepšování modelu.

3.4 AI agenti a napojené nástroje

AI agent je systém, který nejen generuje odpověď, ale může plánovat kroky, používat externí nástroje, číst soubory, vyhledávat, spouštět skripty, pracovat s kalendářem, e-mailem nebo databází. Čím více oprávnění agent má, tím vyšší je riziko.

Pro AI agenty platí:

- přidělujte jen minimální nezbytná oprávnění,
- oddělujte testovací prostředí od produkčního,
- nenechávejte agenta bez kontroly vykonávat nevratné akce,
- udržujte logy kroků a výstupů,
- nepřipojujte agenta k neveřejným datům bez schváleného režimu,
- počítejte s rizikem prompt injection, kdy škodlivý text v dokumentu, webové stránce nebo e-mailu instruuje nástroj k nechtěnému chování.

4. Osobní údaje, GDPR a incidenty

4.1 Základní pravidla pro osobní údaje

Při práci s AI je třeba vycházet z obecných pravidel ochrany osobních údajů. V typických situacích vystupuje UP jako správce osobních údajů. Jednotlivý uživatel odpovídá za to, že do AI vloží jen data, k jejichž použití má oprávnění, a jen v rozsahu nezbytném pro daný účel.

Praktická pravidla:

- vkládejte jen nezbytné minimum dat,
- preferujte anonymizaci nebo agregaci,
- nepoužívejte veřejné nástroje pro citlivé osobní údaje,
- u osobních údajů vždy posuďte, zda jde o povolený režim,
- u nových nebo rozsáhlejších zpracování konzultujte DPO,
- nepoužívejte AI k rozhodování o osobách bez právního a metodického posouzení.

4.2 Příklady incidentů

Za incident může být považováno zejména:

- vložení osobních, studijních, zdravotních, mzdových nebo jiných citlivých dat do veřejného AI nástroje,
- vložení neveřejných smluvních, výzkumných, publikačních nebo zkouškových materiálů do služby bez smluvní ochrany,
- vložení hesla, API klíče, access tokenu nebo jiné tajné hodnoty do promptu,
- vytvoření nebo šíření syntetického obrazu, hlasu nebo videa osoby bez oprávněného účelu a souhlasu,
- použití AI výstupu nebo AI detektoru jako rozhodovacího podkladu bez ověření a odpovídajícího procesu.

4.3 Co dělat při incidentu

Pokud omylem vložíte nevhodná data do AI nebo máte pochybnost, postupujte takto:

1. **Zastavte další zpracování.** Nepokračujte v konverzaci a nevkládejte další data.
2. **Zachovejte základní informace.** Poznamenejte si čas, nástroj, typ vložených dat, zda šlo o veřejný nebo schválený režim, a kdo měl k výstupu přístup.
3. **Nešířte výstup.** Nestahujte a neposílejte vygenerovaný obsah dalším osobám.
4. **Kontaktujte nadřízeného** nebo odpovědnou osobu pracoviště a prorektora pro vědu, tvůrčí činnost a transfer znalostí. Ten provede triáž a podle povahy věci zapojí DPO, CVT, právní oddělení, etickou komisi, vedení součásti nebo jiné odborné pracoviště.
5. **Spolupracujte na nápravě.** Může být nutné zneplatnit token, změnit heslo, požádat poskytovatele o výmaz, vyrozumět správce systému, omezit přístupy nebo posoudit ohlašovací povinnost.

5. Etika, práva osob a syntetická média

5.1 Etika není doplněk, ale základní podmínka

AI může ovlivňovat důvěru, reputaci, akademickou integritu, vztahy mezi vyučujícími a studenty, férovost hodnocení i bezpečnost jednotlivců. Proto musí být její použití přiměřené, transparentní, spravedlivé a respektující práva osob.

Před použitím AI si položte tři otázky:

1. Je použití nástroje férové vůči osobám, kterých se týká?
2. Je přiměřené účelu a riziku?
3. Dokážu použití AI vysvětlit studentovi, kolegovi, účastníkovi výzkumu, nadřízenému, kontrolnímu orgánu nebo veřejnosti?

5.2 Deepfakes, deep nudes, hlasové klony a podvržený obsah

Na UP je nepřípustné používat AI k vytváření nebo šíření obsahu, který bez legitimního důvodu a souhlasu napodobuje konkrétní osobu způsobem, který může poškodit její důstojnost, soukromí, pověst, bezpečí nebo práva.

Zakázáno nebo nepřípustné je zejména:

- vytváření sexuálně explicitních syntetických materiálů zobrazujících reálné osoby,
- vytváření falešných hlasových nahrávek, videí nebo fotografií reálných osob bez legitimního účelu a souhlasu,
- vytváření podvržených důkazů, záznamů, podpisů, obrazových nebo zvukových materiálů,
- šíření syntetických médií, která mohou vyvolat mylný dojem, že osoba skutečně něco řekla nebo udělala,
- použití syntetických médií k šikaně, vydírání, dezinformacím, poškození reputace nebo manipulaci.

Výjimkou mohou být jasně označené vzdělávací, výzkumné, bezpečnostní nebo osvětové ukázky, pokud jsou přiměřené, právně a eticky posouzené, používají syntetické nebo souhlasem ošetřené materiály a minimalizují riziko zneužití.

5.3 Obraz, zvuk, video a grafické výstupy

Pravidla pro AI se nevztahují jen na text. U obrázků, grafů, prezentací, hlasu, hudby, videa, 3D výstupů, kódu a datasetů vždy posuzujte zejména autentičnost, práva osob, licenční omezení, vhodnost zveřejnění a potřebu označení jako AI generovaný nebo AI asistovaný obsah.

5.4 Autorská práva a licenční omezení

Do AI nástrojů nevkládejte cizí autorsky chráněné texty, fotografie, databáze, nahrávky, učebnice, skripta, články nebo jiná díla v rozsahu, který by odporoval licenci, smlouvě,

vydavatelským podmínkám nebo zákonným výjimkám. To platí i tehdy, pokud je materiál snadno dostupný online.

AI výstup nemusí být právně bezproblémový jen proto, že je vygenerovaný AI nástrojem. Před publikací nebo použitím ve výuce, výzkumu či propagaci je třeba posoudit zejména původ vstupů, podobnost s existujícími díly, práva osob, licenci nástroje a účel použití.

6. Rizikové použití AI na univerzitě

6.1 Zakázané nebo vysoce rizikové oblasti

Bez předchozího právního, etického, bezpečnostního a metodického posouzení nepoužívejte AI k:

- určování přístupu ke studiu nebo zařazování osob do vzdělávacích programů,
- automatizovanému hodnocení studijních výsledků, pokud výstup ovlivňuje průběh vzdělávání nebo práva studenta,
- monitorování a detekci zakázaného chování studentů při testech,
- náboru, výběru, hodnocení, povyšování nebo ukončování pracovního vztahu,
- monitorování výkonu zaměstnanců nebo studentů,
- rozpoznávání emocí ve vzdělávacím nebo pracovním prostředí,
- biometrické identifikaci, kategorizaci nebo profilování,
- rozhodování o právech, povinnostech nebo významných zájmech jednotlivců.

Použití AI v uvedených oblastech vyžaduje posouzení účelu, právního základu, proporcionality, lidského dohledu, dokumentace, bezpečnosti, transparentnosti a možnosti odvolání nebo nápravy.

6.2 Lidský dohled a možnost nepoužít výstup

V rizikovějších situacích musí být jasné, kdo odpovídá za rozhodnutí, jak se výstup AI ověřuje a jak lze výstup nepoužít, opravit nebo zvrátit. AI výstup nesmí být používán jako neviditelný autoritativní výrok, zejména pokud se týká studenta, uchazeče, zaměstnance, účastníka výzkumu nebo jiné identifikovatelné osoby.

7. AI ve výuce

7.1 Základní pravidlo pro vyučující

Vyučující má právo a povinnost určit, jak je AI v daném předmětu, úkolu nebo zkoušce povolena, omezena nebo zakázána. Pravidla musí být studentům sdělena srozumitelně a včas. Nejvhodnější je uvádět pravidla přímo v zadání konkrétní aktivity, nikoli zatěžovat sylabus rozsáhlým univerzálním textem.

Do sylabu stačí stručné rámcové ustanovení, například:

„Používání AI se řídí pravidly uvedenými u jednotlivých úkolů a zkoušek. Pokud pravidla nejsou uvedena, smí student použít AI pouze jako podpůrný nástroj pro jazykovou, technickou nebo organizační pomoc; nesmí vydávat AI generovaný obsah za vlastní práci a musí vědomé použití AI přiznat."

Podrobnější pravidla mají být uvedena v zadání seminární práce, projektu, testu, laboratorního protokolu, prezentace nebo zkoušky.

7.2 Pětistupňový model použití AI v konkrétní aktivitě

Pro přehlednost lze u jednotlivých aktivit použít pětistupňový model. Doporučuje se používat jej **na úrovni konkrétního úkolu**, nikoli mechanicky pro celý předmět.

Úroveň	Režim	Vhodné použití
0 – Bez AI	AI není povolena.	Test paměťových znalostí, vlastní argumentace bez pomůcek, kontrolní výkon, kde má být ověřena individuální kompetence.
1 – Technická a jazyková pomoc	AI může pomoci s pravopisem, stylistikou, formátováním nebo překladem, ale nesmí měnit obsahovou podstatu.	Jazyková úprava vlastního textu, kontrola srozumitelnosti, překlepů a formátu.
2 – Brainstorming a struktura	AI může pomoci s nápady, osnovou, otázkami nebo variantami, finální obsah vytváří student.	Návrh osnovy, generování protiargumentů, příprava otázek ke studiu.
3 – Asistovaná tvorba s přiznáním	AI může vytvořit pracovní části textu, kódu, vizualizace nebo analýzy, student je musí zásadně přepracovat, ověřit a přiznat.	Programování, datová analýza, návrhy grafů, první verze abstraktu.
4 – AI jako součást úkolu	Použití AI je předmětem hodnocení; student dokumentuje postup, prompty, ověřování a reflexi limitů.	Kritická evaluace AI, porovnání modelů, audit halucinací, práce s promptem, návrh AI workflow.

7.3 Co mají obsahovat pravidla u konkrétního úkolu

U každého úkolu, kde může AI hrát roli, je vhodné uvést:

- zda je AI povolena, omezena nebo zakázána,
- pro jaké činnosti ji student smí použít,
- zda musí použití AI přiznat,

- jakým způsobem má použití AI popsat,
- zda má přiložit prompty, výstupy nebo reflexi,
- zda se hodnotí proces, výsledek, nebo obojí,
- zda jsou zakázány konkrétní typy pomoci, například generování celého textu, řešení úloh, přepis cizích zdrojů nebo použití neveřejných dat.

7.4 Doporučené formulace do zadání

Varianta A – AI zakázána pro obsahovou část
„Pro obsahové řešení tohoto úkolu není povoleno používat generativní AI. Povolena je pouze základní kontrola překlepů a formátování. Odevzdaný text musí být výsledkem vlastní práce studenta."

Varianta B – AI povolena jako podpůrný nástroj
„AI smíte použít pro brainstorming, osnovu, jazykovou úpravu a kontrolní otázky. Nesmíte odevzdat neupravený AI výstup jako vlastní práci. V závěru uveďte, jaký nástroj jste použili a k čemu."

Varianta C – AI jako součást práce
„Použití AI je součástí zadání. Přiložte stručný popis workflow, vybrané prompty, hlavní výstupy, způsob ověření a reflexi chyb nebo limitů nástroje."

7.5 Detektory AI jsou slabým důkazem

Nástroje pro detekci AI textu mají omezenou spolehlivost, zejména u kratších textů, upravovaných textů, textů v češtině, překladů a textů nerodilých mluvčích. Detektor může být pouze orientačním signálem, nikoli jediným důkazem porušení pravidel.

Při podezření na nepřiznané použití AI je vhodné kombinovat více podkladů:

- zadání a pravidla úkolu,
- historii práce, pracovní verze, poznámky a zdroje,
- ústní obhajobu nebo doplňující otázky,
- porovnání s běžným výkonem studenta,
- posouzení věcných chyb, citací a metodiky,
- komunikaci se studentem a procesní pravidla fakulty.

7.6 Učte studenty odpovědné práci s AI

Smyslem pravidel není pouze AI zakazovat, ale učit studenty rozpoznat, kdy AI pomáhá a kdy škodí. Vhodné výukové aktivity zahrnují:

- porovnání odpovědi AI s odborným zdrojem,
- hledání halucinovaných citací,
- opravu zkresleného nebo jednostranného výstupu,
- reflexi biasu a chyb v češtině,
- tvorbu lepších promptů,

- dokumentaci workflow,
- diskusi o autorských, etických a datových rizicích.

8. AI ve vědě a výzkumu

8.1 AI jako nástroj výzkumného workflow

AI může být užitečná při orientační rešerši, sumarizaci, práci s literaturou, tvorbě kódu, datové analýze, anotaci, vizualizaci, přípravě dotazníků, jazykové úpravě, překladu, tvorbě abstraktů nebo návrhu hypotéz. Je však nutné rozlišovat mezi orientační pomocí a ověřeným vědeckým výstupem.

AI nesmí nahradit:

- odpovědnost autora za data a interpretaci,
- metodologické zdůvodnění,
- kritickou práci se zdroji,
- peer review,
- souhlas účastníků výzkumu,
- pravidla etické komise,
- grantové a publikační podmínky.

8.2 Rešerše a citace

LLM není bibliografická databáze. Může pomoci s orientací v tématu, návrhem klíčových slov nebo vysvětlením pojmů, ale nelze spoléhat na to, že uvedené zdroje existují, nebo že jsou citovány přesně.

Při práci s literaturou:

- ověřujte existenci každé citace v důvěryhodné databázi nebo knihovním systému,
- nekopírujte reference vygenerované AI bez kontroly,
- odlišujte shrnutí zdroje od vlastního hodnocení,
- nevkládejte neveřejné rukopisy nebo recenzní materiály do veřejných nástrojů,
- respektujte licenční podmínky databází, vydavatelů a knihovních zdrojů.

8.3 Výzkumná data

Nepublikovaná výzkumná data, data z klinického, psychologického, pedagogického, sociologického, biologického nebo jiného výzkumu a data získaná od respondentů či účastníků výzkumu patří zpravidla do žluté nebo červené zóny. Před použitím AI je nutné zohlednit informovaný souhlas, etické schválení, plán správy dat, smluvní závazky, grantová pravidla a riziko reidentifikace.

Anonymizace musí být skutečná a přiměřená. Pouhá náhrada jména kódem často znamená jen pseudonymizaci, nikoli anonymizaci.

8.4 Transparentnost ve vědeckých výstupech

Pokud AI významně pomohla s textem, analýzou, kódem, vizualizací, překladem nebo jinou částí výzkumného procesu, je vhodné použití popsat v části metodiky, poděkování nebo poznámce podle pravidel oboru, vydavatele nebo grantové agentury.

Příklad formulace:

> „Při přípravě jazykové verze textu byl použit nástroj [název nástroje/modelu] pro stylistickou kontrolu a návrhy formulací. Všechny věcné závěry, citace a interpretace byly ověřeny autory."

Příklad pro datovou analýzu:

> „Nástroj [název] byl použit k návrhu části analytického skriptu. Kód byl autory zkontrolován, upraven a validován na testovacích datech."

8.5 Recenzní a důvěrné materiály

Recenzent, editor, člen komise nebo hodnotitel nesmí vkládat neveřejný rukopis, grantovou žádost, habilitační materiál, osobní spis, neveřejný posudek nebo jiný důvěrný materiál do veřejného AI nástroje. Použití AI v těchto procesech je možné jen tehdy, pokud to výslovně umožňují pravidla daného procesu a existuje bezpečný režim zpracování.

9. AI v administrativě a podpůrných činnostech

9.1 Běžné administrativní použití

AI může pomoci s návrhem struktury e-mailu, převodem poznámek do zápisu, přípravou osnovy dokumentu, jazykovou úpravou veřejného textu, návrhem prezentace, sumarizací veřejných podkladů nebo přípravou variant formulací. V těchto případech je třeba ověřit věcnou správnost a přizpůsobit výstup kontextu UP.

9.2 Interní dokumenty a smlouvy

Interní dokumenty, smlouvy, ekonomické údaje, mzdové údaje, personální agenda, strategické dokumenty a neveřejné zápisy nevkládejte do veřejných AI nástrojů. Pokud má AI pomoci s jejich zpracováním, musí jít o povolený režim a musí být zohledněna povaha dat.

Bez konzultace nepoužívejte AI k:

- právnímu výkladu smlouvy,
- rozhodnutí o pracovněprávním úkonu,
- zpracování personálních podkladů,
- automatickému vyhodnocování uchazečů,
- zpracování stížností, disciplinárních nebo jiných citlivých podání,
- generování odpovědí v situacích s právním dopadem.

9.3 Komunikace jménem UP

AI výstupy určené pro veřejnou komunikaci, média, sociální sítě, web, tiskové zprávy, marketingové texty nebo reprezentaci UP musí projít lidskou kontrolou. Je třeba ověřit věcnou správnost, tón, soulad s komunikační strategií, práva k použitým obrazovým materiálům a riziko reputační újmy.

10. Praktické scénáře

10.1 Veřejný text

Situace: Chci zlepšit stylistiku veřejného textu o konferenci.
Postup: Pokud text neobsahuje interní informace, osobní údaje, neveřejné údaje ani chráněný obsah, lze použít běžný nástroj. Výstup zkontrolujte a upravte.

10.2 Zápis z porady

Situace: Chci vložit zápis z interní porady do AI a požádat o shrnutí.
Postup: Nejprve odstraňte osobní, strategické, smluvní a citlivé informace. Pokud zápis obsahuje interní informace, používejte jen povolený režim pro žlutou zónu. U citlivých informací konzultujte další postup.

10.3 Seznam studentů

Situace: Chci nechat AI vytvořit analýzu podle seznamu studentů a výsledků testu.
Postup: Veřejný AI nástroj nepoužívejte. Jde o osobní údaje a studijní výsledky. Použijte schválený interní postup nebo konzultujte DPO a odpovědné pracoviště.

10.4 Neveřejné zkouškové zadání

Situace: Chci pomocí AI vygenerovat varianty testových otázek z neveřejného zadání.
Postup: Neveřejná zkušková zadání nepatří do veřejných nástrojů. Lze pracovat s obecným popisem učiva nebo s veřejnými vzorovými otázkami, případně s interním povoleným režimem.

10.5 Grantová žádost nebo rukopis

Situace: Chci vložit návrh grantové žádosti nebo článek před odesláním do AI kvůli jazykové kontrole.
Postup: Ověřte, zda nejde o neveřejné výzkumné know-how, osobní údaje, citlivá data nebo smluvní omezení. Veřejný nástroj bez smluvní ochrany nepoužívejte pro důvěrné materiály.

10.6 API klíč v promptu

Situace: Omylem jsem vložil API klíč do chatu s AI.
Postup: Okamžitě přestaňte s nástrojem pracovat, klíč zneplatněte nebo požádejte správce

o jeho zneplatnění, změňte související tajné hodnoty, zaznamenejte okolnosti a kontaktujte CVT.

10.7 Podezření na AI v seminární práci

Situace: Detektor označil seminární práci jako pravděpodobně vytvořenou AI.
Postup: Detektor nepoužívejte jako jediný důkaz. Zkontrolujte zadání a pravidla, požádejte studenta o vysvětlení postupu, ověřte zdroje a věcné chyby, případně využijte ústní obhajobu nebo proces podle pravidel fakulty.

11. Doporučený proces pro nová AI řešení na UP

Před zavedením nového AI řešení pro výuku, výzkum, administrativu nebo podporu je vhodné provést krátké posouzení:

1. **Bezpečnost:** Jak se řeší přístupy, logy, autentizace, šifrování a audit?
2. **Data:** Jaká data budou vkládána a generována?
3. **Kontrola:** Jak se bude ověřovat kvalita výstupů a jak lze výstup opravit nebo nepoužít?
4. **Odpovědnost**: Kdo je procesním vlastníkem a kdo jsou odborní spolugestoři (například DPO, CVT, právní oddělení, etická komise)?
5. **Riziko:** Dotýká se nástroj osob, hodnocení, rozhodování, pracovněprávní agendy, výzkumných dat nebo veřejné komunikace?
6. **Smlouvy:** Jaké jsou podmínky zpracování dat, retence a trénování?
7. **Školení:** Jaké minimální poučení uživatelé potřebují?
8. **Transparentnost:** Jak budou informováni studenti, zaměstnanci, účastníci výzkumu nebo veřejnost?
9. **Účel:** K čemu má být nástroj používán?
10. **Uživatelé:** Kdo s ním bude pracovat?

12. Triáž, odborné konzultace a odpovědnosti

Pokud si nejste jisti nebo řešíte incident, nepokoušejte se problém vyřešit jen dalším dotazem do AI. Kontaktujte nadřízeného nebo odpovědnou osobu pracoviště a prorektora pro vědu, tvůrčí činnost a transfer znalostí. Ten provede triáž a podle povahy věci zapojí odborné pracoviště.

Téma	Postup
Osobní údaje, GDPR, DPIA, incident s osobními údaji	Prorektor pro vědu, tvůrčí činnost a transfer znalostí; DPO.
Smlouvy, licence, právní výklad, odpovědnost	Prorektor pro vědu, tvůrčí činnost a transfer znalostí; právní oddělení.

Téma	Postup
Kybernetická bezpečnost, účty, API klíče, přístupy, technické nastavení	CVT nebo příslušný správce systému; u bezpečnostního incidentu postupujte podle pravidel informační bezpečnosti.
Akademická integrita, pravidla hodnocení, studijní agenda	Garant předmětu, vedoucí pracoviště, studijní oddělení nebo fakultní etická komise.
Etika výzkumu, účastníci výzkumu, citlivé výzkumné projekty	Etická komise nebo odpovědné pracoviště.
Veřejná komunikace, média, vizuály, reprezentace UP	Oddělení komunikace nebo pověřené pracoviště.

13. Praktický slovníček

AI agent – systém, který může na základě cíle plánovat kroky, používat nástroje a provádět akce, například vyhledávat, číst soubory, psát e-maily nebo spouštět skripty.

AI gramotnost – schopnost rozumět základním vlastnostem, limitům, rizikům a vhodným způsobům použití AI.

AI halucinace – situace, kdy AI vytvoří nepravdivý, nepřesný nebo smyšlený výstup, často formulovaný velmi přesvědčivě.

Anonymizace – nevratné odstranění vazby na konkrétní osobu; takto upravená data už nejsou osobními údaji. Pouhé nahrazení jména kódem obvykle nestačí.

API – rozhraní, přes které může software komunikovat s jinou službou, například s AI modelem.

API klíč / access token – neveřejný přístupový údaj umožňující využívat službu nebo účet. Patří do červené zóny podobně jako heslo.

Autonomní rozhodování – rozhodování, při němž systém vytváří výstup s dopadem na osobu bez odpovídajícího lidského posouzení.

Bias – systematické zkreslení ve vstupech, datech, modelu, interpretaci nebo použití výstupu.

Deepfake – syntetický nebo upravený obrazový, zvukový či video obsah, který vytváří dojem, že konkrétní osoba řekla nebo udělala něco, co ve skutečnosti neřekla nebo neudělala.

Deep nudes – syntetické sexuálně explicitní zobrazení osoby, zpravidla vytvořené bez jejího souhlasu. V univerzitním prostředí je takové použití nepřípustné.

DPA / zpracovatelská smlouva – smluvní ujednání mezi správcem a zpracovatelem osobních údajů.

DPIA / posouzení vlivu na ochranu osobních údajů – posouzení rizik plánovaného zpracování, pokud může zasáhnout do práv a svobod osob.

Embedding – číselná reprezentace textu, obrázku nebo jiného obsahu, používaná například pro vyhledávání podobnosti nebo RAG.

Generativní AI – AI systém vytvářející nový obsah, například text, obrázek, zvuk, video, kód, tabulku nebo návrh řešení.

High-risk AI system / vysoce rizikový AI systém – AI systém spadající do rizikovějších oblastí, například vzdělávání, zaměstnávání, biometrie nebo významné rozhodování o osobách, kde právní rámec vyžaduje zvláštní opatření.

Human in the loop – nastavení, kdy člověk výstup AI kontroluje a nese odpovědnost za jeho použití.

LLM – velký jazykový model, tedy typ AI modelu určený primárně pro práci s jazykem.

Lokální model – AI model provozovaný na vlastním zařízení nebo v interní infrastruktuře; může snížit některá datová rizika, ale sám o sobě neřeší právní, bezpečnostní a kvalitativní požadavky.

No-training režim – nastavení nebo smluvní podmínka, podle níž poskytovatel nepoužívá vstupy a výstupy uživatele k dalšímu trénování modelu.

Opt-out – nastavení, které omezuje využití dat pro zlepšování služby. Samo o sobě nenahrazuje smluvní a bezpečnostní garance.

Prompt – zadání, instrukce nebo kontext vložený do AI nástroje.

Prompt injection – útok nebo nechtěný jev, kdy text v dokumentu, e-mailu, webové stránce nebo jiném vstupu instruuje AI k chování, které uživatel nezamýšlel.

Pseudonymizace – nahrazení přímých identifikátorů kódem nebo zástupným údajem. Data mohou být stále osobními údaji.

RAG / retrieval-augmented generation – postup, kdy AI odpovídá s využitím vyhledaných dokumentů nebo databáze. Kvalita závisí na kvalitě zdrojů, oprávnění k nim a správném nastavení.

Retence dat – doba a způsob uchování vstupů, výstupů a logů poskytovatelem nebo provozovatelem.

Schválený / povolený režim použití – konkrétní kombinace nástroje, účelu, dat, smluvních podmínek, bezpečnostního nastavení a odpovědností, kterou univerzita nebo příslušné pracoviště povolilo.

Správce osobních údajů – subjekt, který určuje účel a prostředky zpracování osobních údajů; v typických pracovních situacích na UP jím bývá univerzita.

Syntetická média – obrazový, zvukový, video nebo jiný mediální obsah vytvořený nebo zásadně upravený AI.

Token jako jednotka modelu – technická jednotka zpracovávaného textu, přibližně část slova nebo slovo; používá se pro omezení délky vstupu a výstupu nebo účtování služby.

Triáž incidentu – úvodní posouzení oznámeného nebo zjištěného neoprávněného použití AI za účelem určení jeho závažnosti, naléhavosti a příslušného postupu řešení (zda se jedná o drobné pochybení, akademický delikt, bezpečnostní problém, porušení ochrany dat nebo závažný etický/procesní incident).

Veřejný AI nástroj – služba dostupná bez zvláštní smluvní ochrany nebo univerzitního schválení; nehodí se pro neveřejná a citlivá data.

Zero Data Retention – režim, ve kterém poskytovatel obsah po zpracování neuchovává nebo jej uchovává jen minimálně a technicky vymezeně.

Zpracovatel osobních údajů – externí subjekt, který zpracovává osobní údaje pro správce a podle jeho pokynů.

Při práci na tomto dokumentu byl použit GPT-5.5 Thinking v režimu plné spolupráce pro zapracování připomínek aktivních účastníků ankety. Prorektor pro vědu, tvůrčí činnost a transfer znalostí Drábek děkuje za spolupráci kolegyním a kolegům (podle abecedy, bez titulů): Cahová, Černík, Dvořáček, Fürst, Hamuľáková, Hulicius, Chamrád, Kopecký, Kryštof, Laštovička, Látal, Mašát, Mazalová, Nétek, Olšan, Otřísal, Petr, Petřík, Šindlerová, Šubová, Tomášek, Tomášková, Vodák, Voráč, Walek, Změlík.