MANAŽÉRSKY CHECKLIST

Connecting your world.

15 BODOV PRE BEZPEČNÉ POUŽÍVANIE AI A GDPR VO FIRME

LiveTalk by T Business
11. 6. 2026

Krátky praktický návod pre podnikateľov, manažérov a firmy, ktoré chcú používať AI rozumne, bezpečne a bez zbytočného GDPR rizika.

Pripravila ho **Eva Balogová, špecialistka na ochranu osobných údajov a GDPR**, na základe skúseností z praxe a najčastejších otázok, ktoré dnes firmy riešia pri používaní AI.

AI dnes neznamená len nový nástroj na rýchle texty, preklady alebo marketing. Znamená aj nové otázky:

Aké údaje do nej vkladáme? Kto ju vo firme používa? Čo sa deje s firemnými informáciami? A vieme vôbec dokázať, že máme veci pod kontrolou?

Tento checklist vám pomôže zistiť, či máte základné pravidlá pre GDPR, AI a ochranu firemných dát nastavené aspoň na úrovni zdravého manažérskeho minima.

PILIER 1: GDPR NIE JE DOKUMENT V ŠANÓNE

Cieľ: Vedieť, aké osobné údaje firma spracúva, prečo ich spracúva a či to vie aj preukázať.

☐ **1. Vieme, aké osobné údaje vo firme spracúvame.**
Máme prehľad o tom, aké údaje spracúvame o zamestnancoch, klientoch, dodávateľoch, uchádzačoch o zamestnanie, návštevníkoch webu alebo iných osobách.

Kontrolná otázka:
Keby sa dnes niekto vo firme spýtal, kde všade máme osobné údaje, vedeli by sme odpovedať?

☐ **2. Máme aktuálne záznamy o spracovateľských činnostiach.**
Nestačí vedieť „nejako približne“, čo robíme s údajmi. GDPR vyžaduje, aby organizácia vedela preukázať, aké spracovateľské činnosti vykonáva. Záznamy o spracovateľských činnostiach sú základným dôkazom poriadku vo firme.

Kontrolná otázka:
Sú naše GDPR dokumenty živé a aktuálne, alebo vznikli raz dávno a odvtedy ich nikto neotvoril?

☐ **3. Vieme, kto má k osobným údajom prístup.**
Nie každý zamestnanec potrebuje vidieť všetko. Prístupy k údajom by mali zodpovedať pracovnej pozícii a reálnej potrebe.

Kontrolná otázka:
Má bývalý zamestnanec, externista alebo brigádnik stále prístup do systémov, kde sú osobné alebo obchodné údaje?

☐ **4. Vieme, čo by sme robili pri incidente.**
Ak dôjde k strate notebooku, odoslaniu e-mailu nesprávnej osobe, úniku údajov alebo napadnutiu účtu, firma musí vedieť rýchlo reagovať. Pri porušení ochrany osobných údajov sa podľa GDPR posudzuje aj povinnosť oznámenia dozornému orgánu do 72 hodín od zistenia incidentu, ak je pravdepodobné riziko pre práva a slobody fyzických osôb.

Kontrolná otázka:
Vedia zamestnanci, komu majú nahlásiť bezpečnostný alebo GDPR incident?

PILIER 2: KONTROLY A CHYBY PODNIKATEĽOV

Cieľ: Neodpovedať úradu emotívne, chaoticky alebo bez dôkazov.

☐ **5. Vieme, že Úrad na ochranu osobných údajov kontroly reálne vykonáva.**
Úrad zverejňuje plán kontrol a zároveň rieši podnety, ktoré dostáva od dotknutých osôb.
Plán kontrol na rok 2026 je zverejnený na stránke Úradu na ochranu osobných údajov SR.
Úrad na ochranu osobných údajov Slovenskej republiky

Kontrolná otázka:
Sledujeme aspoň raz ročne, na čo sa úrad v kontrolách zameriava?

☐ **6. Pri otázkach úradu nereagujeme pod vplyvom emócií.**
Jedna z najväčších chýb firiem je, že na výzvu úradu odpovedajú rýchlo, obranne a bez odbornej prípravy. Odpoveď úradu nie je bežný e-mail. Je to procesný dokument, ktorý môže ovplyvniť ďalší vývoj veci.

Kontrolná otázka:
Máme určenú osobu alebo odborníka, ktorý pripravuje odpovede voči úradu?

☐ **7. Ku každému tvrdeniu máme dôkaz.**
V GDPR nestačí povedať: „My to robíme správne.“ Dôležité je vedieť to preukázať — dokumentom, záznamom, školením, poverením, interným pravidlom alebo rozhodnutím vedenia.

Kontrolná otázka:
Keby prišla kontrola, vedeli by sme doložiť, že zamestnanci boli poučení a pravidlá poznajú?

PILIER 3: AI VO FIRME MENÍ PRAVIDLÁ HRY

Cieľ: Používať AI tak, aby pomáhala firme, ale neohrozovala osobné údaje, obchodné tajomstvo ani reputáciu.

☐ **8. Vieme, ktoré AI nástroje zamestnanci používajú.**
ChatGPT, Copilot, Gemini, Claude, Perplexity, DeepSeek, Grok alebo iné AI nástroje môžu byť vo firme používané aj bez vedomia vedenia. To je problém, pretože firma nevie, aké dáta do nich odchádzajú.

Kontrolná otázka:
Máme zmapované, či zamestnanci používajú AI cez firemné alebo súkromné účty?

☐ **9. Máme pravidlá, čo sa do AI nesmie vkladať.**
Do verejne dostupných AI nástrojov by zamestnanci nemali vkladať osobné údaje, pracovné zmluvy, mzdy, zdravotné údaje, klientské zoznamy, obchodné ponuky, interné stratégie, heslá, zmluvy alebo iné citlivé informácie.

Kontrolná otázka:
Vie zamestnanec rozlíšiť, čo môže do AI vložiť a čo už je riziko?

☐ **10. Rozumieme tomu, že AI sa môže mýliť.**
AI negarantuje pravdu. Vytvára pravdepodobnú odpoveď podľa vstupu, dát a kontextu.
Preto môže vyrobiť nepresnosť, predsudok, vymyslený zdroj alebo sebavedomú chybu.

Kontrolná otázka:
Máme pravidlo, že výstupy z AI sa pred použitím kontrolujú človekom?

☐ **11. Pri AI riešime aj autorské práva a marketing.**
Marketing patrí medzi najčastejšie oblasti využívania AI. Texty, obrázky, slogany alebo kampane vytvorené AI však môžu otvárať aj otázky originality, licencie, zdrojov a práv tretích strán.

Kontrolná otázka:
Máme pravidlá, ako označujeme, kontrolujeme a používame AI výstupy v marketingu?

PILIER 4: SHADOW AI A NAHRÁVANIE STRETNUTÍ

Cieľ: Zabrániť tomu, aby sa AI používala „potichu“ a bez kontroly.

☐ **12. Riešime shadow AI.**
Shadow AI znamená, že zamestnanci používajú AI nástroje bez schválenia firmy často cez súkromný účet, vlastný telefón alebo neoverenú aplikáciu. Motivácia nemusí byť zlá. Problém je, že firma nad tým stráca kontrolu.

Kontrolná otázka:
Máme vo firme zakázané, povolené alebo aspoň upravené používanie AI cez súkromné účty?

☐ **13. Máme pravidlá pre nahrávanie porád, hovorov a stretnutí.**
AI nástroje dnes dokážu automaticky nahrávať, prepisovať a sumarizovať stretnutia. To môže byť praktické, ale zároveň ide o spracúvanie osobných údajov. Účastníci by mali vedieť, že sa nahráva, na aký účel, kde sa záznam uloží, kto k nemu má prístup a ako dlho sa bude uchovávať.

Kontrolná otázka:
Vie každý vo firme, že nahrávanie porady bez pravidiel nie je len technická funkcia, ale aj právna otázka?

PILIER 5: AI ACT A POVINNOSŤ VZDELÁVANIA

Cieľ: Nečakať, kým bude problém. Základná AI gramotnosť už patrí do firemnej reality.

☐ **14. Máme zabezpečenú základnú AI gramotnosť zamestnancov.**
AI Act zavádza povinnosť AI gramotnosti podľa článku 4. Ide o to, aby osoby pracujúce s AI systémami mali primerané znalosti, zručnosti a porozumenie rizikám

Kontrolná otázka:
Prešli naši zamestnanci aspoň základným školením, čo AI je, ako funguje a čo do nej nesmú vkladať?

☐ **15. Vieme, či používame vysokorizikové AI systémy.**
Nie každé používanie AI je vysokorizikové. Ale pozor najmä na oblasti ako HR, hodnotenie zamestnancov, nábor, vzdelávanie, úverovanie, prístup k službám alebo kritická infraštruktúra

Kontrolná otázka:
Používame AI na rozhodovanie o ľuďoch, ich práci, hodnotení, prijatí, odmietnutí alebo prístupe k službe?

30-DŇOVÝ ZÁKLADNÝ PLÁN, AK ZAČÍNATE OD NULY

Ak máte viac ako polovicu bodov nesplnených, nezačínajte veľkým auditom. Začnite prakticky.

Týždeň	Čo urobiť
1	Zmapovať, aké osobné údaje firma spracúva a kde sú uložené. Skontrolovať, či máte aktuálne GDPR dokumenty a záznamy o spracovateľských činnostiach.
2	Zistiť, aké AI nástroje zamestnanci používajú. Rozlíšiť firemné účty, súkromné účty a nástroje používané bez vedomia firmy.
3	Pripraviť krátke interné pravidlá: čo sa do AI môže vkladať, čo sa nesmie, kto výstupy kontroluje a ako sa rieši nahrávanie stretnutí.
4	Urobiť krátke školenie zamestnancov k GDPR, AI a bezpečnému používaniu nástrojov. Zo školenia si nechať prezenčnú listinu alebo elektronický záznam.

ČO BY MALA MAŤ KAŽDÁ FIRMA AKO MINIMUM

- Aktuálne GDPR dokumenty.
- Záznamy o spracovateľských činnostiach.
- Pravidlá pre používanie AI.
- Zoznam používaných AI nástrojov.
- Pravidlá pre nahrávanie stretnutí a hovorov.
- Interný postup pri incidente.
- Preukázateľné školenie zamestnancov.
- Určenú osobu, ktorá tieto témy rieši.

Zaujala vás táto téma alebo máte otázky k vašej konkrétnej situácii?
Radi sa na to s vami pozrieme. Stačí nás kontaktovať cez online formulár.