

# AI ACT, KYBERNETICKÁ BEZPEČNOSŤ A NOVÁ ZODPOVEDNOSŤ ZA SOFTVÉR

ŠEŠŤ PREDPISOV, DVE OTÁZKY A JEDEN SYSTÉM,  
KTORÝM SA TO DÁ ZVLÁDNUŤ.

STAV K 31. AUGUSTU 2026

**G. Lehnert**  
LAWYERS WITH INTEGRITY



# OBSAH

## NUTSHELL – AI GOVERNANCE

|                                       |   |
|---------------------------------------|---|
| ŠEŠŤ PREDPISOV, DVE OTÁZKY            | 4 |
| KALENDÁR TERMÍNOV                     | 4 |
| JEDEN INCIDENT, ŠTYRI HLÁSENIA        | 5 |
| ROZHODOVACÍ TEST: TÝKA SA TO NÁS?     | 5 |
| MODELOVÁ FIRMA: AKO TO VYZERÁ V PRAXI | 6 |
| SLOVNÍK POJMOV A SKRATIEK             | 7 |

## ÚVOD

|                                                         |   |
|---------------------------------------------------------|---|
| VŠETCI HOVORIA O AI ACT. MÁLOKTO VIE, ČO Z NEHO VYPLÝVA | 9 |
|---------------------------------------------------------|---|

## ČASŤ I – AI ACT: ČO Z NEHO PRE VÁS VYPLÝVA

|                                                |    |
|------------------------------------------------|----|
| ČO AI ACT JE A ČO NIE JE                       | 10 |
| ČO JE VLASTNE AI SYSTÉM                        | 10 |
| PRVÁ OTÁZKA: V AKEJ STE ROLE?                  | 10 |
| DRUHÁ OTÁZKA: AKÉ JE RIZIKO VÁŠHO POUŽITIA AI? | 11 |
| ČO PLATÍ UŽ DNES                               | 11 |
| AKO SPLNIŤ OZNAČOVANIE AI OBSAHU V PRAXI       | 12 |
| IKONY EÚ NA OZNAČOVANIE AI OBSAHU              | 13 |
| KTO TO BUDE NA SLOVENSKU DOZOROVAŤ             | 14 |
| ČO PRÍDE V ROKOCH 2027 A 2028                  | 14 |
| PRIENIK S GDPR: DPIA A FRIA                    | 15 |
| SANKCIE                                        | 15 |

## ČASŤ II – KYBERNETICKÁ BEZPEČNOSŤ

|                                                                |    |
|----------------------------------------------------------------|----|
| TRI PREDPISY, TRI ODLIŠNÉ ROVINY                               | 17 |
| CYBER RESILIENCE ACT: BEZPEČNOSŤ VÝROBKU                       | 17 |
| SME SAAS FIRMA – TÝKA SA NÁS CRA?                              | 17 |
| NIS2 A ZÁKON O KYBERNETICKEJ BEZPEČNOSTI: ODOLNOSŤ ORGANIZÁCIE | 18 |
| DORA: FINANČNÝ SEKTOR A JEHO DODÁVATELIA                       | 18 |
| NIE STE V PÔSOBNOSTI? AJ TAK SA VÁS TO DOTKNE.                 | 19 |
| HLÁSENIE INCIDENTOV: POZRITE SI NUTSHELL                       | 19 |
| PREČO KYBERNETICKÁ BEZPEČNOSŤ A AI PATRIA K SEBE               | 19 |
| AK PÔSOBÍTE VO VIACERÝCH ČLENSKÝCH ŠTÁTOCH                     | 19 |

## ČASŤ III – AI AKO VÝROBOK: ZMENA OD 9. DECEMBRA 2026

|                              |    |
|------------------------------|----|
| ČO SA MENÍ                   | 20 |
| JADRO REFORMY: DOKAZOVANIE   | 20 |
| KTO ZODPOVEDÁ A ZA AKÚ ŠKODU | 20 |
| STAV NA SLOVENSKU            | 21 |

|                                                      |    |
|------------------------------------------------------|----|
| POISTENIE: OTÁZKA, KTORÚ TREBA POLOŽIŤ TERAZ         | 21 |
| AKO DLHO UCHOVÁVAŤ LOGY: GDPR VERZUS DŮKAZNÁ POZÍCIA | 21 |
| KDE SA TO SPÁJA S AI GOVERNANCE                      | 22 |

#### ČASŤ IV – AI GOVERNANCE: SPOLOČNÁ ODPOVEĎ

|                                                      |    |
|------------------------------------------------------|----|
| PREČO JEDEN SYSTÉM A NIE PÄŤ PROJEKTOV               | 23 |
| SEDEM DŮVODOV, PREČO TO DÁVA ZMYSEL AJ BEZ REGULÁCIE | 23 |
| AUTORSKÉ PRÁVO: VSTUPY AJ VÝSTUPY                    | 23 |
| PRAKTICKÉ MINIMUM                                    | 24 |
| KTO ZA TO VO FIRME ZODPOVEDÁ                         | 24 |
| INTERNÉ OZNAMOVANIE A OCHRANA OZNAMOVATEĽOV          | 25 |
| PREČO NESTAČÍ SMERNICA: ROZMER SKUTOČNÉHO SPRÁVANIA  | 25 |

#### ZHRNUTIE

|                      |    |
|----------------------|----|
| ČO ROBIŤ TERAZ       | 26 |
| ORIENTAČNÁ NÁROČNOSŤ | 26 |

## ŠEŠT PREDPISOV, DVE OTÁZKY

Firmy dnes riešia AI Act, kybernetickú bezpečnosť a zodpovednosť za softvér ako tri oddelené agendy. Sú to však odpovede na dve otázky, ktoré spolu úzko súvisia – a jeden systém ich rieši naraz.

### REGULÁCIA PRODUKTU: ČO SMIEM UVIESŤ NA TRH ALEBO NASADIŤ

| PREDPIS                                                   | ČO RIEŠI                                               | KOHO SA TÝKA                                                                                               |
|-----------------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>AI Act</b><br>nariadenie (EÚ) 2024/1689                | Za akých podmienok smiem AI vyvíjať a používať         | Každého, kto AI vyvíja, poskytuje alebo používa                                                            |
| <b>Cyber Resilience Act</b><br>nariadenie (EÚ) 2024/2847  | Kybernetická bezpečnosť výrobkov s digitálnymi prvkami | Výrobcov, dovozcov a distribútorov softvéru a pripojených zariadení                                        |
| <b>Zodpovednosť za výrobok</b><br>smernica (EÚ) 2024/2853 | Kto zaplatí, keď výrobok spôsobí škodu                 | Výrobcov a za zákonných podmienok aj dovozcov, distribútorov alebo ďalšie subjekty v dodávateľskom reťazci |

### REGULÁCIA ORGANIZÁCIE: AKO MUSÍ BYŤ RIADENÁ MOJA FIRMA

| PREDPIS                                                                | ČO RIEŠI                                          | KOHO SA TÝKA                                                                |
|------------------------------------------------------------------------|---------------------------------------------------|-----------------------------------------------------------------------------|
| <b>NIS2</b><br>zákon č. 69/2018 Z. z. v znení zákona č. 366/2024 Z. z. | Kybernetická odolnosť organizácie                 | Subjektov v regulovaných sektoroch; pri väčšine z nich rozhoduje aj veľkosť |
| <b>DORA</b><br>nariadenie (EÚ) 2022/2554                               | Digitálna prevádzková odolnosť finančného sektora | Finančných subjektov a ich IKT dodávateľov                                  |

### A ŠIESTY, KTORÝ UŽ POZNÁTE

| PREDPIS                                 | ČO RIEŠI                                                      | KOHO SA TÝKA                                             |
|-----------------------------------------|---------------------------------------------------------------|----------------------------------------------------------|
| <b>GDPR</b><br>nariadenie (EÚ) 2016/679 | Zákonnosť spracúvania osobných údajov a práva dotknutých osôb | Každého, kto spracúva osobné údaje – teda takmer každého |

**GDPR nie je nové – ale bolo by chybou ho z tohto obrazu vynechať.** Môže sa prelínať so všetkými piatimi uvedenými témami. Ak AI systém spracúva osobné údaje, **GDPR platí popri AI Acte**. Pri porušení ochrany osobných údajov môže vzniknúť samostatná oznamovacia povinnosť. Ak spracúvanie pravdepodobne povedie k vysokému riziku pre práva a slobody ľudí, treba vykonať aj posúdenie vplyvu na ochranu osobných údajov – DPIA.

#### NIE STE V PÔSOBNOSTI? AJ TAK SA VÁS TO DOTKNE.

NIS2 aj DORA sa k dodávateľom softvéru dostávajú cez zmluvy. Banka premietne požiadavky DORA do zmluvy s dodávateľom IT služieb; prevádzkovateľ základnej služby to isté podľa zákona o kybernetickej bezpečnosti.

Firma mimo priamej pôsobnosti tak nemusí automaticky plniť všetky zákonné povinnosti. Vybrané požiadavky sa však k nej môžu dostať prostredníctvom zmluvy, a to v lehote požadovanej zákazníkom.

## KALENDÁR TERMÍNOV

### UŽ PLATÍ

| DÁTUM              | ČO                                                                   |
|--------------------|----------------------------------------------------------------------|
| <b>1. 1. 2025</b>  | Zákon o kybernetickej bezpečnosti v znení transpozície NIS2          |
| <b>17. 1. 2025</b> | DORA                                                                 |
| <b>2. 2. 2025</b>  | AI Act – zákazy neprijateľných praktík a povinnosť AI gramotnosti    |
| <b>2. 8. 2025</b>  | AI Act – modely na všeobecné účely, správa a riadenie, sankčný režim |
| <b>1. 9. 2025</b>  | Vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach          |
| <b>2. 8. 2026</b>  | AI Act – povinnosti transparentnosti podľa čl. 50                    |

## NAJBLIŽŠIE TERMÍNY

| DÁTUM       | ČO                                                                                                                                                                                                                   |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11. 9. 2026 | CRA – hlásenie zneužívaných zraniteľností a závažných incidentov. Platí aj pre produkty, ktoré sú na trhu už dnes.                                                                                                   |
| 2. 12. 2026 | AI Act – nové zákazy systémov vytvárajúcich alebo upravujúcich intímny obsah bez súhlasu a materiál sexuálneho zneužívania detí; koniec odkladu pre strojovo čitateľné označovanie u starších generatívnych systémov |
| 9. 12. 2026 | Nový režim zodpovednosti za výrobok – softvér a AI ako výrobok                                                                                                                                                       |

## NESKÔR

| DÁTUM        | ČO                                                                                                      |
|--------------|---------------------------------------------------------------------------------------------------------|
| 2. 8. 2027   | AI Act – národné regulačné sandboxy                                                                     |
| 2. 12. 2027  | AI Act – vysokorizikové systémy podľa prílohy III (nábor, HR, úvery, poistenie, vzdelávanie, biometria) |
| 11. 12. 2027 | CRA – plná uplatniteľnosť vrátane posudzovania zhody a CE označenia                                     |
| 2. 8. 2028   | AI Act – vysokorizikové systémy zabudované do regulovaných výrobkov                                     |

## ČO JE ISTÉ A ČO SA EŠTE HÝBE

ISTÉ – plánujete s tým: všetky dátumy vyššie vyplývajú priamo z nariadení a smerníc EÚ. Nezávisia od slovenského legislatívneho procesu.

V POHYBE – sledujte: slovenský vykonávací zákon k AI Actu (návrh) a slovenský zákon o zodpovednosti za škodu spôsobenú vadným výrobkom (v druhom čítaní).

Menia sa detaily vykonania, nie termíny. **Termín 9. 12. 2026 platí bez ohľadu na to, kedy slovenský zákon nadobudne účinnosť.**

## JEDEN INCIDENT, ŠTYRI HLÁSENIA

V praxi najčastejšie podceňované riziko. Jediná udalosť môže spustiť niekoľko oznamovacích povinností súčasne – s rôznymi adresátmi a rôznymi lehotami.

| PREDPIS     | KTO HLÁSI                              | KOMU                               | LEHOTY                                                                                                                                                                                     |
|-------------|----------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CRA         | Výrobca produktu s digitálnymi prvkami | ENISA / SK-CERT                    | Zneužívaná zraniteľnosť: 24 hodín → 72 hodín → záverečná správa do 14 dní od dostupnosti nápravného opatrenia. Závažný incident: 24 hodín → 72 hodín → záverečná správa do jedného mesiaca |
| ZoKB (NIS2) | Prevádzkovateľ základnej služby        | NBÚ cez JISKB                      | 24 hodín → 72 hodín → 1 mesiac                                                                                                                                                             |
| DORA        | Finančný subjekt                       | Príslušný orgán dohľadu            | Do 4 hodín od klasifikácie incidentu ako závažného, najneskôr však do 24 hodín od jeho zistenia → priebežná správa do 72 hodín → záverečná správa do jedného mesiaca                       |
| GDPR        | Prevádzkovateľ                         | Úrad na ochranu osobných údajov SR | 72 hodín od zistenia; úradu sa incident neoznamuje, ak je nepravdepodobné, že povedie k riziku pre práva a slobody ľudí                                                                    |

**Čo z toho vyplýva:** dodržanie lehôt nie je len právna otázka. Je to otázka toho, či incident vôbec niekto zachytí, či vie, komu ho eskalovať, a či má firma vopred pripravené, ktoré z týchto hlásení sa jej týkajú. Pri DORA môže byť prvé oznámenie potrebné už do štyroch hodín od klasifikácie incidentu ako závažného.

## ROZHODOVACÍ TEST: TÝKA SA TO NÁS?

Deväť otázok, na ktoré viete odpovedať za desať minút. Každé áno vás nasmeruje na kapitolu, ktorú sa oplatí si prečítať. Test slúži na to, aby ste vedeli, čo sa vás konkrétne môže týkať.

| OTÁZKA                                                                                                                         | AK ÁNO                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| 1. Používate nástroj, ktorý generuje text, obrázky, odporúčania alebo predikcie – a nejde len o pevne naprogramované pravidlo? | AI Act sa vás týka. Minimálne v rozsahu AI gramotnosti a zákazov. Pozri kapitolu „Čo je vlastne AI systém“. |

|                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Komunikuje niektorý nástroj priamo s ľuďmi (chatbot, hlasová linka), alebo zverejňujete obsah vytvorený AI?                      | Treba preveriť povinnosti transparentnosti podľa čl. 50. Závisia od typu obsahu a od toho, či ste poskytovateľom alebo prevádzkovateľom systému. Osobitné pravidlá platia najmä pre chatboty, deepfaky a texty o veciach verejného záujmu. Platia od 2. 8. 2026. Pozri kapitoly „Ako splniť označovanie AI obsahu v praxi“ a „Ikony EÚ na označovanie AI obsahu“.     |
| 3. Používate AI pri náboře, hodnotení zamestnancov, prideľovaní práce, posudzovaní úverov alebo poistenia?                          | Môže ísť o vysokorizikový systém podľa prílohy III. Povinnosti sa uplatňujú od 2. 12. 2027. Pri posudzovaní úverovej bonity a pri posudzovaní rizika alebo stanovovaní cien v životnom a zdravotnom poistení treba vykonať aj FRIA. Pozri kapitoly „Čo príde v rokoch 2027 a 2028“ a „Prienik s GDPR: DPIA a FRIA“.                                                   |
| 4. Dodávate akýkoľvek softvér alebo pripojené zariadenie? Túto otázku si položte za každý produkt osobitne, nie za firmu ako celok. | Cyber Resilience Act. Pri každom produkte zvlášť posúdte, či ide o výrobok s digitálnymi prvkami – rozhoduje, kde softvér beží, nie čím sa vaša firma zaoberá. Ohlasovacie povinnosti od 11. 9. 2026. Pozri kapitolu „Sme SaaS firma – týka sa nás CRA?“.                                                                                                             |
| 5. Pôsobíte v regulovanom sektore (energetika, doprava, zdravotníctvo, IT a cloudové služby, výroba, potravinárstvo a ďalšie)?      | Overte si postavenie prevádzkovateľa základnej služby podľa zákona o kybernetickej bezpečnosti. Táto povinnosť platí od 1. 1. 2025. Pozri kapitolu „NIS2 a zákon o kybernetickej bezpečnosti: odolnosť organizácie“.                                                                                                                                                  |
| 6. Ste finančný subjekt, alebo dodávate IKT služby bankám, poisťovniam či obchodníkom s cennými papiermi?                           | Ak ste finančný subjekt, DORA sa na vás môže vzťahovať priamo. Ak finančným subjektom poskytujete IKT služby, jej požiadavky sa k vám spravidla dostanú prostredníctvom zmluvy. Na kritických poskytovateľov IKT služieb sa vzťahuje aj osobitný dohľad. Pozri kapitoly „DORA: finančný sektor a jeho dodávateľia“ a „Nie ste v pôsobnosti? Aj tak sa vás to dotkne“. |
| 7. Budete po 9. 12. 2026 uvádzať na trh softvér, AI systém alebo produkt s AI funkciou?                                             | Nový režim zodpovednosti za výrobok. Pozri tretiu časť brožúry.                                                                                                                                                                                                                                                                                                       |
| 8. Spracúvajú vaše AI nástroje osobné údaje?                                                                                        | GDPR platí ďalej. Pri vysokorizikových použitíach takmer vždy pribudne DPIA. Pozri kapitolu „Prienik s GDPR: DPIA a FRIA“.                                                                                                                                                                                                                                            |
| 9. Trénujete alebo dolaďujete vlastný model na dátach, ktoré ste nevytvorili sami?                                                  | Overte, či môžete dáta na tréningovanie alebo dolaďovanie modelu použiť. Dôležité sú najmä licenčné podmienky, pravidlá pre vyťažovanie textov a dát a prípadná výhrada práv ich nositeľov. Pozri kapitolu „Autorské právo: vstupy aj výstupy“.                                                                                                                       |

**Poznámka k otázke 5:** veľkostné kritériá a zoznam sektorov určuje zákon o kybernetickej bezpečnosti a nie sú intuitívne. NBÚ na tento účel prevádzkuje informačný portál. Ak si nie ste istí, ide o otázku, ktorú sa oplatí posúdiť radšej skôr než neskôr – povinnosť platí od januára 2025.

## MODELOVÁ FIRMA: AKO TO VYZERÁ V PRAXI

**PREČO ROZHODOVACÍ TEST NESTAČÍ NA UZAVRETIE TÉMY**

Test na predchádzajúcej strane je zjednodušený a odpovedá sa v ňom za firmu. Pri dvoch predpisoch je to však nesprávna rovina.

Cyber Resilience Act a nový režim zodpovednosti za výrobok nemožno posudzovať iba za firmu ako celok. Treba **OSOBITNE POSÚDIŤ KAŽDÝ PRODUKT**, ktorý firma dodáva. Firma nie je „v pôsobnosti“ alebo „mimo pôsobnosti“ – jednotlivý produkt je. Samostatná hostovaná služba môže byť mimo pôsobnosti CRA, zatiaľ čo inštalovateľná aplikácia alebo pripojené zariadenie do jeho pôsobnosti môže patriť.

Preto pri otázkach 4 a 7 nestačí jedno nie za firmu. Urobte si zoznam všetkého, čo dodávate – hostovaná služba, mobilná aplikácia, on-premise edícia, agent, SDK, rozšírenie prehliadača, zariadenie s aplikáciou – a otázku si položte pri každej položke zvlášť.

Príklad nižšie ukazuje, že pri jednej firme treba osobitne posudzovať používané AI systémy aj produkty, ktoré dodáva.

Stredne veľká výrobná firma, 90 zamestnancov. Nemá compliance oddelenie. Používa bežné nástroje a predáva stroje s pripojenou aplikáciou. Takto vyzerá výsledok, keď si prejde všetko, čo v skutočnosti používa.

| ČO POUŽÍVA                           | ČO TO JE                               | ČO Z TOHO VYPLÝVA                                                                                                                                                             |
|--------------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft Copilot v kancelárii       | AI systém. Minimálne riziko.           | AI gramotnosť: preškoliť zamestnancov a školenie zdokumentovať. Politika, čo sa doň smie vkladať.                                                                             |
| Chatbot na webe od dodávateľa        | AI systém. Obmedzené riziko.           | Musí sa priznať, že je AI. Zodpovedá poskytovateľ – ale ak beží pod značkou firmy a firma zmenila jeho účel, zodpovednosť sa preklápa na firmu.                               |
| Nástroj na predtriedenie životopisov | AI systém. Vysoké riziko, príloha III. | Od 2. 12. 2027: ľudský dohľad, logy, informovanie zamestnancov a uchádzačov. DPIA takmer isto. FRIA nie – firma nie je verejným subjektom ani neposudzuje úvery či poistenie. |

|                                        |                                   |                                                                                                                                                |
|----------------------------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| AI retuš produktových fotografií       | AI systém. Posúdiť podľa výstupu. | Ak výsledok zobrazuje identifikovateľnú osobu tak, že pôsobí autenticky, ide o deepfake a musí byť označený. Retuš pozadia produktu nie.       |
| Sentiment analýza tiketov podpory      | AI systém. Posúdiť hranicu.       | Ak vyhodnocuje emócie zákazníkov, nejde o zakázanú praktiku. Ak by vyhodnocovala emócie zamestnancov podpory, ide o zákaz na pracovisku.       |
| Stroj s pripojenou mobilnou aplikáciou | Výrobok s digitálnymi prvkami.    | CRA: aplikácia na stiahnutie je v pôsobnosti. Ohlasovanie zraniteľností od 11. 9. 2026. Od 9. 12. 2026 aj nový režim zodpovednosti za výrobok. |
| Interný Excel s regresným modelom      | Pravdepodobne nie je AI systém.   | Lineárna regresia a jednoduché štatistické odhady sú z definície spravidla vylúčené. Posúdenie však treba urobiť a písomne zaznamenať.         |

#### ČO SI Z TOHO ODNIESLA

Týkajú sa jej tri predpisy, nie päť: AI Act, CRA a nový režim zodpovednosti za výrobok. DORA nie. Postavenie podľa zákona o kybernetickej bezpečnosti si musí overiť.

Najbližší termín pre ňu nie je z AI Actu, ale 11. september 2026 – ohlasovanie zraniteľností v mobilnej aplikácii k stroju.

Najprísnejší režim sa jej týka kvôli jednému nástroju, o ktorom nikto nepredpokladal, že bude problém: predtriedeniu životopisov.

Dva nástroje si vyžadujú individuálne posúdenie hranice, nie tabuľkovú odpoveď. To je bežný stav, nie výnimka.

**Späť k rozhodovaciemu testu:** všimnite si posledné dva riadky tabuľky. Tá istá firma je so svojím strojom a pripojenou aplikáciou v pôsobnosti Cyber Resilience Act, a s interným Excelom mimo pôsobnosti AI Actu. Práve preto je otázka č. 4 v teste zjednodušená a musí sa kláďť pri každom produkte zvlášť, nie raz za firmu. Podrobne v kapitole „Sme SaaS firma – týka sa nás CRA?“ v druhej časti brožúry.

## SLOVNÍK POJMOV A SKRATIEK

Brožúra pracuje s pojmami, ktoré sa v praxi používajú prevažne v skratkách. Tento prehľad slúži na rýchlu orientáciu.

| SKRATKA    | ČO ZNAMENÁ                                                                                                   |
|------------|--------------------------------------------------------------------------------------------------------------|
| AI Act     | Nariadenie (EÚ) 2024/1689 o umelej inteligencii.                                                             |
| AI Omnibus | Zjednodušujúci balík z roku 2026, ktorý zmenil harmonogram AI Actu.                                          |
| CRA        | Cyber Resilience Act – nariadenie (EÚ) 2024/2847 o kybernetickej bezpečnosti výrobkov s digitálnymi prvkami. |
| DORA       | Nariadenie (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora.                            |
| DPIA       | Posúdenie vplyvu na ochranu údajov podľa čl. 35 GDPR.                                                        |
| ENISA      | Agentúra Európskej únie pre kybernetickú bezpečnosť.                                                         |
| FRIA       | Posúdenie vplyvu na základné práva podľa čl. 27 AI Actu.                                                     |
| GPAI       | Modely umelej inteligencie na všeobecné účely.                                                               |
| JISKB      | Jednotný informačný systém kybernetickej bezpečnosti, cez ktorý sa podávajú hlásenia NBÚ.                    |
| MIRRI      | Ministerstvo investícií, regionálneho rozvoja a informatizácie SR.                                           |
| NBÚ        | Národný bezpečnostný úrad.                                                                                   |
| NIS2       | Smernica (EÚ) 2022/2555 o kybernetickej bezpečnosti.                                                         |
| PZS        | Prevádzkovateľ základnej služby podľa zákona o kybernetickej bezpečnosti.                                    |
| SBOM       | Súpis softvérových komponentov výrobku.                                                                      |

|         |                                                                               |
|---------|-------------------------------------------------------------------------------|
| SK-CERT | Národná jednotka SR pre riešenie kybernetických bezpečnostných incidentov.    |
| TDM     | Text and data mining – čerpanie textov a údajov, vrátane tréningu AI modelov. |
| ZoKB    | Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti.                           |

#### POZOR NA JEDNO SLOVO V TROCH VÝZNAMOCH

Slovo „prevádzkovateľ“ znamená v každom z predpisov niečo iné. Toto je najčastejší zdroj nedorozumení pri internej komunikácii.

| POJEM                           | VÝZNAM                                                                                                              |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Poskytovateľ (AI Act)           | Kto AI systém vyvíja alebo ho uvádza na trh pod vlastným menom či značkou.                                          |
| Prevádzkovateľ (AI Act)         | Nasadzujúci subjekt – kto AI systém používa v rámci svojej činnosti. V role je väčšina firiem.                      |
| Prevádzkovateľ (GDPR)           | Kto určuje účel a prostriedky spracúvania osobných údajov. Iný pojem než prevádzkovateľ podľa AI Actu.              |
| Prevádzkovateľ základnej služby | Subjekt zapísaný v registri podľa zákona o kybernetickej bezpečnosti. Tretí, opäť odlišný význam toho istého slova. |

## VŠETCI HOVORIA O AI ACT. MÁLOKTO VIE, ČO Z NEHO VYPLÝVA

Za posledné dva roky sa AI Act stal jednou z najčastejšie spomínaných skratiek v podnikovom prostredí. Zároveň patrí medzi najmenej pochopené predpisy. Bežná firma sa dozvie, že „AI Act platí“, prípadne že „sa to odložilo“, a ďalej nevie, či sa jej to týka, čo má urobiť a dokedy.

Realita je pritom prehľadnejšia, než sa zdá. AI Act nereguluje technológiu ako takú – reguluje to, na čo ju používate. Väčšina firiem nie je vývojárom AI, ale jej používateľom. A pre používateľov je zoznam povinností kratší, konkrétnejší a splniteľnejší, než sa všeobecne predpokladá.

Problém je inde: AI Act nestojí sám. Súbežne s ním beží kybernetická regulácia – Cyber Resilience Act pre výroby, zákon o kybernetickej bezpečnosti v znení NIS2 pre organizácie a DORA pre finančný sektor a jeho dodávateľov. A od decembra 2026 pribúda úplne nová rovina: softvér vrátane AI systémov sa po prvýkrát výslovne považuje za výrobok v režime objektívnej zodpovednosti za škodu.

AI Act hovorí, čo smiete. Kybernetická regulácia hovorí, ako to musíte zabezpečiť. Nová úprava zodpovednosti hovorí, čo zaplatíte, ak sa niečo pokazí. AI governance je to, čím sa všetky tri dajú zvládnuť naraz.

Táto brožúra je určená pre nepravnické publikum. Prvá časť vysvetľuje AI Act a jeho praktické dôsledky. Druhá časť sa venuje kybernetickej bezpečnosti a tomu, ako sa tri predpisy prekrývajú. Tretia časť popisuje zmenu zodpovednosti za výrobok. Štvrtá časť ukazuje, prečo je odpoveďou na všetky tri jeden systém a nie päť samostatných projektov.

Ak si chcete urobiť rýchly obraz, stačia dve strany Nutshellu na začiatku brožúry. Zvyšok rozvádza, čo za jednotlivými riadkami stojí.

## ČO AI ACT JE A ČO NIE JE

AI Act (nariadenie (EÚ) 2024/1689) je nariadenie, ktoré platí priamo, bez potreby slovenského vykonávacieho zákona. AI Act nie je len predpis o bezpečnosti výrobkov. Ide o reguláciu založenú na miere rizika, ktorá upravuje vývoj, dodávanie a používanie AI a chráni aj základné práva.

- **Nezakazuje umelú inteligenciu.** Zakazuje niekoľko konkrétnych spôsobov jej použitia a pre niekoľko ďalších stanovuje podmienky.
- **Netýka sa len technologických firiem.** Zaväzuje aj bežné podniky, ktoré AI iba používajú – vrátane HR, marketingu, financií a zákazníckej podpory.
- **Neuplatňuje sa celý od jedného dátumu.** Jednotlivé povinnosti nadobúdajú účinnosť postupne od februára 2025 do augusta 2028.
- **Nenahrádza GDPR ani autorské právo.** Pridáva sa k nim. Ak spracúvate osobné údaje, GDPR platí naďalej v plnom rozsahu.

Harmonogram AI Actu bol v roku 2026 upravený tzv. AI Omnibusom – zjednodušujúcim balíkom, ktorý nadobudol účinnosť 27. júla 2026.

### NAJČASTEJŠÍ OMYL

„Odložili to, takže máme čas.“

Neodložil sa však celý AI Act. Odložené boli povinnosti pre vysokorizikové systémy podľa prílohy III na 2. decembra 2027 a pri systémoch spojených s regulovanými výrobkami na 2. augusta 2028. Viaceré zákazy, povinnosť AI gramotnosti, pravidiel pre veľké modely a povinnosti transparentnosti odložené neboli. Povinnosti transparentnosti platia od 2. augusta 2026, teda už dnes.

## ČO JE VLASTNE AI SYSTÉM

Prvým krokom pri klasifikácii rizika je posúdiť, či daný nástroj vôbec spĺňa definíciu AI systému. Komisia k tejto definícii vydala 6. februára 2025 samostatné nezáväzné usmernenia, ktoré predstavujú dôležité výkladové vodidlo.

Podľa čl. 3 ods. 1 AI Actu je AI systém strojový systém navrhnutý tak, aby fungoval s rôznou mierou autonómie, ktorý môže po nasadení vykazovať adaptívnosť a ktorý na základe explicitných alebo implicitných cieľov odvodzuje zo vstupov, ako generovať výstupy – predikcie, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie.

Kľúčovým prvkom je schopnosť systému „odvodzovať“ zo vstupov, ako vytvoriť výstupy. Práve tá ho spravidla odlišuje od bežného softvéru, ktorý iba vykonáva vopred určené pokyny. Komisia označuje schopnosť odvodzovať za nevyhnutný prvok definície, ale posúdenie musí vždy vychádzať z konkrétnych vlastností systému.

### ČO PODĽA USMERNENÍ KOMISIE AI SYSTÉMOM SPRAVIDLA NIE JE

Systémy fungujúce výlučne na pravidlách, ktoré definoval človek, aby sa automaticky vykonali určité operácie.

Nástroje matematickej optimalizácie vrátane lineárnej a logistickej regresie.

Klasické heuristické systémy, ktoré sa neučia z dát ani zo skúsenosti.

Jednoduché predikčné nástroje využívajúce základné štatistické metódy, napríklad odhad podľa priemeru, bez rozpoznávania zložitejších vzorov.

Základné spracovanie dát podľa vopred daných explicitných inštrukcií, bez učenia a odvodzovania.

Praktický dôsledok pre bežné firemné nástroje:

- **Excel s prognózou podľa lineárnej regresie:** pravdepodobne nie je AI systém.
- **Skript triediaci životopisy podľa pevného zoznamu kľúčových slov:** pravdepodobne nie je AI systém – ale nástroj, ktorý uchádzačov hodnotí modelom naučeným z historických dát, ním spravidla je, a pri použití na nábor alebo výber uchádzačov môže byť vysokorizikový.
- **Chatbot postavený na jazykovom modeli a generátor obrázkov sú AI systémy.** Odporúčací systém a nástroj na skórovanie ním spravidla je, ak pri vytváraní výstupov využíva model alebo inú schopnosť odvodzovania.

Toto si zapíšte: Pri každom nástroji si zaznamenajte, prečo ho považujete alebo nepovažujete za AI systém. AI Act ani usmernenia všeobecne neurčujú formu takéhoto záznamu. Stručné a vecné odôvodnenie v internom registri však môže byť primeraným praktickým riešením.

## PRVÁ OTÁZKA: V AKEJ STE ROLE?

Pre bežnú firmu sú najdôležitejšie dve role, od ktorých sa odvíja rozsah jej povinností.

- **Poskytovateľ** – vyvíjate AI systém alebo ho uvádzate na trh pod vlastným menom či značkou. Sem patria aj firmy, ktoré si dajú AI riešenie vyvinúť na mieru a ponúkajú ho pod svojou značkou. Povinností je najviac.
- **Prevádzkovateľ (nasadzujúci subjekt)** – AI systém iba používate v rámci svojej činnosti. V tejto role je väčšina firiem. Povinností je podstatne menej, nie sú však nulové.

**Pozor na preklopenie role:** pri vysokorizikovom AI systéme sa môžete za určitých okolností stať poskytovateľom, napríklad ak ho uvediete pod vlastným menom alebo značkou, podstatne ho zmeníte alebo zmeníte zamýšľaný účel pôvodne nevysokorizikového systému tak, že sa stane vysokorizikovým.

## DRUHÁ OTÁZKA: AKÉ JE RIZIKO VÁŠHO POUŽITIA AI?

Použitie AI možno na praktické účely rozdeliť do štyroch rizikových pásiem. Rozhodujúci je najmä zamýšľaný účel a spôsob použitia, nie iba samotný nástroj – ten istý jazykový model môže byť pri jednom použití minimálne rizikový a pri inom vysokorizikový.

| PÁSMO                      | TYPICKÉ PRÍKLADY                                                                                                                                                                                                                                                                                                                                        | ČO TO ZNAMENÁ                                                                                                   |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Neprijateľné riziko</b> | Sociálne skórovanie vedúce k neodôvodnenému alebo neprimeranému znevýhodneniu, manipulatívne techniky alebo zneužívanie zraniteľnosti osôb, rozpoznávanie emócií na pracovisku a v školách s výnimkou zdravotných a bezpečnostných dôvodov, necielené získavanie tváří z internetu alebo kamerových záznamov na vytváranie databáz rozpoznávania tváří. | Zakázané. Overiť, že to nerobí ani váš poskytovateľ.                                                            |
| <b>Vysoké riziko</b>       | Nábor a výber uchádzačov, hodnotenie a monitorovanie zamestnancov, pridelovanie práce, povýšenie a ukončenie pracovného pomeru, posudzovanie úverov, ceny a rizika v životnom a zdravotnom poistení, vzdelávanie, biometria, kritická infraštruktúra.                                                                                                   | Najprísnejší režim. Povinnosti nastupujú 2. 12. 2027 – prípravu treba začať skôr.                               |
| <b>Obmedzené riziko</b>    | Chatboty, generovanie textu, obrázkov, zvuku a videa, deepfaky, rozpoznávanie emócií mimo zakázaných kontextov.                                                                                                                                                                                                                                         | Podľa typu systému vzniká povinnosť informovať a označovať obsah vytvorený či upravený AI. Platí od 2. 8. 2026. |
| <b>Minimálne riziko</b>    | Prevažná väčšina bežných nástrojov – filtre nevyžiadanej pošty, odporúčacie systémy, plánovanie, jednoduchá automatizácia.                                                                                                                                                                                                                              | Bez osobitných povinností podľa AI Actu. AI gramotnosť však platí naprieč.                                      |

### KDE SA FIRMY NAJČASTEJŠIE PREKVAPIA

Rozpoznávanie emócií na pracovisku a v školách patrí medzi zakázané praktiky – týka sa to napríklad nástrojov, ktoré vyhodnocujú náladu alebo angažovanosť zamestnancov zo záznamu hovoru alebo z videa.

AI systémy používané pri náboe a hodnotení zamestnancov spravidla patria medzi vysokorizikové. Týka sa to napríklad AI nástrojov, ktoré triedia životopisy, hodnotia uchádzačov alebo pracovný výkon a podstatne ovplyvňujú príslušné rozhodnutie. Na firmy, ktoré ich používajú, sa vzťahujú povinnosti prevádzkovateľov vysokorizikových systémov od 2. decembra 2027.

## ČO PLATÍ UŽ DNES

### 1. AI GRAMOTNOSŤ (OD 2. FEBRUÁRA 2025)

Musíte zabezpečiť, aby osoby, ktoré vo vašom mene AI systémy používajú, mali primeranú úroveň znalostí – teda rozumeli tomu, čo nástroj robí, aké má obmedzenia a aké riziká sa s ním spájajú. Rozsah sa posudzuje podľa toho, na čo AI používate.

**Prakticky:** vyškoliť zamestnancov, ktorí AI reálne používajú, prispôbiť školenie ich rolám a viesť o ňom evidenciu. Bez dokladu o školení povinnosť nepreukázete.

### 2. ZÁKAZ NEPRIJATEĽNÝCH PRAKTÍK (OD 2. FEBRUÁRA 2025)

Zoznam je pomerne úzky, siaha však ďalej, než sa väčšina firiem nazdáva. Patrí sem sociálne skórovanie, manipulatívne techniky zneužívajúce zraniteľnosť osôb, necielené získavanie fotografií tváří z internetu alebo kamerových záznamov na vytváranie alebo rozširovanie databáz rozpoznávania tváří a rozpoznávanie emócií na pracovisku a vo vzdelávacích zariadeniach. Od 2. decembra 2026 k nim pribudne zákaz používať AI na vytváranie alebo úpravu intímneho obsahu identifikovateľnej osoby bez jej súhlasu a materiálu zobrazujúceho sexuálne zneužívanie detí.

**Prakticky:** prejsť reálne používané nástroje – vrátane tých, ktoré si zamestnanci zaviedli sami – a overiť, či niektorá funkcionálna do zoznamu nespadá. Rovnakú otázku položiť dodávateľom.

#### KDE PRESNE JE HRANICA PRI ROZPOZNÁVANÍ EMÓCIÍ

Zákaz sa týka systémov, ktoré na základe biometrických údajov, napríklad tváre alebo vlastností hlasu, rozpoznávajú alebo odvodzujú emócie ľudí na pracovisku alebo vo vzdelávacích zariadeniach. Výnimkou sú systémy používané zo zdravotných alebo bezpečnostných dôvodov.

V zákaze: nástroj, ktorý z hlasu alebo obrazu zamestnanca odvodzuje jeho náladu alebo emócie.

Mimo zákazu: textová analýza spätnej väzby zákazníkov, ktorá hodnotí obsah textu a nevyvodzuje emócie z biometrických údajov. Ak však systém vyhodnocuje emócie zákazníka podľa hlasu alebo obrazu, nejde síce o zakázané použitie na pracovisku, ale systém môže byť vysokorizikový a zákazník musí byť informovaný o jeho používaní.

Pozor na zmiešaný prípad: nástroj, ktorý hodnotí kvalitu hovorov podpory, spravidla vyhodnocuje aj tón operátora. Vtedy sa dostáva na pracovisko. Toto je typický prípad, kde odpoveď nie je tabuľková a je namieste individuálne posúdenie.

### 3. TRANSPARENTNOSŤ A OZNAČOVANIE (OD 2. AUGUSTA 2026)

Toto je povinnosť, ktorá začala platiť najnovšie a týka sa najširšieho okruhu firiem. Vztahuje sa na všetky systémy v pôsobnosti bez ohľadu na to, kedy boli uvedené na trh. Nasledujúca kapitola sa jej venuje podrobne.

## AKO SPLNIŤ OZNAČOVANIE AI OBSAHU V PRAXI

Komisia prijala 20. júla 2026 usmernenia k povinnostiam transparentnosti podľa čl. 50 AI Actu. Vysvetľujú, na koho sa tieto povinnosti vzťahujú, pri akom obsahu sa uplatnia a ako ich Komisia vykladá. Usmernenia sú nezáväzné a záväzný výklad môže dať len Súdny dvor EÚ, v praxi však budú dôležitým vodítkom národných orgánov dohľadu. Popri usmerneniach existuje aj tzv. Kódex postupov o transparentnosti AI-generovaného obsahu. Kódex postupov má dve časti. Poskytovateľom ponúka praktické pravidlá na strojovo čitateľné označovanie a detekciu AI výstupov. Prevádzkovateľom poskytuje pravidlá na označovanie deepfake obsahu a určitých textov vytvorených alebo upravených AI. Dodržiavanie Kódexu postupov môže dotknutým subjektom uľahčiť preukázanie súladu s článkom 50, nenahrádza však samotné zákonné povinnosti.

#### PÄŤ SITUÁCIÍ A KTO V NICH ZODPOVEDÁ

| SITUÁCIA                                         | ČO SA VYŽADUJE                                                                                                                                      | KTO            |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| Chatbot a hlasový asistent                       | Používateľ musí byť informovaný, že komunikuje s AI, najneskôr pri prvom kontakte.                                                                  | Poskytovateľ   |
| Syntetický obsah                                 | Výstup musí byť označený strojovo čitateľným spôsobom a detegovateľný ako umelo vytvorený.                                                          | Poskytovateľ   |
| Deepfake                                         | Obsah zverejnený voči verejnosti musí byť zreteľne označený ako AI-generovaný.                                                                      | Prevádzkovateľ |
| Text o veciach verejného záujmu                  | Označenie sa vyžaduje, ak text neprešiel redakčnou kontrolou a za jeho zverejnenie nenesie redakčnú zodpovednosť konkrétna osoba alebo organizácia. | Prevádzkovateľ |
| Rozpoznávanie emócií a biometrická kategorizácia | Dotknuté osoby musia byť informované.                                                                                                               | Prevádzkovateľ |

#### NAJDRAHŠIE NEDOROZUMENIE: „CHATBOTA NÁM DODÁVA NIEKTO INÝ“

V tabuľke vyššie je pri chatbote uvedený poskytovateľ. Neznamená to, že firma, ktorá chatbota len nasadila, nemá s vecou nič spoločné.

Ak chatbot beží pod vašou značkou, ak ste ho podstatne zmenili alebo ak ste zmenili jeho zamýšľaný účel, stávate sa poskytovateľom vy – so všetkými povinnosťami poskytovateľa.

Aj keď zostanete v role prevádzkovateľa, za informácie, ktoré chatbot poskytuje vašim zákazníkom vo vašom mene, môžete zodpovedať. Zodpovednosti sa automaticky nezabavíte tvrdením, že chatbota vytvorila externá firma. Tým však nie je vylúčená ani prípadná zodpovednosť poskytovateľa.

Praktický krok: pri každom nástroji od poskytovateľa si písomne ujasnite, kto má podľa AI Actu postavenie poskytovateľa a kto postavenie prevádzkovateľa, kto prakticky zabezpečí splnenie jednotlivých povinností podľa článku 50 a ako si strany poskytnú potrebnú súčinnosť. Upravte to aj v zmluve s dodávateľom. Zmluva síce nemení rozdelenie zákonných povinností podľa AI Actu, ale môže upraviť vzájomnú zodpovednosť a nároky medzi stranami.

#### ČO NESPLŇA POŽIADAVKU ZRETEĽNÉHO OZNAČENIA PRE ĽUDÍ?

Usmernenia sú v tomto bode konkrétne. Za jasné a rozlíšiteľné označenie sa nepovažuje drobný text ukrytý v pätičke webovej stránky, bledý štítok na obrázku ani popisok blikajúci vo videu na okamih. Rovnako nestačí vysvetlenie schované v obchodných podmienkach.

#### ČO POSKYTOVATEĽ NEMUSÍ OZNAČOVAŤ STROJOVO?

Nasledujúce výnimky sa týkajú technického, strojovo čitateľného označovania podľa článku 50 ods. 2 AI Act. Nevzťahujú sa automaticky na povinnosť zreteľne označiť deepfake alebo text o veciach verejného záujmu.

- Veľmi krátke výstupy – jednotlivé slová, popisky obrázkov, alternatívny text a označenia v používateľskom rozhraní.
- Zdrojový kód, pričom pojem je vymedzený pomerne široko.
- Súhrny vytvorené AI a podstatné prepisy textu naopak spravidla patria do rozsahu povinnosti strojového označovania.

## TRI VÝNIMKY Z POVINNOSTI ZVEREJNENIA

- **Tvorivé diela.** Ak je deepfake súčasťou zjavne umeleckého, tvorivého, satirického alebo fiktívneho diela, povinnosť sa obmedzuje na zverejnenie primeraným spôsobom, ktorý nebráni zobrazeniu alebo vnímaniu diela.
- **Použitie povolené zákonom.** Povinnosť sa neuplatní, ak je použitie povolené zákonom na odhaľovanie, prevenciu, vyšetrovanie alebo stíhanie trestných činov.
- **Redakčná kontrola textu.** Povinnosť sa neuplatní, ak text prešiel ľudským preskúmaním alebo redakčnou kontrolou a konkrétna osoba nesie za zverejnenie redakčnú zodpovednosť.

## OTÁZKA SPÄTNÉHO OZNAČOVANIA

Povinnosť označiť už existujúci obsah spätne nevzniká. Rozhodujúci moment sa však líši podľa typu obsahu: pri obrázkových, zvukových a video deepfakoch je rozhodujúci dátum vytvorenia obsahu, takže obsah vytvorený pred 2. augustom 2026 sa spätne neoznačuje. Pri textoch o veciach verejného záujmu je rozhodujúci dátum zverejnenia – text vytvorený pred 2. augustom, ale zverejnený neskôr, označiť treba, ak sa neuplatní výnimka pre redakčnú kontrolu.

Osobitný odklad platí pre poskytovateľov generatívnych systémov, ktoré už boli na trhu: povinnosť zabezpečiť strojovo čitateľné označenie výstupov musia splniť do 2. decembra 2026.

### PRAKTICKÝ POSTUP

Prejsť webové chatboty a hlasové linky: informujú používateľa najneskôr pri prvom kontakte, že komunikuje s AI?

Prejsť marketingové vizuály a videá: obsahujú AI-generovaný alebo upravený obsah, ktorý môže klamlivo pôsobiť ako autentické zobrazenie skutočnej alebo vierohodne pôsobiacej osoby, predmetu, miesta či udalosti? Ak áno, je označený zreteľne, nie iba drobným textom v pätičke?

Zaviest pravidlo pre budúci obsah. Jednorazová kontrola nestačí – označovanie sa musí stať súčasťou schvaľovacieho procesu.

Overiť u poskytovateľov generatívnych nástrojov, či a ako implementujú strojovo čitateľné označovanie a či pristúpili ku Kódexu postupov.

Zvážiť použitie ikon EÚ – sú zadarmo, prešli testovaním a klientovi aj orgánu dohľadu signalizujú vedomý prístup. Na zvýšenie zrozumiteľnosti je vhodné ich doplniť textovým štítkom. Samotné použitie ikony však neznamená, že firma pristúpila ku Kódexu postupov.

## IKONY EÚ NA OZNAČOVANIE AI OBSAHU

Európska únia vytvorila súbor ikon, ktoré môžu tvorcovia, vydavatelia a ďalšie nasadzujúce subjekty používať na označovanie obsahu vytvoreného alebo upraveného generatívnou AI. Ikony sú voľne dostupné a tvoria súčasť oddielu 2 Kódexu postupov.

### KDE IKONY STIAHNUŤ

Ikony sú voľne dostupné na stránke Európskej komisie: [digital-strategy.ec.europa.eu](https://digital-strategy.ec.europa.eu/en/policies/ai-label) → Politiky → Ikony EÚ na označovanie obsahu vytvoreného umelou inteligenciou.

Na stiahnutie sú dva zip súbory – jeden vo formáte SVG, druhý vo formáte PNG. Každý obsahuje všetky tri ikony vo všetkých štyroch farebných variantoch.

Použitie je bezplatné a nevyžaduje uvedenie Európskej komisie ani Úradu pre umelú inteligenciu.

Pre tlač a väčšie formáty odporúčame SVG, pre rýchle nasadenie na webe a v sociálnych sieťach PNG.

### DÔLEŽITÉ ROZLIŠENIE

Používanie ikon EÚ je dobrovoľné. Ak však subjekt pristúpil ku Kódexu postupov, musí dodržiavať jeho pravidlá. Samotné povinnosti podľa článku 50 AI Actu dobrovoľné nie sú.

Použitie ikony samo osebe nie je dôkazom súladu s právnymi predpismi. Za strojovo čitateľné označenie výstupov zodpovedá poskytovateľ AI systému. Za zreteľné označenie deepfaku alebo príslušného textu zodpovedá prevádzkovateľ, ktorý obsah zverejňuje alebo sprístupňuje.

## TRI IKONY A KEDY KTORÚ POUŽIŤ

| IKONA                                                                                                           | KEDY SA POUŽÍVA                                                                                                                                                                                                                                                    | PRÍKLAD                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Základná ikona</b><br>    | Na všeobecné označenie, že pri vytvorení alebo úprave obsahu bola použitá AI. Základná ikona sa môže používať spolu so slovným upozornením, napríklad „hlas vytvorený AI“. Môže byť tiež klikateľná a po otvorení zobrazovať podrobnejšie informácie o použití AI. | Deepfake video s textovým štítkom „generovaný hlas“, za ktorým nasleduje základná ikona                    |
| <b>Plne vytvorené AI</b><br> | Celý obsah je vytvorený umelou inteligenciou, bez prvkov vytvorených človekom a bez ľudskej redakčnej kontroly – s výnimkou samotného zadania.                                                                                                                     | Deepfake video s politikom alebo fiktívnou udalosťou; plne AI komponovaná hudba; súhrny správ vytvorené AI |

|                                                        |                                                                                                                                                            |                                                                                                           |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <p>Čiastočne upravené AI</p> <p><b>AI MODIFIED</b></p> | <p>Existujúci obsah vytvorený človekom bol umelou inteligenciou čiastočne upravený tak, že sa z neho stal deepfake alebo text o veci verejného záujmu.</p> | <p>Vymenená tvár na autentickej fotografii; autentická fotografia prázdneho bytu zariadená pomocou AI</p> |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|

### FORMÁTY A VARIANTY

- Každá ikona má štyri varianty: čiernu, bielu, čiernu s 50 % priehľadnosťou a bielu s 50 % priehľadnosťou.
- K dispozícii sú vo formátoch SVG a PNG na stiahnutie zo stránok Európskej komisie.
- Ikony prešli používateľským testovaním. Vo všetkých sledovaných ukazovateľoch fungovali lepšie vtedy, keď ich sprevádzal textový štítok – napríklad „upravené“. Samotná ikona bez textu je pre príjemcu horšie zrozumiteľná.

### PRAVIDLÁ UMIESTNENIA IKON

Nasledujúci prehľad je zhrnutím, nie úplným výpočtom. Podrobné špecifikácie, ku ktorých plneniu sa zaväzujú signatári, obsahuje oddiel 2 Kódexu postupov.

- Ikona má byť jasne vnímateľná a rozlíšiteľná najneskôr v okamihu, keď je osoba obsahu vystavená po prvýkrát.
- Má byť umiestnená tam, kde ju neprekrývajú iné prvky.
- Má byť vložená priamo do obsahu – s výnimkou tvorivých diel – ak nie sú k dispozícii rovnocenné alternatívy, napríklad prekrytie používateľského rozhrania.
- Musí zostať viditeľná aj vtedy, keď obsah niekto ďalej zdieľa alebo si ho stiahne. Toto je bod, na ktorý sa v praxi najčastejšie zabúda.

### PRÍSTUPNOSŤ

- Ikona v dostatočne viditeľnej veľkosti.
- Sprievodný štítok jednoduchým jazykom, bez žargónu, mätúcich formulácií a bez skratiek okrem „AI“.
- Čitateľnosť asistenčnými technológiami – alternatívny text alebo označenia ARIA, ktoré naznačujú, že obsah je vytvorený alebo upravený AI.
- Ak sa označenie zobrazuje len obmedzený čas, musí zostať viditeľné dosť dlho, aby ho stihli prečítať aj používatelia s kognitívnymi ťažkosťami.
- Ak sa po kliknutí na ikonu zobrazujú ďalšie informácie o použití AI, musí byť zjavné, že ikona je klikateľná. Zobrazené informácie musia byť prístupné aj osobám používajúcim čítačku obrazovky alebo ovládanie pomocou klávesnice.

### LICENCIA

Ikony sú verejne dostupné na voľné použitie bez toho, aby bolo potrebné uvádzať Európsku komisiu alebo Úrad pre umelú inteligenciu. Signatári Kódexu postupov ich však majú používať v súlade so špecifikáciami umiestnenia. Použitie ikon subjektom, ktorý signatárom Kódexu nie je, sa nemá vykladať ako signál, že Kódex dodržiava.

## KTO TO BUDE NA SLOVENSKU DOZOROVAŤ

Slovensko zatiaľ nemá schválený vykonávací zákon k AI Actu ani formálne určený dozorný orgán. MIRRI predložilo integrovaný návrh zákona koncom januára 2026; pripomienkové konanie prinieslo stovky pripomienok a návrh je vo fáze vyhodnocovania.

Otvorená zostáva aj základná otázka, kto bude hlavným dozorným orgánom. Zvažuje sa buď MIRRI ako jednotné kontaktné miesto. Popri hlavnom dozore majú mať kompetencie sektorové orgány – Úrad na ochranu osobných údajov, Národný bezpečnostný úrad, Slovenská obchodná inšpekcia, ŠÚKL, Národná banka Slovenska pre finančný sektor a Úrad pre normalizáciu ako notifikačný orgán.

Absencia určeného orgánu nemá vplyv na platnosť povinností. AI Act je nariadenie a uplatňuje sa priamo. Praktický dôsledok je len ten, že vymáhací aparát sa na Slovensku buduje s odstupom. Na dozorný orgán však nečakajú ani nároky poškodených osôb, ani požiadavky odberateľov v tendrach a dodávateľských auditoch – a pri sporoch o zodpovednosť za výrobok od decembra 2026 už vôbec nie.

## ČO PRÍDE V ROKOCH 2027 A 2028

Od 2. decembra 2027 nastupujú povinnosti pri samostatných vysokorizikových systémoch podľa prílohy III. Ak takýto systém iba používate, budete musieť najmä:

- používať systém v súlade s návodom poskytovateľa;
- zabezpečiť ľudský dohľad osobou, ktorá má na to potrebnú spôsobilosť, právomoc a podporu;
- monitorovať prevádzku systému a uchovávať automaticky generované logy;
- pred nasadením systému informovať zamestnancov a ich zástupcov, ak sa systém bude používať na pracovisku;
- informovať osoby, o ktorých systém rozhoduje alebo pomáha rozhodovať, že sa na ne takýto systém používa;

- oznamovať poskytovateľovi a orgánom závažné incidenty a riziká.

Od 2. augusta 2028 sa príslušné povinnosti začnú uplatňovať aj na vysokorizikové AI systémy zabudované do regulovaných výrobkov podľa prílohy I – napríklad do zdravotníckych pomôcok, výťahov, hračiek alebo rádiových zariadení.

Popri tom možno očakávať ďalšie vodidlá: harmonizované technické normy, ďalšie usmernenia Komisie a slovenský vykonávací zákon s určením dozorných orgánov a sankčného rámca.

## PRIENIK S GDPR: DPIA A FRIA

AI Act GDPR nenahrádza. Ak AI systém spracúva osobné údaje – čo je pri HR, marketingu a zákazníckej podpore takmer pravidlom – platia obe úpravy súčasne. V praxi to znamená dva posudzovacie dokumenty, ktoré sa oplatí robiť naraz.

### DPIA (DATA PROTECTION IMPACT ASSESSMENT) – POSÚDENIE VPLYVU NA OCHRANU ÚDAJOV

Vyplyva z čl. 35 GDPR a nie je novinkou. Nasadenie AI do náboru, hodnotenia zamestnancov, úverového rozhodovania alebo profilovania zákazníkov však povinnosť DPIA takmer vždy vyvolá, keďže ide o systematické a rozsiahle vyhodnocovanie osobných aspektov s právnymi alebo podobne významnými účinkami.

### FRIA (FUNDAMENTAL RIGHTS IMPACT ASSESSMENT) – POSÚDENIE VPLYVU NA ZÁKLADNÉ PRÁVA

Je nové posúdenie podľa čl. 27 AI Actu a v slovenskej diskusii sa jej venuje málo pozornosti. Povinnosť sa síce nevzťahuje na každého, ale okruh je širší, než sa na prvý pohľad zdá. Vzťahuje sa na:

- Subjekty verejného práva a súkromné subjekty poskytujúce verejné služby (napr. v oblasti vzdelávania, zdravotnej starostlivosti, sociálnych služieb alebo sociálneho bývania), ak nasadzujú vysokorizikový systém podľa prílohy III, s výnimkou systémov používaných v oblasti kritickej infraštruktúry,
- Ktorýkoľvek prevádzkovateľ systémov na posudzovanie úverovej bonity alebo určovanie úverového skóre fyzických osôb, s výnimkou systémov používaných na odhaľovanie finančných podvodov a na posudzovanie rizika a stanovovanie cien v životnom a zdravotnom poistení – bez ohľadu na to, či ide o verejný alebo súkromný subjekt.

FRIA sa vykonáva pred prvým nasadením systému a jej výsledky sa oznamujú orgánu dohľadu. Nejde o jednorazový dokument – ak sa systém podstatne zmení alebo sa pretrénuje, FRIA sa musí aktualizovať.

**Kľúčová úspora:** ak už máte k danému spracúvaniu vypracované DPIA, čl. 27 ods. 4 AI Actu umožňuje, aby FRIA na DPIA nadviazala a dopĺňala ju. Nie je potrebné písať dva nezávislé dokumenty od nuly. Platí to však len vtedy, ak sa DPIA a FRIA pripravujú koordinovane – nie keď ich robia dve oddelenia, ktoré o sebe nevedia.

### V ČOM SA DPIA A FRIA LÍŠIA

DPIA sa pýta na údaje: čo zbierate, za akým účelom, ako to uchováate a či je spracúvanie zákonné.

FRIA sa pýta na ľudí: ktoré základné práva systém ovplyvňuje, kto je jeho rozhodnutiami dotknutý, čo sa stane, keď sa systém pomýli, a či má dotknutá osoba reálnu možnosť rozhodnutie napadnúť.

DPIA a FRIA sa preto môžu čiastočne prekrývať, ale nejde o totožné posúdenia.

Povinnosť vypracovať FRIA podľa článku 27 sa pri vysokorizikových systémoch podľa prílohy III začne uplatňovať 2. decembra 2027. Na systémy uvedené na trh alebo do prevádzky pred týmto dátumom sa nové povinnosti spravidla uplatnia iba vtedy, ak po 2. decembri 2027 významne zmení spôsob ich fungovania, účel alebo technické riešenie. Pri vysokorizikových systémoch určených na používanie orgánmi verejnej moci musí byť súlad zabezpečený najneskôr do 2. augusta 2030.

## SANKCIE

- **Porušenie zakázaných postupov podľa článku 5 AI Act:** pokuta až do 35 miliónov EUR alebo 7 % celosvetového ročného obratu za predchádzajúci finančný rok.
- **Porušenie ostatných povinností vrátane povinností transparentnosti podľa čl. 50 AI Act:** pokuta až do 15 miliónov EUR alebo 3 % celosvetového ročného obratu za predchádzajúci finančný rok.

Popri pokutách však treba počítať s dôsledkami, ktoré bývajú v praxi citeľnejšie: zákaz uvádzania systému na trh alebo stiahnutie z prevádzky, nároky dotknutých osôb, reputačné dopady a – od decembra 2026 – nároky z náhrady škody podľa nového režimu zodpovednosti za výrobok.

### ČO TIE ČÍSLA ZNAMENAJÚ PRE BEŽNÚ SLOVENSKÚ FIRMU

Uvedené sumy sú horné hranice pre najzávažnejšie porušenia, nie sadzobník. Pokuta musí byť účinná, primeraná a odrádzajúca a prihliada sa na veľkosť podniku, závažnosť a úmysel. Pri podnikoch, ktoré nie sú malými alebo strednými podnikmi, sa ako horná hranica použije vyššia z uvedených súm. Pri malých a stredných podnikoch vrátane startupov sa použije nižšia hranica.

Dnes, v auguste 2026: Slovensko nemá schválený vykonávací zákon ani určený dozorný orgán. To môže ovplyvniť praktickú rýchlosť a spôsob kontroly, neodkladá to však povinnosti AI Actu, ktoré sa už uplatňujú. Po schválení zákona a určení príslušných orgánov možno očakávať postupné rozvíjanie kontrolnej praxe.

Po schválení slovenského vykonávacieho zákona a vytvorení funkčného systému dohľadu sa bude kontrolná prax postupne rozvíjať. Organizácie, ktoré si už teraz nastavujú pravidlá používania AI, určujú zodpovedné osoby a pripravujú potrebnú dokumentáciu, sa môžu vyhnúť neskorším časovo aj finančne náročnejším úpravám.

Niektoré následky môžu vzniknúť nezávisle od kontroly dozorného orgánu. Môže ísť napríklad o nárok poškodenej osoby, nárok zamestnanca alebo uchádzača, vypadnutie z tendra kvôli nezodpovedanému dotazníku a zmluvná požiadavka odberateľa z finančného sektora.

Kybernetická bezpečnosť sa často vníma ako technická agenda IT oddelenia. Regulačne však ide o tri samostatné predpisy s odlišnou logikou, odlišným okruhom povinných osôb a odlišnými termínmi. Firma môže spadať pod jeden, dva aj všetky tri naraz.

### TRI PREDPISY, TRI ODLIŠNÉ ROVINY

- **Cyber Resilience Act** rieši bezpečnosť výrobu. Týka sa toho, kto uvádza na trh softvér alebo pripojené zariadenia.
- **Zákon o kybernetickej bezpečnosti (transpozícia NIS2)** rieši odolnosť organizácie. Týka sa najmä firiem pôsobiach v regulovaných sektoroch, spravidla od určitej veľkosti.
- **DORA** rieši digitálnu prevádzkovú odolnosť finančného sektora a nepriamo, najmä prostredníctvom zmluvných požiadaviek, aj jeho dodávateľov služieb informačných a komunikačných technológií.

### CYBER RESILIENCE ACT: BEZPEČNOSŤ VÝROBKU

CRA (nariadenie (EÚ) 2024/2847) je prvý celoeurópsky predpis, ktorý stanovuje povinné požiadavky na kybernetickú bezpečnosť výrobkov s digitálnymi prvkami – teda hardvéru aj softvéru – počas celého ich životného cyklu. Nadobudol účinnosť 10. decembra 2024. Pre väčšinu firiem sú najdôležitejšie dve etapy jeho uplatňovania.

#### NAJBLIŽŠÍ TERMÍN: 11. SEPTEMBER 2026

Od tohto dňa platia ohlasovacie povinnosti. Výrobcovia musia hlásiť aktívne zneužívané zraniteľnosti a závažné incidenty, ktoré majú vplyv na bezpečnosť produktu. V oboch prípadoch sa podáva včasné varovanie do 24 hodín a následné oznámenie do 72 hodín. Pri aktívne zneužívanej zraniteľnosti sa záverečná správa podáva najneskôr do 14 dní od sprístupnenia nápravného alebo zmierňujúceho opatrenia. Pri závažnom incidente sa podáva do jedného mesiaca od 72-hodinového oznámenia.

**Kľúčový detail:** ohlasovacia povinnosť sa vzťahuje aj na produkty, ktoré sú na trhu už dnes, nielen na nové. Firma, ktorá sa sústreďí len na termín v roku 2027, bude v omeškaní viac než rok.

#### PLNÁ UPLATNITEĽNOSŤ: 11. DECEMBER 2027

Od tohto dňa musia nové výrobky uvádzané na trh spĺňať podstatné kyberneticko-bezpečnostné požiadavky – bezpečnosť už v návrhu, bezpečné predvolené nastavenia, poskytovanie bezpečnostných aktualizácií počas deklarovaného podporného obdobia, súpis komponentov softvéru a proces riadenia zraniteľností. Pripája sa posudzovanie zhody a CE označenie.

Na výrobky uvedené na trh pred 11. decembrom 2027 sa tieto požiadavky uplatnia iba vtedy, ak po tomto dátume prejdú podstatnou zmenou. Ohlasovacie povinnosti sa však na staršie výrobky vzťahujú už od 11. septembra 2026.

Komisia zverejnila 27. júla 2026 praktické usmernenie, ktoré spresňuje najmä rozsah pôsobnosti pri softvérových produktoch, náhradných dieloch, podstatných zmenách, podporných obdobiach a ohlasovacích povinnostiach.

### SME SAAS FIRMA – TÝKA SA NÁS CRA?

Toto je pre slovenský softvérový sektor otázka číslo jedna a odpoveď nie je taká, akú väčšina firiem čaká. Kľúčové je posudzovať každý produkt samostatne a zároveň určiť postavenie firmy vo vzťahu k nemu. Jedna firma môže mať čisto hostovanú službu mimo pôsobnosti CRA a súčasne inštalovateľnú aplikáciu, na ktorú sa CRA vzťahuje. Hostovaná časť však môže byť za určitých podmienok súčasťou regulovaného produktu.

#### KDE VEDIE HRANICU JÚLOVÉ USMERNENIE KOMISIE

- **Softvér, ktorý beží na zariadení používateľa** – napr. stiahnuteľná aplikácia, mobilná aplikácia z obchodu, rozšírenie prehliadača, lokálne inštalovaný klient, on-premise inštalácia alebo agent – spravidla je výrobkom s digitálnymi prvkami, ak sa sprístupňuje na trhu v rámci obchodnej činnosti.
- **Webová aplikácia používaná výlučne cez prehliadač** ani informačná webová stránka spravidla nie sú výrobkom s digitálnymi prvkami. Samotný prístup cez prehliadač však automaticky neznamená, že služba je mimo CRA – jej cloudová časť môže byť súčasťou iného výrobku s digitálnymi prvkami.

#### TROJSTUPŇOVÝ TEST PRI CLOUDOVEJ ČASŤI PRODUKTU

Cloudová alebo serverová časť sa stáva súčasťou výrobku vtedy, keď sú splnené všetky tri podmienky súčasne:

- spracovanie údajov prebieha na diaľku – vo verejnom cloude, v privátnom cloude alebo na serveroch výrobcu;
- bez tohto spracovania by výrobok nedokázal plniť niektorú zo svojich funkcií;
- softvér navrhol a vyvinul výrobca alebo bol vyvinutý na jeho zodpovednosť.

Ak sú splnené všetky tri podmienky, cloudová časť patrí do posudzovania rizika, technickej dokumentácie aj posudzovania zhody. Ak splnené nie sú, cloudová časť sa nepovažuje za súčasť tohto výrobku; jej právne postavenie však treba posúdiť samostatne.

**Ak ste teda mimo CRA, znamená to pokoj?** Nie nevyhnutne. Poskytovanie SaaS môže predstavovať poskytovanie cloudovej služby podľa NIS2 a slovenského zákona o kybernetickej bezpečnosti. Neplatí to však automaticky pre každú SaaS firmu – treba posúdiť charakter služby, veľkosť podniku a ďalšie zákonné podmienky. CRA a zákon o kybernetickej bezpečnosti preto treba posudzovať samostatne.

### PRAKTICKÝ POSTUP PRE SOFTVÉROVÚ FIRMU

Nerobte jedno posúdenie za firmu. Urobte zoznam artefaktov, ktoré dodávate: hostovaná služba, mobilná aplikácia, on-premise edícia, agent, SDK, rozšírenie. Pri každom si odpovedzte, kde beží. To je prvá deliaca čiara. Pri každom produkte, ktorý spadá pod CRA, si zistíte, kto má ktorú verziu – pri vydaní opravy to budete potrebovať.

Súbežne si overte postavenie podľa zákona o kybernetickej bezpečnosti. Pri softvérových a cloudových firmách je to bežné.

## NIS2 A ZÁKON O KYBERNETICKEJ BEZPEČNOSTI: ODOLNOSŤ ORGANIZÁCIE

Smernica NIS2 bola na Slovensku transponovaná zákonom č. 366/2024 Z. z., ktorým sa novelizoval zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti. Novela nadobudla účinnosť 1. januára 2025 a od 1. septembra 2025 ju dopĺňa vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach.

### KOHO SA TÝKA

Okruh povinných subjektov sa oproti predchádzajúcej úprave výrazne rozšíril. Rozhoduje najmä kombinácia sektora, veľkosti podniku a typu poskytovanej služby. Pri niektorých službách sa veľkosť podniku neposudzuje. Ak pôsobíte v niektorom z regulovaných sektorov – energetika, doprava, zdravotníctvo, IT služby, výroba, potravinárstvo a ďalšie – je namieste overiť si postavenie prevádzkovateľa základnej služby. NBÚ na tento účel prevádzkuje orientačný nástroj; výsledok však nenahrádza vlastné právne posúdenie.

### HLAVNÉ POVINNOSTI

- Registrácia – overiť si postavenie prevádzkovateľa základnej služby a podať oznámenie NBÚ.
- Bezpečnostné opatrenia podľa vyhlášky č. 227/2025 Z. z.
- Manažér kybernetickej bezpečnosti – určený interne alebo externe.
- Hlásenie závažných incidentov v trojstupňovom režime: včasné varovanie do 24 hodín, oznámenie do 72 hodín, záverečná správa do jedného mesiaca.
- Hlásenie významných kybernetických hrozieb, udalostí odvrátených v poslednej chvíli a zraniteľností verejne dostupných systémov, ktoré nemožno včas odstrániť.
- Audit kybernetickej bezpečnosti v zákonnej lehote od zápisu do registra. Subjekty, ktoré neprevádzkujú kritickú základnú službu, môžu v prvej lehote využiť samohodnotenie, auditu certifikovaným audиторom sa však napokon nevyhnú.

Za nesplnenie povinností môže NBÚ ukladať pokuty; sankcionovaní môžu byť podľa zákona aj priamo jednotlivci, napríklad štatutári alebo manažéri kybernetickej bezpečnosti.

**Dôraz na vedenie:** NIS2 kladie zodpovednosť za kybernetickú bezpečnosť výslovne na vrcholový manažment. Nejde o agendu, ktorú možno v celom rozsahu delegovať na IT.

## DORA: FINANČNÝ SEKTOR A JEHO DODÁVATELIA

DORA (nariadenie (EÚ) 2022/2554) sa uplatňuje od 17. januára 2025 a zjednocuje pravidlá pre riadenie rizík informačných a komunikačných technológií vo finančnom sektore. Pokrýva päť oblastí: riadenie IKT rizika, riadenie a hlásenie incidentov, testovanie digitálnej prevádzkovej odolnosti, riadenie rizika IKT tretích strán a dobrovoľné zdieľanie informácií o kybernetických hrozbách.

Pôsobnosť je široká – od úverových inštitúcií, platobných inštitúcií a inštitúcií elektronických peňazí cez investičné spoločnosti a poisťovne až po poskytovateľov služieb kryptoaktív a služieb hromadného financovania.

### ČO Z DORA PLYNIE PRE DODÁVATEĽOV

Finančné subjekty môžu uzatvárať zmluvy o IKT službách len s poskytovateľmi, ktorí spĺňajú primerané normy informačnej bezpečnosti. Ak sa zmluva týka kritických alebo dôležitých funkcií, finančný subjekt musí pred jej uzavretím náležite posúdiť, ako poskytovateľ uplatňuje najaktuálnejšie normy kvality v oblasti informačnej bezpečnosti.

Nariadenie navyše zavádza úniový dohľad nad poskytovateľmi IKT služieb tretej strany, ktorých európske orgány dohľadu označia za kritických. Bežní poskytovatelia podliehajú požiadavkám DORA najmä nepriamo, prostredníctvom zmlúv s finančnými subjektmi. To platí aj pre poskytovateľov mimo EÚ. Ak je však poskytovateľ mimo EÚ označený za kritického, musí do 12 mesiacov zriadiť dcérsku spoločnosť v Únii, inak finančné subjekty v EÚ jeho služby nemôžu využívať.

## NIE STE V PÔSOBNOSTI? AJ TAK SA VÁS TO DOTKNE.

Toto je najčastejšie prehliadaný mechanizmus celej kybernetickej regulácie. NIS2 aj DORA sa k dodávateľom dostávajú nepriamo – cez zmluvy.

- Banka alebo poisťovňa premietne požiadavky DORA do zmluvy s dodávateľom IT služieb, vrátane práv na audit, oznamovacích povinností a požiadaviek na testovanie.
- Prevádzkovateľ základnej služby robí to isté podľa zákona o kybernetickej bezpečnosti; slovenská úprava navyše osobitne upravuje postavenie tretích strán s významným vplyvom na zabezpečovanie kybernetickej bezpečnosti.

Firma, na ktorú sa DORA alebo zákon o kybernetickej bezpečnosti priamo nevzťahuje, tak môže dostať vybrané bezpečnostné požiadavky prostredníctvom zmluvy. Môže ísť napríklad o oznamovanie incidentov, spoluprácu pri testovaní, pravidlá subdodávok, kontinuitu služieb a práva na kontrolu a audit. Pri službách podporujúcich kritické alebo dôležité funkcie sú zmluvné požiadavky podstatne prísnejšie.

Dodávateľ ich pritom musí splniť v lehote dohodnutej so zákazníkom. Pre poskytovateľov softvéru je preto pripravenosť na tieto požiadavky obchodnou otázkou aj vtedy, keď sami nepatria do priamej pôsobnosti DORA.

## HLÁSENIE INCIDENTOV: POZRITE SI NUTSHELL

Prehľad toho, ktoré hlásenie sa uplatní, komu sa podáva a v akých lehotách, nájdete v tabuľke „Jeden incident, štyri hlásenia“ na druhej strane Nutshellu v úvode tejto brožúry. Je to strana, ktorú odporúčame vytlačiť a mať po ruke.

Podstata sa dá zhrnúť jednou vetou: jediná udalosť môže spustiť niekoľko oznamovacích povinností súčasne, s rôznymi adresátmi a rôznymi lehotami. Pri DORA môže byť potrebné podať prvotné oznámenie už do 4 hodín od klasifikácie incidentu ako závažného; pri ostatných uvedených režimoch je najkratšia základná lehota 24 hodín.

## PREČO KYBERNETICKÁ BEZPEČNOSŤ A AI PATRIA K SEBE

Prepojenie nie je len tematické. Je priamo právne.

- AI systém môže byť súčasne výrobkom s digitálnymi prvkami podľa CRA. Jeden produkt tak môže spadať pod oba predpisy naraz.
- Nový režim zodpovednosti za výrobok výslovne pokrýva chyby vzniknuté po uvedení na trh vrátane oblasti kyberneticko-bezpečnostných aktualizácií. Zanedbaná aktualizácia sa tak môže stať vadou výrobku.
- Ak poškodený preukáže, že výrobok nespĺňal povinné požiadavky na bezpečnosť určené na ochranu pred rizikom, ktoré spôsobilo konkrétnu škodu, predpokladá sa, že výrobok bol vadný. Ide však o vyvrátiteľnú domnienku.
- Logy a záznamy, ktoré vznikajú kvôli kybernetickej bezpečnosti, sa môžu čiastočne prekryvať so záznamami, ktorými sa preukazuje riadne používanie AI systému.

## AK PÔSOBÍTE VO VIACERÝCH ČLENSKÝCH ŠTÁTOCH

Táto brožúra vychádza zo slovenskej právnej úpravy. Ak má vaša firma pobočky, predaj alebo dodávateľov v iných členských štátoch, jeden rozdiel je podstatný a v praxi sa naň zabúda.

- **AI Act, CRA a DORA sú nariadenia.** Platia priamo a v rovnakom znení vo všetkých členských štátoch. Líšia sa však dozorné orgány, vnútroštátne postupy a národné sankčné konania.
- **NIS2 je smernica.** Každý členský štát ju transponuje vlastným zákonom. Okruh povinných subjektov, vnútroštátne postupy a sankcie sa preto môžu líšiť a niektoré štáty môžu zaviesť aj prísnejšie požiadavky.
- **Aj nový režim zodpovednosti za výrobok vychádza zo smernice, tá však zavádza prevažne úplnú harmonizáciu.** Základné pravidlá zodpovednosti by preto mali byť v členských štátoch rovnaké, hoci procesné pravidlá a spôsob ich uplatnenia pred súdmi sa môžu líšiť.

Praktický dôsledok: súlad dosiahnutý na Slovensku nie je automaticky súladom v Českej republike, Rakúsku alebo Poľsku. Pri skupinách firiem odporúčame nastaviť spoločný rámec governance a k nemu národné dodatky, nie päť samostatných riešení.

Popri AI Acte a kybernetickej regulácii prichádza tretia zmena, ktorá zatiaľ zostáva v tieni – a pre mnohé firmy bude mať väčší praktický dopad. Ide o smernicu (EÚ) 2024/2853 o zodpovednosti za chybné výrobky, ktorá nahrádza úpravu z roku 1985. Keďže ide o smernicu, jej pravidlá sa musia najprv premietnuť do slovenského práva. Členské štáty sú povinné prijať potrebnú právnu úpravu najneskôr do 9. decembra 2026.

Nejde o „ďalšiu AI reguláciu“. Ide o modernizáciu klasickej objektívnej zodpovednosti za vadný výrobok – teda zodpovednosti, pri ktorej poškodený nemusí preukazovať zavinenie výrobcu.

## ČO SA MENÍ

- **Softvér je výrobok.** Za výrobok sa po novom výslovne považuje aj softvér bez ohľadu na spôsob jeho poskytovania – teda aj softvér dostupný cez cloud alebo ako služba (SaaS). Výrobkom je tiež digitálny výrobný súbor a surovina. Do režimu zodpovednosti za výrobok sa tak dostávajú AI systémy aj produkty s AI funkciami. Samotná informácia alebo obsah vytvorený AI však výrobkom automaticky nie sú.
- **Výnimka.** Režim sa nevzťahuje na slobodný a otvorený softvér vyvíjaný alebo dodávaný mimo obchodnej činnosti.
- **Rozhodujúci je dátum uvedenia na trh.** Nový režim sa vzťahuje na výrobky uvedené na trh alebo do prevádzky od 9. decembra 2026. Ak je starší výrobok po tomto dátume podstatne zmenený a následne znovu uvedený na trh alebo do prevádzky, považuje sa za nový výrobok. Podstatná zmena môže vzniknúť aj aktualizáciou softvéru alebo ďalším učením AI systému.

## JADRO REFORMY: DOKAZOVANIE

Pri klasickom výrobku je reťazec dokazovania predstaviteľný: brzda mala vadu, vozidlo nezabrzdilo, vznikla škoda. Pri AI systéme má poškodený spravidla nulovú možnosť zistiť, čo sa vo vnútri systému odohralo. Nová úprava túto asymetriu rieši dvoma nástrojmi.

### SPRÍSTUPNENIE DŮKAZOV

Ak žalobca predloží skutočnosti a dôkazy postačujúce na podporu vierohodnosti nároku, súd môže žalovanému nariadiť, aby sprístupnil relevantné dôkazy, ktoré má k dispozícii. Sprístupnenie musí byť nevyhnutné a primerané a súd je povinný chrániť dôverné informácie a obchodné tajomstvo.

### VYVRÁTITELNÉ DOMNIENKY

- Ak žalovaný príkaz na sprístupnenie nesplní, nastupuje domnienka vadnosti výrobku.
- Domnienka vadnosti nastupuje aj vtedy, ak žalobca preukáže, že výrobok nespĺňal povinné bezpečnostné požiadavky, určené na ochranu pred rizikom, ktoré spôsobilo konkrétnu škodu.
- Ak je pre žalobcu z dôvodu technickej alebo vedeckej zložitosti nadmerne obtiažne preukázať vadnosť alebo príčinnú súvislosť, uplatní sa domnienka aj tu. Nestačí však konštatovať, že „AI je black box“ – žalobca musí preukázať aspoň pravdepodobnosť vadnosti alebo kauzality.

Všetky domnienky sú vyvrátiteľné. Dôkazné bremeno však nesie žalovaný, pričom kvalitná technická dokumentácia, logy a záznamy o vývoji, testovaní a aktualizáciách môžu mať rozhodujúci význam.

## KTO ZODPOVEDÁ A ZA AKÚ ŠKODU

### ROZŠÍRENÝ OKRUH ZODPOVEDNÝCH

- Výrobca výrobku a výrobca chybného komponentu. Ak je výrobca usadený mimo EÚ, zodpovednosť môže za zákonných podmienok niesť aj dovozca, splnomocnený zástupca alebo poskytovateľ logistických služieb. Za určitých podmienok môže zodpovedať aj distribútor alebo online platforma.
- Za výrobcu sa môže považovať aj ten, kto výrobok podstatne zmenil mimo kontroly pôvodného výrobcu a následne ho uviedol na trh alebo do prevádzky.
- Režim dopadá aj na dodávateľov z tretích krajín, ktorí uvádzajú výrobok na trh EÚ.

### ROZŠÍRENÝ ROZSAH ŠKODY

- Smrť a poškodenie zdravia vrátane medicínsky uznaného poškodenia psychického zdravia.
- Majetková škoda – ruší sa doterajší minimálny finančný limit 500 €.
- Zničenie alebo poškodenie údajov, ak nejde o údaje používané na profesionálne účely.

**Dôležité:** zodpovednosť za škodu spôsobenú vadným výrobkom nemožno voči poškodenému vopred zmluvne vylúčiť ani obmedziť.

## STAV NA SLOVENSKU

K 7. augustu 2026 transpozícia ešte nie je dokončená, legislatívny proces je však v pokročilom štádiu.

- Vláda SR schválila návrh zákona 8. apríla 2026. Ide o úplne nový zákon z dielne Ministerstva hospodárstva SR, ktorý nahradí zákon č. 294/1999 Z. z.
- Národná rada SR posunula návrh 2. júna 2026 do druhého čítania.
- Navrhovaná účinnosť je 9. december 2026, s pôsobnosťou na výrobky uvedené na trh alebo do prevádzky od tohto dátumu.
- Návrh rozširuje definíciu výrobku o softvér a digitálne výrobné súbory, zavádza pojmy komponent a súvisiaca služba, ruší doterajšiu hranicu 500 € pri škode na majetku, rozširuje náhradu škody o medicínsky uznané poškodenie psychického zdravia a škodu na údajoch, predlžuje lehotu pri neskoro sa prejavujúcej ujme na zdraví až na 25 rokov a rozširuje okruh zodpovedných subjektov.

Keďže je návrh v druhom čítaní, jeho znenie sa ešte môže zmeniť. Termín 9. decembra 2026 však vyplýva priamo zo smernice a je nezávislý od rýchlosti slovenského legislatívneho procesu.

## POISTENIE: OTÁZKA, KTORÚ TREBA POLOŽIŤ TERAZ

Keďže zodpovednosť za škodu spôsobenú vadným výrobkom nemožno voči poškodenému zmluvne vylúčiť ani obmedziť, poistenie zostáva jediným nástrojom, ktorým firma toto riziko reálne prenáša. Práve tu je však najväčšia medzera.

Staršie poisťné podmienky môžu vychádzať z tradičného chápania výrobku ako hmotnej veci. Preto odporúčame s maklérom alebo poisťovňou prejsť tri otázky:

- **Kryje poisťka softvér ako výrobok?** A to nielen ako súčasť dodaného zariadenia, ale samostatne dodávaný softvér alebo AI systém.
- **Kryje nové kategórie škody?** Zničenie alebo poškodenie údajov a medicínsky uznané poškodenie psychického zdravia staršie poisťné podmienky nemusia pokrývať alebo ich môžu zaraďovať do iného druhu poistenia.
- **Kryje poisťka aj nároky uplatnené s veľkým časovým odstupom?** Pri neskoro sa prejavujúcej ujme na zdraví počítá slovenský návrh zákona na zániku práva s lehotou až 25 rokov. To je horizont, ktorý presahuje bežné poisťné programy aj obvyklú archiváciu dokumentácie.

Zároveň je vhodné preveriť, či poistenie kryje aj náklady na právne zastúpenie v konaní, znalcov a technických expertov v spore, v ktorom môže byť firma povinná sprístupniť technické dôkazy. Dôležité je aj to, či sa tieto náklady započítavajú do poisťného limitu a či ich vynaloženie podlieha predchádzajúcemu súhlasu poisťovne.

## AKO DLHO UCHOVÁVAŤ LOGY: GDPR VERZUS DÔKAZNÁ POZÍCIA

Na prvý pohľad tu stojí protirečenie. Nový režim zodpovednosti za výrobok umožňuje súdu nariadiť sprístupnenie dôkazov a za určitých podmienok zavádza vyvrátiteľné domnienky vadnosti alebo príčinnej súvislosti. Bez záznamov firma nevyvráti domnienku vadnosti, a lehoty na uplatnenie nároku siahajú pri neskoro sa prejavujúcej ujme na zdraví až do 25 rokov. GDPR naopak vyžaduje minimalizáciu údajov a ich uchovávanie len po dobu nevyhnutnú na daný účel. IT oddelenie sa oprávnené pýta, ktorá povinnosť platí.

Protirečenie to však nie je. GDPR nezakazuje dlhé uchovávanie – vyžaduje, aby preň existoval doložitelný účel. A uplatnenie, výkon alebo obhajoba právnych nárokov je uznaným účelom, ktorý dlhšie uchovávanie odôvodňuje.

### AKO TO NASTAVIŤ

- **Rozlíšte, čo naozaj potrebujete.** Dôkaznú hodnotu môžu mať najmä verzie modelu, konfigurácia, testovacie a validačné záznamy, záznamy o ľudskom dohľade a história incidentov. Spravidla nie je potrebné uchovávať kompletne prevádzkové logy so všetkými osobnými údajmi.
- **Oddel'te dva režimy.** Krátka prevádzková retencia pre bežné logy a dlhšia archívna retencia pre úzko vymedzený dôkazný súbor. To je zásadný rozdiel oproti tomu, keď sa všetko uchováva dlho pre istotu.
- **Minimalizujte, čo archivujete.** Tam, kde stačí pseudonymizovaný alebo agregovaný záznam, nie je dôvod archivovať priame identifikátory.
- **Obmedzte prístup.** Archív určený na obhajobu nároku nemá byť bežne prístupný prevádzke.
- **Zdokumentujte rozhodnutie.** V záznamoch o spracovateľských činnostiach uveďte predpokladané lehoty na vymazanie, ak je to možné. Podrobné odôvodnenie dlhšej retencie zachyťte v retenčnej politike a podľa okolností aj v posúdení oprávneného záujmu alebo DPIA. Samotné zdokumentovanie však ešte nezákonné uchovávanie údajov neurobí zákonným.

**Zhrnuté:** otázka neznie iba „dlho alebo krátko“, ale „čo presne, kde, kto k tomu má prístup a prečo“. Toto je typicky rozhodnutie, ktoré musí padnúť spoločne – nie samostatne v IT a samostatne u zodpovednej osoby pre ochranu údajov.

## KDE SA TO SPÁJA S AI GOVERNANCE

Najdôležitejšia myšlienka tejto brožúry nie je veta „AI je výrobok“. Je to kombinácia troch prvkov:

- AI Act vyžaduje najmä pri vysokorizikových systémoch technickú dokumentáciu, logy a záznamy súvisiace s ľudským dohľadom. Kybernetická regulácia k tomu pridáva bezpečnostnú dokumentáciu a záznamy o zraniteľnostiach a incidentoch;
- nová úprava zodpovednosti môže z tejto dokumentácie urobiť dôležitý dôkazný materiál v civilnom spore;
- Ak žalovaný napriek príkazu súdu nesprístupní relevantné dôkazy, ktorými disponuje, vzniká za zákonných podmienok domnienka vadnosti výrobku. Chýbajúca dokumentácia sama osebe túto domnienku nezakladá, môže však výrazne oslabiť dôkaznú pozíciu firmy.

AI Governance sa tým presúva z roviny „regulatory compliance“ do roviny „litigation readiness“. To, čo dnes vyzerá ako administratívna povinnosť, môže neskôr významne ovplyvniť výsledok sporu.

Praktický dôsledok je nenápadný, ale podstatný: retenčné lehoty pre logy, verzie modelov a testovacie záznamy by sa mali nastavovať nie podľa toho, ako dlho ich potrebuje IT, ale podľa toho, ako dlho môže byť voči firme uplatnený nárok.

## PREČO JEDEN SYSTÉM A NIE PÄŤ PROJEKTOV

Firma, ktorá si päť predpisov rozdelí na päť samostatných projektov, urobí tú istú prácu päťkrát a napriek tomu jej ostanú medzery na styčných plochách. Register nástrojov, klasifikácia rizika, ľudský dohľad, logy, incident proces a zmluvná dokumentácia s dodávateľmi sú prvky, ktoré si vyžaduje viac než jeden z týchto predpisov.

AI Governance je súbor pravidiel, rolí a záznamov, ktorými firma riadi, ako sa u nej AI a digitálne nástroje používajú. Nie je to technologický projekt ani jeden dokument v šuflíku. Je to prevádzkový systém, ktorý odpovedá na štyri otázky: čo používame, na čo to používame, kto za to zodpovedá a ako to vieme späťne doložiť.

Kým regulácia stanovuje hranice, Governance je jediné, čím ich firma vie reálne ustrážiť – a jediné, čím ich vie preukázať.

## SEDEM DÔVODOV, PREČO TO DÁVA ZMYSEL AJ BEZ REGULÁCIE

### 1. BEZ PREHLADU NEVIETE, ČO SA U VÁS DEJE

Prax je konzistentná: reálne používanie AI vo firmách výrazne presahuje to, čo bolo formálne schválené. Zamestnanci používajú nástroje, ktoré si zaviedli sami, často do nich vkladajú citlivé podklady a firma o tom nevie. Prvý krok Governance – jednoduchý register – býva zároveň prvým momentom, keď vedenie vidí skutočný obraz.

### 2. OCHRANA OBCHODNÉHO TAJOMSTVA A DÔVERNÝCH INFORMÁCIÍ

Vloženie zmluvy, cenníka, klientskeho zoznamu alebo interného rozpočtu do nevhodného nástroja môže ohroziť ochranu obchodného tajomstva, porušiť zmluvnú mlčanlivosť voči klientovi alebo pravidlá ochrany osobných údajov. Toto riziko nevyplýva zo žiadneho z uvedených predpisov – existuje bez ohľadu na ne.

### 3. ZA VÝSTUP ZODPOVEDÁTE VY

Ak vaša firma použije AI výstup voči klientovi, úradu alebo súdu, nemôžete sa zbaviť vlastnej zodpovednosti iba odkazom na poskytovateľa modelu. To nevylučuje prípadnú zodpovednosť dodávateľa. Riziko vzniká pri chybnom výpočte, nesprávnej informácii aj pri diskriminačnom rozhodnutí v náboře. Ľudský dohľad preto nie je len administratívna formalita, ale miesto, kde sa toto riziko zachytáva.

### 4. DUŠEVNÉ VLASTNÍCTVO

Pri AI výstupoch treba riešiť dve samostatné otázky: či vôbec vzniká chránené dielo a či výstup neporušuje práva tretích osôb. Bez pravidiel a záznamov o tom, ako výstup vznikol, nie je ani jedno preukázateľné.

### 5. RÝCHLOSŤ REAKCIE NA INCIDENT

Pri DORA môže byť prvé oznámenie potrebné už do 4 hodín od klasifikácie incidentu ako závažného, najneskôr však do 24 hodín od jeho zistenia. Ak sa incident klasifikuje ako závažný až neskôr, štvorhodinová lehota plyní od tejto klasifikácie. Lehoty sa často nezmeškajú pre chýbajúcu právnu analýzu, ale preto, že incident nikto včas nezachytil alebo nevedel, komu ho eskalovať. Toto je organizačná otázka, ktorá sa rieši vopred, nie v deň incidentu.

### 6. OBCHODNÁ POŽIADAVKA KLIENTOV A ODBERATEĽOV

Dotazníky v tendroch, prílohy k rámcovým zmluvám a dodávateľské audity sa na AI Governance a kybernetickú bezpečnosť pýtajú čoraz častejšie. Vo finančnom sektore a u prevádzkovateľov základných služieb to už nie je otázka preferencie, ale zmluvná požiadavka vyplývajúca z DORA a zo zákona o kybernetickej bezpečnosti.

### 7. DÔKAZNÁ POZÍCIA PRI ZODPOVEDNOSTI ZA VÝROBOK

Dokumentácia, ktorá vzniká kvôli regulácii, sa novým režimom zodpovednosti mení na dôkazný materiál v civilnom spore. Podrobne v tretej časti tejto brožúry.

## AUTORSKÉ PRÁVO: VSTUPY AJ VÝSTUPY

Autorskoprávne riziko pri AI má dve strany a firmy spravidla vidia len jednu z nich.

### VÝSTUPNÁ STRANA

Otázka, či AI výstup je chráneným dielom a či neporušuje práva tretích osôb. Slovenský Autorský zákon vychádza z toho, že autorom môže byť len fyzická osoba – výstup bez ľudského tvorivého vstupu preto autorskoprávnu ochranu nezakladá. Ak však človek tvorivými rozhodnutiami výslednú podobu podstatne ovplyvnil, ochrana jeho tvorivého vkladu nie je vylúčená. Samostatnou otázkou je, či výstup nepreberá chránené tvorivé prvky konkrétneho cudzieho diela. Samotné napodobnenie štýlu autora spravidla nestačí.

### VSTUPNÁ STRANA

Táto strana sa v diskusii takmer nespomína, hoci je relevantná pre každú firmu, ktorá trénuje vlastný model alebo doladuje existujúci model na dátach či obsahu, ku ktorým nemá vlastné práva.

- Smernica DSM zaviedla pravidlá pre vyťažovanie textov a dát (TDM). Slovenský autorský zákon ich prevzal ako „použitie diela pri čerpaní

údajov“. Rozlišuje osobitnú výnimku na účely výskumu a všeobecnú výnimku, ktorá umožňuje vyhotoviť rozmnoženinu diela na účely čerpania údajov, ak má používateľ k obsahu zákonný prístup a nositeľ práv takéto použitie výslovne nevyhradil.

- Pri všeobecnom čerpaní údajov si nositelia práv môžu takéto použitie na účely TDM výslovne vyhraď – tzv. opt-out – a to strojovo čitateľným spôsobom, napríklad cez metadáta alebo podmienky používania webovej stránky. Ak je výhrada uplatnená, na čerpanie údajov je potrebné povolenie nositeľa práv. To neplatí rovnako pre osobitnú výnimku čerpania údajov na účely vedeckého výskumu.
- AI Act v čl. 53 ukladá poskytovateľom modelov na všeobecné účely povinnosť mať politiku dodržiavania autorského práva vrátane rešpektovania týchto výhrad a zverejniť dostatočne podrobné zhrnutie obsahu použitého na tréning.

**Prakticky:** ak firma trénuje alebo doladzuje model na dátach, ktoré nevytvorila sama alebo na ich použitie nemá licenciu, je namieste vedieť, odkiaľ dáta pochádzajú, či nie sú zaťažené výhradou práv a čo o pôvode tréningových dát hovorí zmluva s dodávateľom modelu. Záznam o pôvode dát je zároveň tým istým typom dokumentácie, o ktorej hovorí tretia časť tejto brožúry.

## PRAKTICKÉ MINIMUM

Nasledujúci prehľad je základom, ktorý zvládne aj stredne veľká firma bez samostatného compliance tímu.

| PRVOK                              | PREČO NA ŇOM ZÁLEŽÍ                                                                                                                                                                                                                         |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Register AI nástrojov              | Bez zoznamu neviete, čo sa u vás používa. Reálne používanie spravidla ďaleko presahuje to, čo bolo schválené.                                                                                                                               |
| Interná politika používania AI     | Určuje, čo sa smie vkladať do nástrojov, čo nie, a kto rozhoduje o nasadení nového nástroja.                                                                                                                                                |
| Klasifikácia rizika použitia       | Rovnaký nástroj je pri sumarizácii poznámok minimálne rizikový a pri triedení životopisov vysokorizikový. Rozhoduje účel, nie technológia.                                                                                                  |
| Ľudský dohľad                      | Určiť, kde musí rozhodnutie potvrdiť človek, kto to je a čo presne posudzuje. Schvaľovateľ, ktorý len klikne, dohľadom nie je.                                                                                                              |
| Záznamy a logy                     | Verzie modelov a promptov, testovanie pred nasadením, kto čo použil. Od 9. 12. 2026 ide zároveň o dôkazný materiál.                                                                                                                         |
| Označovanie AI obsahu              | Pravidlo, ktoré zabezpečí, že označenie sa nasadí aj na budúci obsah, nielen jednorazovo na existujúci – vrátane toho, ktorá ikona sa kedy použije.                                                                                         |
| Školenie a jeho evidencia          | AI gramotnosť je povinnosť od 2. 2. 2025. Bez evidence ju nepreukázate.                                                                                                                                                                     |
| Proces riešenia incidentov         | Kto zachytí incident, komu ho eskaluje a ktoré hlásenia sa v danom prípade uplatnia. Vopred nastavený proces je rozhodujúci na dodržanie krátkych lehôt, ktoré môžu pri DORA začínať už 4 hodinami od klasifikácie incidentu ako závažného. |
| Zmluvná dokumentácia s dodávateľmi | Informačné a súčinnosť povinnosti, regres, aktualizácie, kybernetická bezpečnosť, práva k výstupom.                                                                                                                                         |
| DPIA a FRIA                        | Pri vysokorizikových systémoch takmer vždy pribudne posúdenie vplyvu na ochranu údajov a pri niektorých subjektoch aj posúdenie vplyvu na základné práva. Robia sa súbežne, nie oddelene.                                                   |
| Určený vlastník agendy             | Bez konkrétnej osoby alebo výboru zostane zoznam úloh zoznamom. Podrobne v samostatnej kapitole nižšie.                                                                                                                                     |

## KTO ZA TO VO FIRME ZODPOVEDÁ

Toto je otázka, na ktorej väčšina implementácií stroskotá. Firma si odnesie zoznam úloh, ale nie meno človeka, ktorý ich má urobiť. Zoznam potom putuje medzi IT, právnym oddelením a HR, kde ho každý považuje za agendu toho druhého.

Regulácia sama v tomto smere naznačuje odpoveď. Zákon o kybernetickej bezpečnosti vyžaduje určeného manažéra kybernetickej bezpečnosti a zodpovednosť za kybernetickú bezpečnosť kladie výslovne na vrcholový manažment. AI Act pri vysokorizikových systémoch vyžaduje, aby ľudský dohľad vykonávala osoba, ktorá má na to spôsobilosť, právomoc a podporu. V oboch prípadoch ide o konkrétnu osobu, nie o oddelenie.

### ČO ODPORÚČAME

- **Určiť vlastníka agendy AI Governance.** Jedna osoba, ktorá zastrešuje register nástrojov, klasifikáciu rizika a komunikáciu s dodávateľmi. Nemusí ísť o novú pozíciu.
- **Zriadiť malý výbor, nie veľký.** Zástupcovia IT, práva, HR a prevádzky. Jeho úlohou je schvaľovať nasadenie nových nástrojov a rozhodovať sporné klasifikácie rizika, nie stretávať sa.
- **Prepojiť roly, ktoré už existujú.** Zodpovedná osoba pre ochranu osobných údajov, manažér kybernetickej bezpečnosti a vlastník AI agendy riešia prekrývajúce sa otázky. DPIA a FRIA sú ich spoločný výstup.
- **Zakotviť eskaláciu na vedenie.** Pri incidente s krátkou oznamovacou lehotou musí byť vopred jasné, kto rozhoduje a kto ho zastupuje v neprítomnosti.

## INTERNÉ OZNAMOVANIE A OCHRANA OZNAMOVATEĽOV

Nesúlad v oblasti AI a kybernetickej bezpečnosti sa spravidla najskôr dozvie zamestnanec, nie vedenie. Práve preto stojí za zváženie, ako sa téma prepája so zákonom č. 54/2019 Z. z. o ochrane oznamovateľov protispoločenskej činnosti.

- Zamestnanec, ktorý upozorní na nesúlad – napríklad na nástroj spadajúci do zakázaných praktík alebo na nenahlásený incident – môže byť za splnenia zákonných podmienok chránenou osobou.
- Firmy, na ktoré sa vzťahuje povinnosť mať vnútorný systém preverovania oznámení, by mali zabezpečiť, aby tento kanál pokrýval aj oznámenia tohto typu a aby o ňom zamestnanci vedeli.
- Postih zamestnanca, ktorý takéto oznámenie podal, môže vytvoriť samostatné právne riziko popri riziku vyplývajúcom zo samotného nesúladu.

Z praktického hľadiska je to zároveň prvok Governance: interné oznamovanie je často najrýchlejší spôsob, ako sa firma o probléme dozvie skôr, než sa o ňom dozvie orgán dohľadu alebo poškodený.

**Poznámka:** či konkrétne oznámenie spadá do vecnej pôsobnosti zákona o ochrane oznamovateľov, závisí od povahy porušenia. Odporúčame to posúdiť individuálne.

---

## PREČO NESTAČÍ SMERNICA: ROZMER SKUTOČNÉHO SPRÁVANIA

Najčastejšia chyba je, že firma prijme internú politiku, podľa ktorej „sa použitie AI dokumentuje“, a považuje vec za vyriešenú. Politika však sama osebe nevytvára žiadny záznam.

Skutočná otázka znie: dá sa o dva alebo tri roky spätne zrekonštruovať, kto, aký systém, v akej verzii, na základe akých vstupov a s akým ľudským dohľadom použil? Ak odpoveď znie nie, firma nemá Governance – má dokument.

Rozdiel medzi jedným a druhým je predovšetkým otázkou skutočného správania ľudí a nastavenia procesov: či je jednoduchšie postupovať správne než obísť pravidlo, či má schvaľovateľ reálnu možnosť rozhodnutie zmeniť, či sa záznam vytvára automaticky alebo závisí od disciplíny jednotlivca a či niekto v piatok večer vie, že incident treba eskalovať do rána. Toto je oblasť behaviorálnej compliance a pri AI aj pri kybernetickej bezpečnosti rozhoduje o výsledku viac než formulácia internej smernice.

## ČO ROBIŤ TERAZ

Zoznam je zoradený podľa priority, nie podľa predpisu. Ak urobíte tento mesiac len jednu vec, nech je to register AI nástrojov – bez neho sa nedá urobiť nič ďalšie a odhalí veci, o ktorých vedenie spravidla nevie.

| KEDY                                | ČO                                                                                                                                                              |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PRIORITA 1</b><br>tento mesiac   | Prejsť rozhodovací test na začiatku brožúry a zistiť, ktoré predpisy sa vás týkajú. Bez toho je zvyšok zoznamu hádanie.                                         |
| <b>PRIORITA 1</b><br>tento mesiac   | Zostaviť register AI nástrojov reálne používaných vo firme vrátane tých, ktoré nikto neschválil, a pri každom zaznamenať, či ide o AI systém a v akom je pásme. |
| <b>PRIORITA 1</b><br>tento mesiac   | Overiť, či niektoré použitie nespadá do zakázaných praktík – pozor najmä na vyhodnocovanie emócií zamestnancov.                                                 |
| <b>PRIORITA 1</b><br>tento mesiac   | Skontrolovať chatboty a AI obsah na webe: je zrejme, že ide o AI? Táto povinnosť už platí a náprava je lacná.                                                   |
| <b>PRIORITA 2</b><br>do 11. 9. 2026 | Ak uvádzate na trh softvér na stiahnutie alebo pripojené zariadenie: nastaviť proces zachytenia a hlásenia zneužívaných zraniteľností v 24-hodinovom režime.    |
| <b>PRIORITA 2</b><br>do 11. 9. 2026 | Určiť vlastníka agendy a eskalačnú cestu pri incidente, vrátane zástupu.                                                                                        |
| <b>PRIORITA 2</b><br>do 11. 9. 2026 | Overiť postavenie podľa zákona o kybernetickej bezpečnosti a v prípade potreby sa zaregistrovať.                                                                |
| <b>PRIORITA 3</b><br>do 12/2026     | Identifikovať softvérové a AI produkty, ktoré uvediete na trh po 9. 12. 2026, a prepojiť ich s release plánom.                                                  |
| <b>PRIORITA 3</b><br>do 12/2026     | Nastaviť dvojrežimovú retenciu logov – prevádzkovú a dôkaznú – vrátane zápisu odôvodnenia.                                                                      |
| <b>PRIORITA 3</b><br>do 12/2026     | Revidovať zmluvy s dodávateľmi AI a IKT a preveriť poistenie zodpovednosti za výrobok.                                                                          |
| <b>PRIEBEŽNE</b>                    | Zaviesť internú politiku používania AI, preškoliť zamestnancov a školenie zdokumentovať.                                                                        |
| <b>PRIEBEŽNE</b>                    | Prípraviť sa na prílohu III a na DPIA či FRIA, ak používate AI v náboře, hodnotení zamestnancov, úveroch alebo poistení.                                        |
| <b>PRIEBEŽNE</b>                    | Ak dodávate finančnému sektoru alebo prevádzkovateľom základných služieb: pripraviť sa na zmluvné požiadavky podľa DORA a ZoKB.                                 |

## ORIENTAČNÁ NÁROČNOSŤ

Klienti sa spravidla pýtajú, aký veľký záväzok to je, skôr než oslovia právnik. Nasledujúci odhad je orientačný a vychádza z bežnej strednej firmy s niekoľkými desiatkami zamestnancov. Skutočná náročnosť závisí od počtu nástrojov, sektora a od toho, koľko z uvedeného už firma má.

| ÚLOHA                                     | ORIENTAČNE      | KTO                                        | ČO TO OBNÁŠA                                                                       |
|-------------------------------------------|-----------------|--------------------------------------------|------------------------------------------------------------------------------------|
| Register AI nástrojov                     | 2–4 týždne      | Vlastnými silami                           | Jeden zodpovedný človek na čiastočný úväzok plus krátky dopyt naprieč oddeleniami. |
| Posúdenie, čo je AI systém a v akom pásme | 1–2 týždne      | Vlastnými silami, hraničné prípady externe | Pri väčšine nástrojov je odpoveď jasná. Sporné sú spravidla dva až tri.            |
| Interná politika a školenie               | 2–4 týždne      | Šablóna externe, zvyšok interne            | Text politiky, schválenie vedením, školenie a evidencia účasti.                    |
| Kontrola označovania AI obsahu            | dni až 2 týždne | Vlastnými silami                           | Prevažne úprava textov a nastavení, nie prestavba procesov.                        |
| Posúdenie postavenia podľa ZoKB alebo CRA | 1–2 týždne      | Odporúčame externe                         | Analýza sektora, veľkosti a typu služby alebo hraníc výroby; prípadná registrácia. |
| Proces hlásenia incidentov                | 2–4 týždne      | Interne, s externým overením               | Určenie rolí, eskalačná cesta, zástup a nácvik 4 prípadne 24-hodinovej lehoty.     |
| Revízia zmlúv s dodávateľmi               | priebežne       | Externe                                    | Závisí od počtu zmlúv; spravidla sa rieši pri obnove alebo dodatku.                |
| DPIA alebo FRIA k jednému systému         | rádovo týždne   | Spoločne                                   | Podklady dodá firma, metodiku a posúdenie rizika spravidla externý poradca.        |

Uvedené časy sú doby trvania jednotlivých úloh, nie súčet práce. Väčšina z nich beží paralelne, preto ich jednoduché sčítanie výsledok nadhodnotí.

### SÚHRNNE: ČO TO ZNAMENÁ PRE PLÁN A ROZPOČET

Celkové trvanie: pri paralelnom postupe zvládne stredne veľká firma základné nastavenie za 6 až 10 týždňov od rozhodnutia začať.

Interná práca: rádovo 15 až 30 človeko-dní rozložených do tohto obdobia. Ide o čiastočný úväzok jedného zodpovedného človeka a kratšie vstupy z IT, HR a prevádzky – nie o vyčlenenú pozíciu.

Externá podpora: pri firme bez zvláštností rádovo nízke desiatky hodín právneho poradenstva. Ťažisko je v posúdení postavenia podľa zákona o kybernetickej bezpečnosti alebo hraníc výrobu podľa CRA, v šablónach a v revízii zmlúv.

Čo náklad zvyšuje: vysokorizikové použitie (DPIA a FRIA), postavenie prevádzkovateľa základnej služby, produkty v pôsobnosti CRA, pôsobenie vo viacerých členských štátoch a veľký počet dodávateľských zmlúv.

Čo náklad znižuje: existujúca dokumentácia GDPR, zavedený systém riadenia informačnej bezpečnosti a malý počet reálne používaných AI nástrojov.

Tieto čísla sú orientačné. Slúžia na to, aby ste vedeli, či hovoríme o týždňoch alebo o rokoch – nie ako cenová ponuka.

Prevažná časť tejto práce je jednorazová. Po nastavení ide o priebežnú údržbu – aktualizáciu registra pri novom nástroji, ročné školenie a revíziu pri zmene systému.

### AK SI Z BROŽÚRY ODNESIETE TRI VECI

1. Odklad sa týkal len vysokorizikových AI systémov. Zákazy, AI gramotnosť a povinnosť označovať AI obsah platia už dnes.
2. Najbližší termín nie je z AI Actu. Je to 11. september 2026 a ohlasovacie povinnosti podľa Cyber Resilience Act – aj pre produkty, ktoré sú na trhu už dnes.
3. Od 9. decembra 2026 sa AI governance mení z regulačnej agendy na dôkaznú pozíciu. Kto nemá záznamy, nemá čím vyvrátiť domnienku vadnosti.

*Radi s vami prejdeme, čo z uvedeného sa týka práve vašej firmy – od auditu používania AI a nastavenia registra a internej politiky, cez posúdenie postavenia podľa zákona o kybernetickej bezpečnosti a revíziu zmlúv s dodávateľmi až po prípravu na nový režim zodpovednosti k 9. decembru 2026.*

*Pre klientov, ktorí chcú začať vlastnými silami, vieme poskytnúť pripravené podklady – šablónu internej politiky používania AI, štruktúru registra AI nástrojov, kontrolný zoznam pre klasifikáciu rizika a vzorové zmluvné doložky pre dodávateľov AI a IKT služieb. Nahradiť posúdenie konkrétnej situácie šablóny nedokážu, výrazne však skracujú prvý krok.*

Tento materiál je informatívnym prehľadom a nenahrádza právne poradenstvo. Zohľadňuje právny stav k 31. augustu 2026. Slovenský návrh zákona o zodpovednosti za škodu spôsobenú vadným výrobkom je v druhom čítaní a slovenský vykonávací zákon k AI Actu nebol k tomuto dňu schválený; znenie oboch sa môže zmeniť.

## KONTAKTNÉ ÚDAJE



### **LUCIE SCHWEIZER**

#### **PARTNER**

D: +421 2 5980 0411  
M: +421 911 737 437  
lucie.schweizer@lehnert.sk



### **BARBARA NÉMETHOVÁ**

#### **ADVOKÁTKA**

D: +421 2 5980 0411  
M: +421 905 239 394  
barbara.nemethova@lehnert.sk

