Výklad k vybraným ustanovením Vzoru interního předpisu

Tento výkladový komentář slouží jako podpůrný metodický materiál k vzoru vnitřní směrnice. Jeho účelem je přiblížit smysl vybraných ustanovení, upozornit na související otázky, které je vhodné při jejich aplikaci zohlednit, a nabídnout doporučení k jejich praktickému nastavení v podmínkách konkrétního úřadu.

Výkladový komentář není závazným materiálem a nepředstavuje jednotný nebo vyčerpávající návod pro všechny orgány veřejné správy. Rovněž samotný vzor směrnice je koncipován jako doporučující rámec, který je třeba přizpůsobit zejména velikosti a působnosti úřadu, povaze vykonávaných agend, používaným informačním systémům, úrovni řízení rizik, bezpečnostním požadavkům a personálním či organizačním kapacitám.

Při využití vzoru směrnice i tohoto výkladového komentáře je proto nezbytné posoudit vlastní potřeby a podmínky konkrétní organizace tak, aby výsledná úprava byla přiměřená, srozumitelná, prakticky proveditelná a zároveň odpovídala relevantním právním a bezpečnostním požadavkům.

Čl. 1 *Úvodní ustanovení*

Toto ustanovení vymezuje základní účel směrnice: nejde o zákaz AI, ale o nastavení podmínek pro její bezpečné a odpovědné používání při výkonu práce. Je vhodné zdůraznit, že směrnice má současně podporovat využití AI tam, kde je to přínosné, a předcházet právním, bezpečnostním a reputačním rizikům. Úřad by si měl upřesnit, jaké cíle od využívání AI očekává a ve kterých agendách má AI pouze podpůrnou roli.

Samotná směrnice vytváří jen rámec a její praktická použitelnost závisí na doplnění konkrétních příloh a interních procesů. Smyslem je umožnit jednotný základ pro různé úřady, nikoli předepsat jeden univerzální model. Úřad by proto neměl ponechat přílohy jen formálně, ale doplnit je podle své agendy, technického prostředí a úrovně rizik.

Čl. 2, odst. 2 *Rozsah působnosti*

Pravidla se nevztahují jen na interní zaměstnance, ale i na všechny osoby a subjekty, které jménem organizace pracují s jejími daty nebo využívají AI v souvislosti s její činností. Praktický význam má zejména promítnutí těchto požadavků do smluv, bezpečnostních příloh a provozních pravidel. Úřad by si měl ujasnit, které typy dodavatelských vztahů a externích rolí tímto ustanovením pokrývá.

Použití soukromého zařízení pro služební účely by u AI mělo být povoleno pouze výslovně a za podmínek MDM (Mobile Device Management) /MAM (Mobile Application Management), řízení účtů, zákazu ukládání dat mimo organizaci a zákazu

použití soukromých AI účtů. Jinak vzniká vysoké riziko úniku interních nebo chráněných informací. Použití soukromých zařízení či soukromých účtů nemá být automatické, ale jen výslovně povolené a podmíněné interními pravidly. Úřad by si měl stanovit, zda tento režim vůbec připustí, a pokud ano, za jakých technických a bezpečnostních podmínek.

Čl. 3 odst. 1 *Definice AI/AI nástroje*

Evropská komise vydala výkladové pokyny, které mají pomoci určit, zda konkrétní software nebo funkce do této definice spadá. Dostupné zde: commission_guidelines_on_the_definition_of_an_artificial_intelligence_system_established_by_regulation_eu_20241689_ai_actenglish_nf2skcqfrtjdfggjavcodopcwz4_112455.PDF. Další užitečný výkladový materiál zde: Rules for trustworthy artificial intelligence in the EU | EUR-Lex.

Čl. 3 odst. 2 *Povolené použití AI*

Definice hovoří o schváleném způsobu použití nástroje. Důvod je jednoduchý: AI Act pracuje mimo jiné s pojmem „*zamýšlený účel*“, tedy s tím, k jakému účelu a v jakém kontextu je systém používán, a u používání AI zdůrazňuje také pokyny k použití, lidský dohled, relevanci vstupních dat a uchovávání logů. Schválení proto dává větší smysl vztahovat ke kombinaci nástroj + use case + data + role + prostředí + logování + lidská kontrola, ne jen k samotnému produktu.

Definice takto

- odděluje nástroj od konkrétního způsobu použití – jeden a tentýž nástroj může být přijatelný pro jazykovou či stylistickou podporu, ale nepřijatelný pro práci s citlivými nebo spisovými daty. To odpovídá logice AI Actu.
- zohledňuje lidský dohled a provozní pravidla, protože používání AI má být navázáno na instrukce k použití, lidský dohled, kvalitu vstupních dat a logování.
- je prakticky vymahatelná, protože umožňuje vést evidenci schválení v přehledné podobě (například v příloze nebo registru povolených použití).

Čl. 3 odst. 3 *Volně dostupné nástroje*

Volně dostupným nebo neschváleným AI nástrojem může být i AI funkcionalita ukrytá v jiné službě, například překladač, vyhledávač, prohlížečový plugin, kancelářský doplněk, mobilní aplikace nebo SaaS nástroj, pokud nebyla [organizací] samostatně posouzena a schválena. Rozhodující není název služby, ale to, zda je provozována ve schváleném prostředí a za schválených podmínek.

Čl. 3 odst. 3 *Citlivý případ užití*

Citlivý může být i případ, kdy nejsou použita zvláštní data, ale výstup se promítá do rozhodování nebo veřejné komunikace. Úřad by si měl dopředu stanovit typické příklady citlivých případů užití ve svých agendách.

Čl. 4 odst. 1 a 2 *AI jako podpůrný nástroj*

V podmínkách veřejné správy je důležité zdůraznit, že AI nesmí nahrazovat odpovědnost úřední osoby ani odpovědnost orgánu veřejné správy za výsledek. Úřad by měl zaměstnance vést k tomu, že AI může pomoci připravit podklad, ale nemůže „převzít“ rozhodnutí.

Zákaz míří zejména na situace, kdy by AI byla používána jako faktický rozhodovací mechanismus bez samostatného lidského posouzení. Nepřípustné není jen automatické vydání rozhodnutí, ale i nekritické převzetí závěrů AI do úředního postupu. Úřad by měl zaměstnancům dát příklady, co je ještě podpůrné využití a co už je nepřiměřené nahrazení lidského uvážení, využít k tomu lze mj např. zdroje Evropské komise, dostupné zde: zde: Rules for trustworthy artificial intelligence in the EU | EUR-Lex.

Čl. 4 odst. 3 *Přezkoumatelné použití*

přezkoumatelnost znamená možnost zpětně pochopit, jak byl nástroj použit, jaké vstupy byly zadány, kdo výstup zkontroloval a jak byl použit v dalším procesu. Neznamená to nutně složité technické logování v každém případě, ale přiměřenou dohledatelnost podle rizika použití. Nastavení míry evidence je v rukou úřadu, základní povinnosti podle úrovně rizika nastavuje AI Act.

Čl. 4 odst. 8 *Míra kontroly a požadavky na schválení*

Možná klasifikační matice rizik

Kritérium	Nízké riziko	Střední riziko	Vysoké riziko
Dopad na práva osob	bez dopadu na práva či postavení osob	může nepřímo ovlivnit posouzení, komunikaci nebo pracovní postup vůči osobě	může ovlivnit práva, povinnosti, oprávněné zájmy nebo přístup ke službě / rozhodnutí
Povaha dat	veřejná data, anonymizovaná data, testovací data bez vazby na osoby	interní neveřejná data, běžné osobní údaje, provozní data	zvláštní kategorie osobních údajů, údaje ze správních spisů, citlivá interní data,

			bezpečnostně významné informace
Možnost právních účinků	výstup má pouze podpůrný nebo pomocný charakter	výstup je jedním z podkladů pro lidské rozhodnutí	výstup může přímo nebo fakticky založit, změnit nebo významně ovlivnit rozhodnutí či úřední postup
Zveřejnění výstupu	výstup zůstává interní a je dále upraven člověkem	výstup je sdílen interně nebo navenek po kontrole člověkem	výstup je zveřejněn navenek, použit v oficiální komunikaci nebo předán třetí straně s omezenou či žádnou úpravou
Reputační dopad na organizaci	případná chyba má omezený interní dopad	chyba může vést ke stížnosti, nedorozumění nebo omezenému reputačnímu poškození	chyba může vést k významné reputační újmě, mediálnímu dopadu, ztrátě důvěry nebo právnímu sporu

Jednoduché rozhodovací pravidlo pro zařazení do kategorie:

- Nízké riziko – pokud jsou všechna posuzovaná kritéria v úrovni nízké.
- Střední riziko – pokud je alespoň jedno kritérium ve střední úrovni a žádné není ve vysoké.
- Vysoké riziko – pokud je alespoň jedno kritérium ve vysoké úrovni.

Úroveň rizika	Míra kontroly	Minimální požadavek na schválení
Nízké	základní kontrola uživatelem	bez individuálního schválení, pokud jde o již schválený nástroj a schválený případ užití; uživatel odpovídá za kontrolu výstupu
Střední	povinná lidská kontrola před použitím výstupu	schválení vedoucím útvaru nebo věcným garantem + konzultace s IT/bezpečností nebo správcem AI agendy podle interních pravidel

Vysoké	zesílená lidská kontrola, povinné logování, omezený okruh oprávněných uživatelů	formální schválení určenou odpovědnou rolí / komisí (např. gestor AI, bezpečnost, právní, DPO podle povahy použití) před nasazením

Čl. 5 odst. 1 a 2 *Povolené způsoby použití*

Jde o příklady běžně akceptovatelných případů užití, nikoli o automatické povolení bez dalších podmínek. Rozhodující je vždy i typ použitého nástroje, druh dat a účel využití. Povolené činnosti by měly být navázány na katalog případů užití v úřadu. U každé činnosti má být uvedeno, zda je povolena bez omezení, povolena pouze se schváleným nástrojem, povolena pouze bez neveřejných dat, nebo podléhá individuálnímu schválení.

Povolené použití neznamená automaticky použitelný výstup. I u běžně povolených scénářů musí zaměstnanec zkontrolovat věcnou správnost a případně zvážit, zda je nutné využití AI deklarovat. Úřad by měl sjednotit, jakou úroveň ověření očekává u různých typů výstupů.

Čl. 6 odst. 1 *Zakázané způsoby použití*

V praxi bývá hranice mezi schváleným a neschváleným prostředím nejasná. Je vhodné mít na paměti, že zakázané by mělo být použití nepovolených soukromých účtů, neschválených cloudových služeb, neprověřených pluginů, mobilních aplikací a nepřímé vkládání dat prostřednictvím integrovaných AI funkcí. Zaměstnanec často ani nemusí vnímat, že používá AI funkcionalitu třetí strany. Je vhodné doplnit příklady typických rizikových situací, aby zaměstnanci rozuměli, co vše může představovat nepřípustné jednání.

Čl. 6 odst. 2 *Zakázané způsoby použití*

AI nesmí bez výslovně schváleného režimu vytvářet závazné stanovisko, rozhodnutí, kontrolní závěr, právní posouzení, hodnocení osoby ani podklad, který by nebyl samostatně lidsky ověřen a přezkoumatelný.

Omezení míří nejen na formální rozhodnutí, ale i na podklady a výstupy, které mohou mít faktický dopad na práva osob nebo na činnost úřadu. Smyslem je zabránit tomu, aby lidské ověření bylo jen formální nebo zástupné. Úřad by měl určit, které typy dokumentů a úkonů jsou v tomto ohledu zvlášť citlivé.

Čl. 7 odst. 1, 2 a 3 *Práce s daty a informacemi*

Minimální datový standard pro každé použití AI. Zaměstnanec má vždy nejprve zvažovat, zda je vůbec nutné konkrétní data do nástroje zadávat a zda nelze jejich citlivost snížit. Úřad by měl zaměstnancům přiblížit, jak v praxi rozpoznat, kdy je možné použít anonymizovaná nebo obecnější data místo konkrétních informací.

Použití schváleného nástroje samo o sobě neznamená, že do něj lze vložit jakákoli data. Rozhodující jsou konkrétní podmínky schválení a způsob, jak služba data zpracovává, ukládá a případně dále využívá. Důležité je také myslet na autorská práva ke vkládaným vstupům.

Lze doporučit vést datovou mapu AI služby: kde vzniká vstup, kudy data tečou, kde se ukládají, kdo je správcem/zpracovatelem, kdo jsou subdodavatelé, v jaké jurisdikci jsou data zpracována a zda jsou použita pro další učení modelu.

Čl. 8 odst. 2 *Minimální standard ověřování*

Minimální standard ověření by měl být odstupňován podle typu výstupu. Jiná kontrola postačí u stylistické úpravy interního textu a jiná u právního stanoviska, veřejné komunikace, podkladu pro rozhodnutí nebo materiálu pro vedení. U rizikových výstupů je vhodné postupovat dle klasifikační matice rizik.

Druhá kontrola je vhodná zejména u výstupů s vyšším dopadem – například pro veřejnou komunikaci, právní podklady, rozhodovací materiály nebo výstupy s dopadem na osoby a jejich práva. Nejde o povinnost plošnou, ale o opatření pro rizikovější situace. Úřad by si měl předem určit, které typy výstupů takovou validaci vyžadují.

Čl. 9 odst. 1 *Transparentnost a deklarace využití AI*

Deklarace použití AI by měla rozlišovat drobným technickým či jazykovým využitím od významného obsahového využití AI (primárně viz ustanovení AI Act). Povinnost deklarace lze doporučit stanovit zejména pro výstupy určené pro externí aktéry, veřejně publikované materiály, podklady pro vedení a výstupy s možným dopadem na práva osob.

Smyslem deklarace není zaměstnance nikterak postihovat, ale umožnit přiměřenou transparentnost a důvěru ve výstup. Úřad by si měl ujasnit, kdy je deklarace povinná interně, kdy externě a kde postačí interní evidenční stopa.

Čl. 10 odst. 1, 2, 5 *Schvalování AI nástrojů*

Příloha nepředstavuje jen seznam technologií, ale nástroj řízení rizik a provozních podmínek.

Seznam schválených nástrojů by neměl být statický. Je vhodné zavést časově omezené schválení, pravidelnou revizi, evidenci verzí/modelů, kontrolu změn poskytovatele a povinnost znovuposouzení při změně modelu, funkcionality, smluvních podmínek nebo datových toků.

Schvalování nemá být formální administrativní krok, ale proces, který má ověřit účelnost, rizika a podmínky bezpečného provozu. Smyslem žádosti je popsat nejen nástroj, ale i konkrétní případ použití, data, role a očekávaný přínos.

Výsledek posouzení by neměl být pouze ano/ne, ale měl by obsahovat konkrétní podmínky schválení: povolený účel, zakázané vstupy, povolené role, kontrolní mechanismy, logování, retenční pravidla, požadavky na deklaraci AI, termín revize a odpovědného vlastníka.

Čl. 11 *Role*

Jde o doporučené rozdělení odpovědností, které si každý úřad může přizpůsobit své velikosti a organizační struktuře. Důležité je, aby zůstalo jasné, kdo odpovídá za strategii, kdo za koordinaci, kdo za konkrétní případ použití a kdo za metodickou podporu a další dílčí aspekty problematiky AI v úřadu.

Čl. 11 odst. 5 *AI officer – koordinace schvalování*

U citlivých nebo vysoce rizikových použití lze doporučit schvalovací výbor nebo víceúrovňové schválení zahrnující vlastníka agendy, ICT, bezpečnost, pověřence pro ochranu osobních údajů a právní posouzení.

Čl. 11 odst. 10 *Eskalace*

Možnost konzultace není jen doplňková služba, ale důležitá součást bezpečného používání AI. Smyslem je podpořit zaměstnance, aby řešili nejistotu včas, a ne až ve chvíli, kdy dojde k incidentu nebo chybnému použití nástroje. Úřad by si měl zajistit srozumitelný kontaktní bod a jednoduchý eskalační postup.

Čl. 12 odst. 1 *Vzdělávání*

AI Act ve svém čl. 4 výslovně hovoří o povinnosti zajištění AI gramotnosti. Školení by nemělo být jednorázové a stejné pro všechny, ale průběžné, založené na rolích zaměstnanců, typu práce, kterou vykonává a evidované. Jiný rozsah potřebuje běžný uživatel, vedoucí, vlastník případu užití, AI officer, ICT, bezpečnost či pověřenec pro ochranu osobních údajů.

Čl. 13 odst. 1 *Evidence*

Minimální základ interní governance AI. Evidence nemá být samoúčelná, ale má umožnit dohledatelnost, řízení přístupů a průběžné vyhodnocování využívání AI v organizaci. Úřad by si měl zvolit takovou míru evidence, která je proveditelná, ale zároveň přiměřená významu a rizikovosti využívání AI.

Čl. 13 odst. 3 *Incidenty*

Nejde jen o únik dat nebo zneužití účtu, ale také o halucinovaný právní nebo věcný výstup použitý v praxi, diskriminační výstup, prompt injection, únik promptu, neoprávněné použití dat pro trénování, chybné autonomní jednání agentního nástroje nebo reputační škodu. Smyslem je včasné zachycení problémů a poučení z nich, nikoli jen formální hlášení.

Doporučené přílohy

Přílohy nejsou jen technickým doplněním, ale klíčovým nástrojem, jak převést obecný vzor do podmínek konkrétního úřadu. Zde se obvykle nastavují konkrétní schválené nástroje, typy dat, případy užití, míra rizikovosti a odpovědnosti. Úřad by měl zvážit, které přílohy skutečně potřebuje hned od začátku a které může doplňovat postupně.

Kromě příkladů uvedených ve vzoru lze doporučit také další, např. formulář posouzení dopadů, vzor záznamu o schválení, pravidla auditní stopy, pravidla pro AI incidenty, pravidla pro veřejné zakázky/pořizování AI a vzor minimálních smluvních požadavků na AI služby.