Obecný vzor vnitřního předpisu k používání AI jako pracovního nástroje v organizaci

Vnitřní směrnice č. [XX]/[Rok]

o používání nástrojů umělé inteligence (AI) v [Název organizace]

1. Úvodní ustanovení (předmět a účel)

1. Tato směrnice stanoví pravidla pro bezpečné, odpovědné a transparentní používání nástrojů umělé inteligence (AI) při plnění služebních/pracovních úkolů zaměstnanců v [Název organizace]. Má podporovat bezpečné a účelné využití AI.
2. Směrnice má zajistit zejména:
    - soulad s právními předpisy a vnitřními pravidly[1],
    - ochranu dat a informací,
    - lidskou kontrolu výstupů a odpovědnost zaměstnanců,
    - používání pouze schválených/povolených AI nástrojů.
3. Směrnice je obecný rámec. Konkrétní seznam nástrojů, datové kategorie, procesy, případy využití a odpovědné role doplňuje [organizace] v přílohách.

2. Rozsah působnosti

1. Směrnice je závazná pro:
    - zaměstnance ve služebním/pracovním poměru,
    - externí spolupracovníky, dodavatele a jejich subdodavatele, včetně poskytovatelů SaaS a AI služeb, administrátorů a dalších osob jednajících pro [organizaci] nebo jejím jménem, a to v rozsahu jejich smluvních, provozních nebo jiných obdobných povinností, pokud přicházejí do styku s informacemi [organizace]; povinnost dodržovat tuto směrnici musí být současně odpovídajícím způsobem promítnuta do smluvních vztahů, zpracovatelských smluv (DPA), bezpečnostních příloh a souvisejících provozních pravidel.
2. Směrnice se vztahuje na používání AI:
    - na služebních/pracovních zařízeních,

[1] *Tato směrnice je zpracována v souladu zejména s relevantními ustanoveními nařízení Evropského parlamentu a Rady (EU) o umělé inteligenci (AI Act), nařízení (EU) 2016/679 (GDPR), zákona o kybernetické bezpečnosti a jeho prováděcích předpisů, včetně transpozice směrnice NIS2, a dále zohledňuje interní pravidla bezpečnostní klasifikace informací.*

- v ICT prostředí organizace,
- při výkonu služby/práce, i když je nástroj dostupný přes web (cloud),
- při práci na dálku,
- při použití soukromého zařízení pro služební/pracovní účely, pokud to [organizace] připouští.

3. Vymezení pojmů

Pro účely této směrnice se rozumí:

1. AI / AI nástroj je jakýkoliv strojový systém/software/aplikace/webová služba/integrovaná funkce/služba poskytovaná prostřednictvím API, která je navržena tak, aby s určitou mírou autonomie na základě pokynů, dat nebo jiných vstupů odvozovala, jak vytvářet výstupy, zejména predikce, obsah, klasifikace, doporučení, rozhodnutí nebo jiné výsledky, které mohou ovlivnit virtuální nebo fyzické prostředí. Za AI / AI nástroj se považují také integrované AI funkce v kancelářských balících, vyhledávačích, prohlížečových rozšířeních, SaaS aplikacích, agentních nástrojích a obdobných digitálních službách.
2. chválené/povolené použití AI nástroje je pouze takové použití AI nástroje, které bylo posouzeno a povoleno podle [čl. 10] pro konkrétní kombinaci alespoň těchto parametrů: nástroj, případ užití, kategorie dat, uživatelská role, prostředí použití, režim logování a způsob lidské kontroly. Schválení se nevztahuje na AI nástroj obecně, ale pouze na schválený rozsah jeho použití. Schválená použití jsou uvedena [v Příloze č. XY].
3. Volně dostupný AI nástroj je veřejně dostupná služba mimo řízené prostředí [organizace] (typicky bez smluvně a technicky ošetřených záruk).
4. Chráněné informace jsou zejména osobní údaje, údaje ze správních řízení, obchodní tajemství, bezpečnostní informace a další zákonem chráněné údaje. Chráněné mohou být i interní informace [organizace], které nejsou určeny ke zveřejnění. [konkrétní kategorizaci doplní organizace v Příloze č. XY].
5. AI-asistovaný výstup je výstup nebo jeho část, který byl vytvořen, upraven nebo významně ovlivněn s využitím nástroje AI a podléhá kontrole odpovědným zaměstnancem.
6. Citlivý případ užití je takové využití nástroje AI, které se týká chráněných informací, osobních údajů, práv nebo oprávněných zájmů osob anebo může mít významný dopad na činnost [organizace], na rozhodování v jejích agendách či její důvěryhodnost.

4. Základní zásady používání AI

1. AI je podpůrný nástroj. Rozhodování a odpovědnost zůstává na zaměstnanci/organizaci.
2. AI nesmí nahrazovat roli rozhodující úřední osobu, správní uvážení, principy hodnocení důkazů ani odpovědnost orgánu veřejné správy.
3. Použití AI musí být přezkoumatelné.
4. AI se použije jen tehdy, když:
    - je to účelné a přiměřené,
    - jsou známy limity nástroje a rizika (halucinace, zkreslení, stereotypy, diskriminace).
5. Vstupy i výstupy se posuzují uvážlivě a věcně.
6. AI se použije v souladu s právními předpisy, interními pravidly (ISMS/bezpečnost, spisová služba, GDPR apod.) a etickými principy.
7. Jsou preferována důvěryhodná řešení s důrazem na lidský dohled, technickou spolehlivost, ochranu soukromí, transparentnost, nediskriminaci a odpovědnost.
8. Míra kontroly a požadavky na schválení se odvíjejí od rizikovosti použití, dopadu na práva osob, povahy dat, možnosti vzniku právních účinků zveřejnění výstupů a reputačního dopadu.

5. Povolené způsoby využití AI

[Organizace může vymezit i doporučené scénáře]

1. Typicky povolené činnosti (příklady):
    - jazykové a stylistické úpravy interních textů,
    - návrhy osnov, tezí, shrnutí,
    - pomocné analýzy a nápady, které jsou následně ověřeny,
    - tvorba konceptů prezentací či podkladů (bez vkládání chráněných informací).
2. U každého výstupu, který AI ovlivnila, platí čl. 8 (ověření) a případně čl. 9 (deklarace).

6. Zakázané nebo omezené způsoby využití AI

1. Bez výjimky je zakázáno:
    - zadávat chráněné informace (zejm. osobní údaje, údaje ze správních řízení, obchodní tajemství apod.) do volně dostupných AI nástrojů, tedy

do nástrojů, které nejsou schváleny [organizací], anebo jsou používány mimo schválené prostředí [organizací], včetně jejich využívání prostřednictvím soukromých účtů.

2. Dále je zakázáno/omezeno [doplní organizace]:
    - používat AI pro automatické generování závazných stanovisek, rozhodnutí bez adekvátního lidského posouzení,
    - používat neschválené nástroje, soukromé účty, cloudové služby, neprověřené pluginy, mobilní aplikace i nepřímé vkládání dat prostřednictvím integrovaných AI funkcí.
    - přímé přebírání výstupů AI do oficiálních dokumentů bez kontroly či adekvátního lidského zásahu.

7. Práce s daty a informacemi

1. Vždy se uplatní [doplní organizace]:
    - minimalizace dat (jen to, co je nutné),
    - anonymizace/pseudonymizace, pokud lze,
    - respekt k interní klasifikaci informací.
2. U schválených nástrojů se stanoví [doplní organizace]:
    - jaké datové kategorie smí do nástroje,
    - zda se data používají pro trénování/modelové učení (a jak je to smluvně ošetřené, jaké jsou možnosti omezení),
    - dále se eviduje kde se data ukládají, jak dlouho, jak se zpracovávají, kdo k nim má přístup, jak se k datům přistupuje, jaký je management incidentů a režim ukončení v rámci životního cyklu AI,
    - jaká je preference řízených / on-premise řešení pro citlivé případy
3. V případě nejistoty, zda je vstup „bezpečný“, se postupuje z výchozího bezpečného režimu „data se do AI nesmí zadat“ a dále podle čl. 11 (konzultace/eskalace).

8. Kontrola a ověřování výstupů AI

1. Výstupy AI mohou být chybné, zavádějící nebo zkreslené; informace získané prostřednictvím AI je nutné ověřit.
2. Minimální standard ověření [doporučená formulace]:
    - faktická kontrola (zdroje, údaje, citace),
    - kontrola souladu s právem a interními pravidly,

- kontrola tónu, srozumitelnosti a nediskriminace,
- u určených výstupů validace další osobou dle interních pravidel.

3. Pokud AI generuje odkazy či zdroje, ověřuje se, že existují a odpovídají obsahu.

9. Transparentnost a deklarace využití AI

1. Zaměstnanec má povinnost přiměřeně deklarovat využití AI v písemných výstupech dle pravidel [organizace] (např. formulace typu „Při zpracování tohoto materiálu byl využit nástroj …“)
2. [Organizace doplní]:
   - kdy je deklarace povinná (interně / vůči veřejnosti),
   - doporučené znění [Příloha č. XY].

[10. Schvalování a pořizování AI nástrojů (povolování)]

1. Zaměstnanci smí používat pouze AI nástroje uvedené v [Příloze č. XY (Schválené nástroje)]. Seznam schválených nástrojů je pravidelně revidován a aktualizován AI officerem (čl. 11).
2. Pokud organizační útvar potřebuje nový AI nástroj, podá žádost o schválení [Příloha č. XY]. Součástí žádosti je zejména analýza potřeb a cílů, účelu, očekávání a přínosů, volba nástroje, smluvní režim, zdroje dat, odhad nákladů, zajištění aktuálnosti/úplnosti dat a forma uveřejňování výstupů, určení vlastníka případu použití.
3. Žadatel popíše také bezpečnostní opatření (ochrana před únikem, šifrování, řízení přístupů apod.) a návrh ukončení či omezení použití.
4. Posouzení provádí [role doplní organizace]:
   - AI officer
   - útvar ICT (integrace, vhodnost nástroje),
   - manažer kybernetické bezpečnosti / bezpečnostní role (rizika, zabezpečení, práce s daty),
   - pověřenec pro ochranu osobních údajů (GDPR dopady),
   - právní útvar
   - [relevantní aktéři organizace]
5. Výsledek posouzení:
   - schválení / podmíněné schválení / zamítnutí s odůvodněním,
   - nastavení podmínek schválení, provozu a monitoringu.

6. [Organizace] může upravit postupy a kritéria pro pilotní projekty či provozní nasazení AI nástrojů.

11. Role, odpovědnosti a eskalace

1. Každý zaměstnanec odpovídá za svou práci bez ohledu na to, zda použil AI.
2. [Organizace návazně na svůj organizační řád] odpovídá za nastavení schváleného prostředí, školení, dostupnost bezpečných nástrojů, kontrolní mechanismy a vymahatelnost pravidel.
3. Vedoucí zaměstnanec:
    - dbá na dodržování směrnice ve svém útvaru,
    - určuje, které typy výstupů vyžadují zvýšenou kontrolu.
4. AI sponzor:
    - zajišťuje strategické zastřešení využívání AI v úřadu, dává této agendě legitimitu, určuje její směr a podporuje adopci AI na úrovni vedení.
    - podporuje přijetí interních pravidel pro využívání AI a vytváří podmínky pro jejich prosazování v rámci organizace.
    - rozhoduje o strategickém směřování v oblasti AI, zejména o prioritách, celkovém rámci zavádění a zajištění potřebných zdrojů a financování.
    - sleduje strategický dopad využívání AI a ve spolupráci s nejvyšším vedením i vyhodnocuje přínosy, potřeby a další rozvoj této agendy.
5. AI officer
    - řídí zavádění AI v úřadu po exekutivní a koordinační stránce a odpovídá za implementaci pravidel, procesů a rámce pro její využívání.
    - koordinuje spolupráci relevantních útvarů, zejména v oblastech IT, HR, legislativy, bezpečnosti a dat, a propojuje strategické zadání vedení s praktickou realizací. Řídí a koordinuje činnost AI ambasadorů
    - schvaluje nebo koordinuje schvalování konkrétních nástrojů AI, případů užití a limitů jejich používání v organizaci.
    - odpovídá za řízení adopce AI, sledování bariér, přínosů a potřeb zaměstnanců, včetně koordinace vzdělávání a průběžného vyhodnocování dopadů.

6. AI ambasador:
    - podporuje bezpečné a smysluplné využívání AI v každodenní praxi zaměstnanců a pomáhá převádět schválená pravidla do srozumitelného a použitelného postupu.
    - šíří osvětu, sdílí zkušenosti a příklady dobré praxe, organizuje podporu a pomáhá kolegům zorientovat se ve schválených možnostech využívání AI.
    - sbírá podněty, potřeby a zpětnou vazbu z praxe, pomáhá identifikovat vhodné případy užití a předává tyto informace AI officerovi.
    - podporuje adopci schválených nástrojů AI formou kolegiální podpory a přispívá ke zlepšování školení, metodik a uživatelské podpory.
7. Vlastník případu využití:
    - odpovídá za konkrétní nasazení AI v dané agendě nebo procesu a jeho kontinuální vyhodnocování,
    - vymezuje účel, očekávaný přínos, vstupy a hranice konkrétního případu využití a odpovídá za jeho věcnou správnost,
    - zajišťuje, aby využití AI bylo přiměřené riziku, bylo testováno a mělo nastavenou lidskou kontrolu výstupů,
    - sleduje a vyhodnocuje přínosy, zkušenosti a navrhuje úpravy, rozšíření či ukončení daného využití.
8. ICT / bezpečnost:
    - ve spolupráci s AI officerem posuzuje AI nástroje z pohledu ICT a bezpečnosti,
    - ve spolupráci s AI officerem stanovuje a průběžně aktualizuje pravidla, stanovuje technická a organizační opatření,
    - stanovuje podmínky pro bezpečnost, integraci, práci s daty a používání on-premise či cloudových řešení
    - zajišťuje průběžný monitoring, reporting vedení
    - řeší incidenty, nápravná opatření a zlepšování.
9. Pověřenec pro ochranu osobních údajů:
    - dohlíží na soulad využívání AI s ochranou osobních údajů,
    - posuzuje, zda a jak lze zpracovat osobní údaje, vč. požadavků na minimalizaci, anonymizaci a právní titul,
    - doporučuje ochranná opatření,

- Poskytuje metodickou podporu při nastavování transparentnosti, práv subjektů údajů a souladu s GDPR a souvisejícími předpisy.

10. Eskalace:
    - pokud vznikne pochybnost o práci s daty, bezpečnosti nebo právním či etickém dopadu, zaměstnanec konzultuje [kontakt/útvar].
    - V případě rozdílnosti stanovisek věc posuzuje [kontakt/útvar].

12. Vzdělávání, osvěta a sdílení zkušeností

1. [Organizace] zajistí základní proškolení všech zaměstnanců, kteří při výkonu práce používají nebo mohou používat nástroje AI, a to v rozsahu odpovídajícím platné legislativě, pravidlům této směrnice a rizikům spojeným s využíváním AI nástrojů.
2. Vedoucím zaměstnancům a určeným zaměstnancům zapojeným do pořizování, správy, posuzování nebo intenzivnějšího využívání nástrojů AI zajistí [organizace] rozšířené vzdělávání. Rozšířené vzdělávání zajistí [organizace] specificky také AI officerovi a AI ambasadorům.
3. Obsah a rozsah vzdělávání se přizpůsobuje roli zaměstnance, povaze jeho činností a míře rizika spojené s konkrétním využitím AI.
4. [Organizace] podporuje průběžnou osvětu, zejména formou metodických doporučení, interních sdělení, krátkých školení nebo jiných vhodných forem sdílení základních pravidel a novinek.
5. [Organizace] současně podporuje sdílení zkušeností a příkladů dobré praxe mezi útvary, aby bylo využívání AI bezpečné, účelné a v souladu s právními a interními požadavky.

13. Evidence, monitoring, incidenty, rozvoj

1. [Organizace stanoví], jak se eviduje:
    - seznam povolených nástrojů,
    - schválené účely použití,
    - přístupy a oprávnění, využití licencí
    - školení.
2. Odpovědné role průběžně sledují vývoj a reagují aktualizací politik, předpisů, školením, řízením rizik apod.
3. Incidenty (únik dat, zneužití účtu, podezřelé chování nástroje či generování nežádoucích, nevhodných výstupů) se hlásí podle [interní směrnice k incidentům] [kontakt/útvar].

4. Odpovědný útvar eviduje zjištěné incidenty, způsoby jejich řešení a další doporučení.

14. Kontrola dodržování a následky porušení

1. Kontrolu provádí [útvar/role].
2. Porušení směrnice se řeší dle [služebních/ pracovněprávních předpisů] a interních pravidel.
3. Uplatní se i nápravné kroky, poučení a úprava procesu, pokud jde o systémový problém.

15. Závěrečná ustanovení

4. Účinnost od: [datum]
5. Revize směrnice [minimálně 1× ročně nebo při významné změně technologií/legislativy].
6. Gestor: [útvar/jméno]
7. Schvaluje: [funkce]
8. Přílohy jsou součástí směrnice.

Doporučené přílohy

- **Příloha XY:** Seznam schválených AI nástrojů, účely jejich použití a podmínky jejich použití.
- **Příloha XY:** Klasifikace dat a informací.
- **Příloha XY:** Vzorové formulace deklarace využití AI (interní/externí).
- **Příloha XY:** Formulář žádosti o schválení AI nástroje
- **Příloha XY:** Katalog případů užití AI
- **Příloha XY:** Klasifikační matice rizik
- **Příloha XY:** Matice odpovědností a rolí