GDPR *live*

# PONUKA RIEŠENIA PRE TRVALO UDRŽATEĽNÝ SÚLAD S NARIADENÍM EÚ O OCHRANE OSOBNÝCH ÚDAJOV (General Data Protection Regulation - GDPR)

Ponuka služieb je pripravená na základe dlhoročných skúseností z riadenia projektov v oblasti manažérstva procesov, kvality a informačnej bezpečnosti a zabezpečí Vám trvalo udržateľný súlad ochrany fyzických osôb pri spracovaní osobných údajov podľa Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 a Zákona o ochrane osobných údajov č. 18/2018.

Proces zabezpečenia súladu s nariadením GDPR sme rozdelili do nasledovných oblastí:

**1. Školenie** v oblasti ochrany osobných údajov - pravidelné vzdelávanie zamestnancov v oblasti ochrany osobných údajov pri nástupe do zamestnania a v pravidelných intervaloch 0,5 - 1 roka s cieľom priebežného zvyšovania povedomia o problematike ochrany osobných údajov. Školenia budú ukončené overením znalosti, zdokumentované certifikátom úspešného absolvovania školenia.

**2. Diagnostika** pripravenosti spoločnosti na zabezpečenie GDPR - vstupná diagnostika súčasného stavu spracovania ochrany osobných údajov prevádzkovateľa prostredníctvom elektronického portálu GDPR live. Výstupom vstupnej diagnostiky bude excelovský súbor, ktorý bude tvoriť základ pre vykonanie analýzy a posúdenia súladu s GDPR.

**3. Analýza** - rozdelenie identifikovaných osobných údajov prevádzkovateľa podľa kľúčových činností (pôsobností) organizačných útvarov. K identifikovaným osobným údajom je potrebné priradiť účel spracúvania a príslušný právny základ, na základe ktorých sú tieto osobné údaje spracovávané. V rámci analýzy je potrebné taktiež stanoviť rozsah vplyvu spracovania osobných údajov na dotknuté osoby (zamestnanci, zákazníci, dodávatelia, odberatelia, sprostredkovatelia) a zhodnotiť, či zistené spracúvanie osobných údajov neprevažuje nad právami a záujmami dotknutých osôb (uviesť, prečo sa spracúvanie nedá uskutočniť menej rušivým spôsobom). Osobitnú pozornosť je potrebné pri analýze venovať aj kategórii citlivých osobných údajov.
Druhou časťou analýzy je stanovenie organizačných rolí spracovávateľov osobných údajov GDPR z pohľadu kompetencií a zabezpečenia kontinuálneho vzdelávania.

**4. DPIA** (Data Protection Impact Assessment), resp. PIA (Privacy Impact Assessment) ďalej len ako „DPIA“ - p**osúdenie vplyvu na ochranu údajov** - predstavuje analýzu a hodnotenie rizík pôsobiacich na práva a slobody dotknutých osôb a identifikáciu bezpečnostných incidentov pre splnenie požiadavky ohlasovacej povinnosti Úradu pre ochranu osobných údajov (do 72 hodín od zistenia akéhokoľvek narušenia ochrany spracúvaných údajov).
V prípade, ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ **pred spracúvaním** vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov.
Posudzovanie vplyvu na ochranu osobných údajov je poskytovateľ povinný vykonať pred tým, ako zaháji proces, ktorý napĺňa niektorý z nasledovných predpokladov:
a) napĺňa predpoklady v zmysle čl. 35 ods. 3. písm. a), b) alebo c),
b) spracovanie údajov označil príslušný dozorný úrad za rizikové,
c) spracovanie, u ktorého existuje pravdepodobnosť, že toto spracovanie závažným spôsobom ohrozí práva fyzických osôb.

Vo firemnom prostredí sú osobné údaje evidované buď v digitálnej forme (informačné systémy), alebo v listinnej podobe. Bezpečnosť spracúvania osobných údajov je potrebné zabezpečiť prijatím primeraných opatrení, ktoré zahŕňajú aj **pseudonymizáciu** a **šifrovanie** osobných údajov, **dôvernosť, integritu, dostupnosť a odolnosť** systémov spracúvania a služieb, **obnovenie dostupnosti** osobných údajov a **prístupu k nim** v prípade fyzického alebo technického incidentu a **proces pravidelného testovania**, posudzovania a **hodnotenia účinnosti opatrení** na zaistenie bezpečnosti spracúvania.

**5. Revízia zmlúv** prevádzkovateľa - posúdenie dodržiavania Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 a Zákona o ochrane osobných údajov č. 18/2018 v zmluvách a stanovenie retenčnej doby pre spracúvanie osobných údajov (lehoty na vymazanie rôznych kategórií údajov).

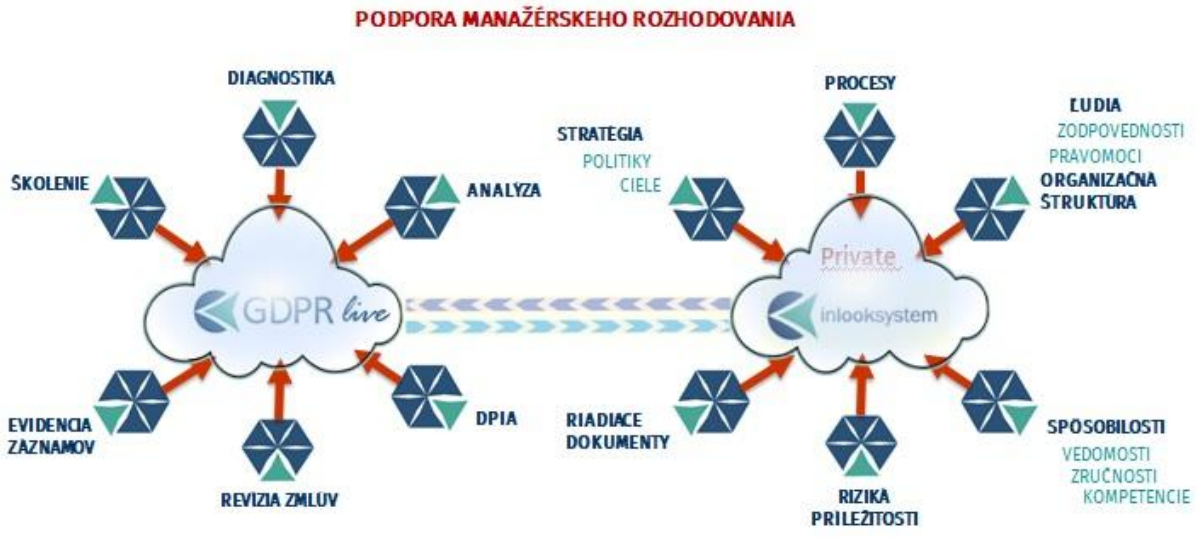
**6. Evidencia záznamov** o spracovateľských činnostiach. Každý prevádzkovateľ vedie záznamy o spracovateľských činnostiach, za ktoré je zodpovedný v písomnej podobe vrátane elektronickej podoby. Záznamy musia obsahovať všetky nasledovné informácie:

a) meno/názov a kontaktné údaje prevádzkovateľa a v príslušnom prípade spoločného prevádzkovateľa, zástupcu prevádzkovateľa a zodpovednej osoby;
b) účel spracovania;
c) opis kategórií dotknutých osôb a kategórií osobných údajov;
d) kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, vrátane príjemcov v tretích krajinách alebo medzinárodných organizáciách;
e) v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácii vrátene označenia predmetnej tretej krajiny alebo medzinárodnej organizácie

Povinnosti uvedené v oblasti 6 sa nevzťahujú na spoločnosť, ktorá zamestnáva menej ako 250 osôb, **pokiaľ** nie je pravdepodobné, že spracúvanie, ktoré vykonáva, povedie k riziku pre práva a slobody dotknutej osoby, pokiaľ je toto spracúvanie príležitostné alebo **nezahŕňa** osobitné kategórie údajov podľa článku 9 ods. 1..

**INFORMAČNÁ PODPORA RIEŠENIA**

- ✓ **GDPR live** – vzdelávací a informačný portál
- ✓ **InLook system®** – informačná podpora objektivizácie systému riadenia



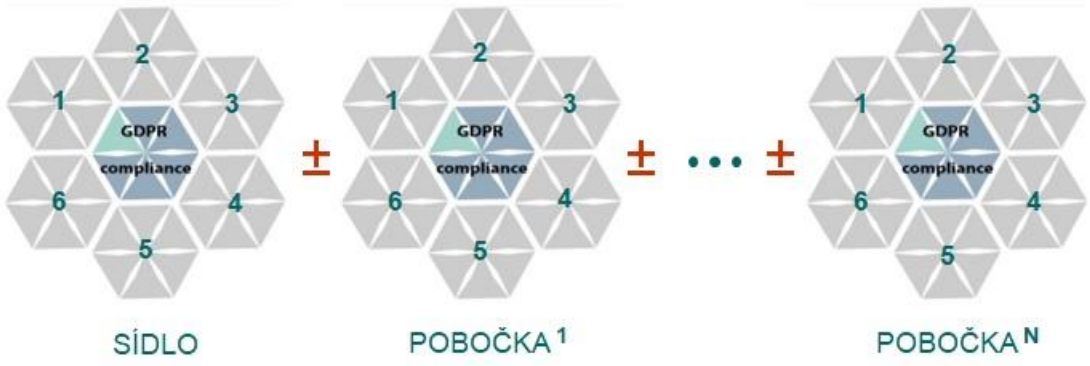
GDPR *live*

**VÝSTUPOM RIEŠENIA JE:**

- ✓ identifikácia vplyvu GDPR na riadenie biznis procesov
- ✓ posúdenie organizačnej, personálnej, technickej a právnej časti pripravenosti prevádzkovateľa zabezpečovať požiadavky GDPR kontinuálne
- ✓ GDPR súlad (GDPR compliance)*

GDPR compliance – následná permanentná, odborná, v čase sa vyvíjajúca činnosť, ktorú musí prevádzkovateľ kontinuálne zabezpečovať, vylepšovať, prehodnocovať a upravovať.

PREVÁDZKOVATEĽ / SPROSTREDKOVATEĽ OSOBNÝCH ÚDAJOV PROSTREDNÍCTVOM RIEŠENIA GDPR SÚLADU **KONTINUÁLNE** IDENTIFIKUJE:




1. **Koľko ?** organizačných útvarov, prevádzok, stredísk, pobočiek spracúva osobné údaje v mene prevádzkovateľa;
2. **Kto ?** je zodpovedný za prácu s osobnými údajmi;
3. **Aké ?** osobné údaje sa spracovávajú;
4. **Kde ?** sa osobné údaje spracovávajú;
5. **Kam / Komu ?** sa osobné údaje prenášajú;
6. **Ako ?** sú osobné údaje zabezpečené.

Tešíme sa na spoluprácu,
váš tím GDPR *live*