30 krokov súladu s novou právnou úpravou ochrany osobných údajov

Úvod

Urobiť konkrétny návod, ako postupovať pri vytváraní súladu s Nariadením/zákonom č. 18/2018 Z. z. je prakticky nemožné, pretože nie je cieľom splnenie explicitne ustanovených požiadaviek, ale v súlade s novým prístupom zodpovednosti prevádzkovateľ je povinný kedykoľvek preukázať súlad s celým Nariadením/zákonom č. 18/2018 Z. z., počnúc základnými zásadami spracúvania až po bezpečnosť pri spracúvaní osobných údajov.

Odporúčame implementáciu rozplánovať do niekoľkých krokov. Prvým krokom je zoznámenie sa s obsahom a požiadavkami, ktoré Nariadenie a zákon č. 18/2018 Z. z. kladie na prevádzkovateľov a sprostredkovateľov. Toto oboznámenie upozorní na rozdiely v prebiehajúcich procesoch oproti požiadavkám, ktoré sú kladené na subjekty novou právnou úpravou ochrany osobných údajov. Podotýkame, že pre prevádzkovateľov, ktorí sú doteraz v súlade so zákonom č. 122/2013 Z. z. o ochrane osobných údajov nebude nová právna úprava predstavovať revolúciu, ale skôr evolúciu v oblasti ochrany osobných údajov a prevádzkovatelia môžu kontinuálne pokračovať v spracúvaní osobných údajov, po zohľadnení niektorých nových inštitútov a povinností.

1. Oboznámenie sa so základnými pojmami

- čo je to osobný údaj?

- kto je dotknutá osoba, kedy je v mojom prostredí fyzická osoba identifikovaná alebo identifikovateľná, aby sa na ňu vzťahovala právna úprava ochrany osobných údajov?

- kto je prevádzkovateľ, teda ten kto určil účel a prostriedky spracúvania a kto spracúva osobné údaje dotknutých osôb vo vlastnom mene? Prevádzkovateľ je funkčný pojem, ktorého cieľom je prideliť zodpovednosť tam, kde je aj skutočný vplyv a má objektívnu zodpovednosť za spracúvanie osobných údajov. Spracúvanie osobných údajov môže byť prevádzkovateľovi uložené aj priamo zákonom.

- kto je sprostredkovateľ, teda ten kto spracúva osobné údaje v mene prevádzkovateľa, podľa jeho pokynov a v rozsahu a podľa sprostredkovateľskej zmluvy, alebo iného právneho aktu, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi? Sprostredkovateľská zmluva a iný právny akt musia spĺňať náležitosti podľa čl. 28 ods. 3 Nariadenia/§ 34 ods. 3 zákona č. 18/2018 Z. z.

2. Prípravná fáza implementácie - zostavenie projektového tímu, výstupom ktorého je určenie zodpovednosti a stanovenie kompetencií jednotlivých členov tímu. Vypracuje sa úvodná analýza, vrátane mapovania aktuálneho spracúvania osobných údajov. Vymedzia sa oblasti spracúvania osobných údajov- tu sa uvádza agenda,

oblasť, či proces, pri ktorom dochádza k spracúvaniu osobných údajov, napríklad: evidencia obyvateľov, klientska databáza, personálna a mzdová agenda zamestnancov.

3. Kde sme a kde chceme byť? To znamená vykonať analýzu súčasného stavu, s cieľom porovnať si kde je prevádzkovateľ súladný a kde naopak ide v rozpore s požadovanou úrovňou ochrany osobných údajov.

4. Popis organizačnej štruktúry prevádzkovateľa - odkaz na existujúci organizačný poriadok, interné predpisy a smernice, majúce vzťah aj k problematike ochrany osobných údajov alebo k riadeniu bezpečnosti, pravidlá vedenia spisov a archivácie, požiarny, evakuačný plán, reklamačný poriadok. Táto dokumentácia môže byť podkladom pre novú politiku ochrany osobných údajov.

5. Pomocou akých prostriedkov dochádza k spracúvaniu osobných údajov? Prostriedkami spracúvania sa rozumejú zvolené postupy pre konkrétne spracúvanie, nástroje, ktoré budú použité pri spracúvaní osobných údajov. Prevádzkovateľ vyhodnotí ich bezpečnosť a stav. Právna úprava sa vzťahuje na spracúvanie osobných údajov vykonávané:

- *úplne*, t. j. pri spracúvaní sa využívajú iba technológie (napr. aplikácia) *alebo*
- *čiastočne automatizovanými prostriedkami* (kombinácia technológie a ľudského faktora napr. vyplnenie excelovskej tabuľky) *a*
- a na spracúvanie *inými než automatizovanými prostriedkami* t. j. manuálne, napr. zber vyplnených papierových prihlášok, vedenie pracovných zmlúv v papierovej podobe; *v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.*

6. Aké typy osobných údajov spracúvam? Diferencujeme tri typy osobných údajov:
- *bežné* (všeobecné) osobné údaje napr. meno, priezvisko, adresa, rodné číslo. Podmienky, za ktorých je spracúvanie zákonné sú vymedzené v čl. 6 ods. 1 Nariadenia/§ 13 ods. 1 zákona č. 18/2018 Z. z.
- *osobitné kategórie osobných údajov*, napr. údaje o zdraví, biometrické údaje. Podmienky, za ktorých je spracúvanie týchto citlivých údajov dovolené, sú vymedzené v čl. 9 ods. 2 Nariadenia/§ 16 ods. 2 zákona č. 18/2018 Z. z.
- osobné údaje týkajúce sa uznania viny za *trestné činy a priestupky*.

7. Identifikovať kategórie dotknutých osôb - napr. klienti, pacienti, súťažiaci, občan, dodávatelia, zraniteľná skupina dotknutých osôb - maloletí, dôchodcovia, zamestnanci.

8. Identifikovať účel, pre ktorý tieto osobné údaje budem spracúvať. Účelom rozumieme vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť. Zjednodušene - konkrétny cieľ, ktorý chcem spracúvaním dosiahnuť.

9. Vedieť popísať celý životný cyklus osobných údajov - od momentu ich získania až po ich likvidáciu.

10. Analýza základných zásad spracúvania - mnoho subjektov opomína, že samotná bezpečnosť spracúvania nám začína už v základných zásadách. Zásady spracúvania sa nám prelínajú celou právnou úpravou a je potrebné z nich vychádzať pri interpretácii a aplikácii jednotlivých ustanovení.

11. Na akom právnom základe spracúvam osobné údaje a aké spracovateľské operácie s nimi ďalej vykonávam. Prevádzkovateľ musí pre každý účel spracúvania disponovať primeraným právnym základom v súlade s čl. 6 ods. 1 Nariadenia/§ 13 ods. 1 zákona č. 18/2018 Z. z., ktorý vymedzuje podmienky, za ktorých je spracúvanie zákonné. Je potrebné vykonať revíziu právnych základov, zrušené boli mnohé právne základy upravené v zákone č. 122/2013 Z. z., napr. priamy marketing v poštovom styku, ďalšie spracúvanie už zverejnených osobných údajov, jednorazový vstup, monitorovanie priestorov prístupných verejnosti.

12. Ako bol získaný súhlas so spracúvaním osobných údajov? U osobných údajov, ktoré sú spracúvané na základe súhlasu dotknutých osôb vyhodnotiť, či súhlas udelený podľa zákona č. 122/2013 Z. z. spĺňa podmienky platne udeleného súhlasu podľa Nariadenia/zákona č. 18/2018 Z. z., aby prevádzkovateľ mohol kontinuálne pokračovať na tomto súhlase dotknutej osoby v spracúvaní osobných údajov.

13. Identifikácia príjemcov, vrátane sprostredkovateľov - vykoná sa audit sprostredkovateľských zmlúv, ktorého výsledkom je dodatkovanie alebo vypracovanie novej zmluvnej dokumentácie v súlade s požiadavkami novej právnej úpravy. Vykoná sa revízia právnych základov pokiaľ ide o poskytovanie resp. sprístupňovanie osobných údajov ďalším prevádzkovateľom.

14. Kto má prístup k osobným údajom a na základe akého oprávnenia? Kto a akým spôsobom v prostredí prevádzkovateľa alebo sprostredkovateľa prichádza do styku s osobnými údajmi? Disponuje pokynmi prevádzkovateľa ako má zaobchádzať s osobnými údajmi?

Je zabezpečené, že tieto fyzické osoby majú prístup len k tým údajom, ktoré potrebujú pre výkon svojich úloh? *Ak nie*- vytvorenie bariér, tzv. čínske múry.

Zavedie sa aj účinný mechanizmus kontroly dodržiavania smerníc a interných postupov, pokiaľ ide o bezpečnosť spracúvania osobných údajov napr. ročný/polročný audit, priebežná kontrola zamestnancov na pracovisku, aké dokumenty zamestnanci vynášajú z pracoviska atď. Ľudský faktor je vo všeobecnosti najčastejšou príčinou vzniku bezpečnostných incidentov.

15. Prevádzkovateľ a sprostredkovateľ podniknú kroky na zabezpečenie povinnosti, aby každá osoba, ktorá koná na základe **poverenia** prevádzkovateľa alebo

sprostredkovateľa (touto sa môže tiež rozumieť **oprávnená osoba** konajúca **za** prevádzkovateľa alebo sprostredkovateľa) a má prístup k osobným údajom ich spracúvala len na základe **pokynov prevádzkovateľa** *(poučovacia povinnosť v kontexte čl. 32 ods. 4 Nariadenia a čl. 29 Nariadenia/§ 39 ods. 4 zákona č. 18/2018 Z. z. a § 36 zákona č. 18/2018 Z. z.)* alebo v súlade s osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná a zároveň, v zmysle § 79 zákona č. 18/2018 Z. z. naďalej platí, že prevádzkovateľ a sprostredkovateľ je povinný zaviazať **mlčanlivosťou** o osobných údajoch fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa.

16. Prevádzkovateľ zabezpečí pravidelné vzdelávanie zamestnancov - v oblasti ochrany osobných údajov, a to s cieľom priebežného zvyšovania povedomia o danú problematiku aspoň v intervale 0,5-1 roka a vždy pri nástupe do zamestnania.

17. Informačná povinnosť - v rozsahu podľa čl. 13 alebo čl. 14 Nariadenia/§ 19 alebo § 20 zákona č. 18/2018 Z. z. sa dotýka každého **prevádzkovateľa**, bez ohľadu na to, či osobné údaje boli získané od dotknutej osoby alebo z iného zdroja a bez ohľadu na skutočnosť, na akom právnom základe prevádzkovateľ spracúva osobné údaje. Vyhodnotí sa najčastejší spôsob komunikácie s dotknutou osobou- osobne, e-mailom, prostredníctvom webového sídla. Prevádzkovatelia, ktorí už v zmysle zákona č. 122/2013 Z. z. si plnili informačnú povinnosť voči dotknutým osobám sú povinní ju doplniť v rozsahu, v akom dotknutá osoba nedisponuje danými informáciami, napríklad formou oslovenia verejnosti prostredníctvom webového sídla, alebo zaslaním notifikačného e-mailu. K informačnej povinnosti pribudli napr. kontaktné údaje prevádzkovateľa, kontaktné údaje zástupcu prevádzkovateľa, ak bol poverený, kontaktné údaje zodpovednej osoby, vyžaduje sa konkrétnejšie poučenie o právach dotknutých osôb a ďalšie.

18. Zabezpečí sa spôsob vybavovania agendy práv dotknutých osôb - zhodnotí sa pripravenosť na uplatňovanie nových práv zo strany dotknutých osôb. Prevádzkovateľ zabezpečí technické a organizačné zázemie pre spracovanie žiadostí dotknutých osôb, ideálne prostredníctvom na to určených vzorových formulárov, alebo poskytne dotknutej osobe možnosť prístupu do samostatného rozhrania, zabezpečujúceho kontrolu nad spracúvaním jej osobných údajov, najmä pokiaľ ide o právo na prístup k osobným údajom, alebo právo na opravu. Na webovom sídle prevádzkovateľa môžu byť publikované pokyny a vzory k žiadostiam o uplatňovanie práv dotknutých osôb. Výsledkom má byť spracovanie žiadostí v riadnom termíne a v deklarovanej kvalite.

19. Prevádzkovateľ si vedie záznamy o spracovateľských činnostiach a zabezpečuje ich priebežnú aktualizáciu. Vedenie evidenčného listu, osobitná registrácia a oznamovacia povinnosť je nahradená jednotným vedením záznamov o spracovateľských činnostiach, ktoré je povinní viesť si tak **prevádzkovateľ** ako aj **sprostredkovateľ**. Súčasťou vypracúvania záznamov o spracovateľských činnostiach je aj revízia práv na prístup k jednotlivým úložiskám a zhodnotenie ich stavu z pohľadu bezpečnosti.

20. Vyhodnotiť, či sa na prevádzkovateľa alebo sprostredkovateľa vzťahuje obligatórna povinnosť určenia zodpovednej osoby - prípadne zvážiť potrebu a výhody jej dobrovoľného určenia a preukázať splnenie jej kvalifikačných predpokladov. Určia sa úlohy zodpovednej osoby.

21. Lehota uchovávania údajov a archivačná doba - v súlade s prijatým registratúrnym poriadkom a podľa lehôt stanovených osobitným zákonom.

22. Analýza rizík - každý **prevádzkovateľ a sprostredkovateľ je povinný** v súlade s čl. 32 Nariadenia/§ 39 zákona č. 18/2018 Z. z. vykonať **analýzu rizík**, ktorej výstupom je prijatie primeraných technických a organizačných opatrení; je potrebné posúdiť riziká a dopady na celú svoju **spracovateľskú činnosť** ako aj na práva a slobody fyzických osôb. Užitočným podkladom môže byť už v súčasnosti vypracovaný bezpečnostný projekt, ak spĺňa požiadavky zákonnej úpravy.

Bezpečnostný projekt NEZAHADZOVAŤ! Posúdenie vplyvu ≠ Bezpečnostný projekt!

23. Prijatie primeraných bezpečnostných opatrení

a) **Technické opatrenia** - napr. zabezpečenie objektu pomocou mechanických zábranných prostriedkov (uzamykateľné dvere, okná, mreže), bezpečné uloženie fyzických nosičov osobných údajov (uloženie listinných dokumentov v uzamykateľných skriniach alebo trezoroch), zariadenie na ničenie fyzických nosičov osobných údajov (napr. zariadenie na skartovanie listín), pravidlá prístupu tretích osôb k osobným údajom, identifikácia, autentizácia a autorizácia osôb, používanie logov, firewall, ochrana proti hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok), pravidlá sťahovania súborov z verejne prístupnej počítačovej siete, ochrana pred nevyžiadanou poštou, zálohovanie atď.

   Nariadenie/zákon č. 18/2018 Z. z. vymedzuje niektoré bezpečnostné opatrenia- anonymizácia, šifrovanie, pseudonymizácia, ktoré prevádzkovateľ môže **dobrovoľne** zaviesť do svojich procesov.

b) **Organizačné opatrenia** - vzdelávanie, určenie pokynov, ktoré je osoba povinná uplatňovať pri spracúvaní osobných údajov, vymedzenie osobných údajov, ku ktorým má mať konkrétna osoba prístup na účel plnenia jej povinností alebo úloh, správa hesiel, kontrola vstupu do objektu a chránených priestorov prevádzkovateľa (napr. prostredníctvom technických a personálnych opatrení), režim údržby a upratovania chránených priestorov, pravidlá spracúvania osobných údajov mimo chráneného priestoru, zaobchádzanie so služobnými mobilmi, notebookmi a ich ochrana, používanie e-mailov len na pracovné účely, kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy

a periodicity jej realizácie, informovanie dotknutých osôb o kontrolnom mechanizme, ak je u prevádzkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania).

24. Monitoring rizika. Prevádzkovatelia musia neustále posudzovať riziká, ktoré vznikajú v dôsledku ich spracovateľských činností, nakoľko spracúvanie osobných údajov je živým mechanizmom. Po prijatí bezpečnostných opatrení sa vyžaduje testovanie a hodnotenie, napr. formou penetračných testov, alebo iným testovaním prijatých opatrení**.** Vyžaduje sa pravidelná aktualizácia a optimalizácia.

25. Dokumentovať zavedenie politiky ochrany osobných údajov. Nie je povinnosťou pre každého prevádzkovateľa. Nový prístup zodpovednosti znamená, že prevádzkovateľ je zodpovedný za dodržiavanie zásad spracúvania a zároveň prevádzkovateľ musí byť schopný kedykoľvek tento súlad aj preukázať. Na preukázanie súladu s novou právnou úpravou môže slúžiť dodržiavanie schváleného kódexu správania, dodržiavanie certifikačného mechanizmu, záznamy o spracovateľských činnostiach, ale napríklad aj dokumenty preukazujúce implementovanie politiky ochrany a bezpečnosti dát. Komplexnosť dokumentácie záleží od okolností a rizikovosti konkrétneho spracúvania.

26. Posúdenie vplyvu na ochranu údajov. Podľa čl. 35 ods. 1 Nariadenia/§ 42 ods. 1 zákona č. 18/2018 Z. z. je **každý prevádzkovateľ** povinný vykonať právnu analýzu s poukazom identifikovania tých **spracovateľských operácii**, u ktorých je predpoklad, že povedú k **vysokému riziku** pre práva a slobody fyzických osôb. Ak takéto spracovateľské operácie prevádzkovateľ identifikuje, len vtedy je povinný pristúpiť k vypracovaniu **posúdenia vplyvu**, ktorého obsahové náležitosti sú vymedzené v čl. 35 ods. 7 Nariadenia/§ 42 ods. 4 zákona č. 18/2018 Z. z., a čoho súčasťou je aj analýza rizík. V čl. 35 ods. 3 Nariadenia/§ 42 ods. 3 zákona č. 18/2018 Z. z sa uvádza niekoľko príkladov, kedy spracovateľská operácia povedie k vysokému riziku a bude sa vyžadovať posúdenie vplyvu. Je potrebné vychádzať aj z vyhlášky úradu, ktorá bude obsahovať výpočet spracovateľských operácií, pri ktorých bude potrebné vypracovať posúdenie vplyvu tzv. blacklist spracovateľských operácií.

27. Predchádzajúca konzultácia - je povinná pred začatím samotného spracúvania a len ak z posúdenia vplyvu vyplýva, že zostatkové „zvyškové„ riziko spracúvania na práva a slobody fyzických osôb, aj po prijatí bezpečnostných opatrení na ich zmiernenie, je naďalej vysoké.

- Cieľom predchádzajúcej konzultácie je len usmernenie, alebo návrh možných ďalších opatrení, nie získať súhlas/ povolenie úradu na spracúvanie
- Zodpovednosť za spracúvanie je naďalej na prevádzkovateľovi

28. Incident management

Zavedie sa:

- postup pri ohlasovaní bezpečnostných incidentov a zistených zraniteľných miest na účel včasného prijatia preventívnych alebo nápravných opatrení
- evidencia bezpečnostných incidentov a použitých riešení
- identifikácia (oznámením alebo na základe monitoringu) a odstraňovanie následkov bezpečnostných incidentov
- analýza incidentu: cieľom vyhodnotiť, či bezpečnostný incident je/nie je zároveň aj porušením ochrany osobných údajov
- oznamovacia povinnosť voči úradu, v prípade ak došlo k porušeniu ochrany osobných údajov do 72 hod.
- oznamovacia povinnosť voči dotknutým osobám- bez zbytočného odkladu, ak sa vyhodnotí vysoké riziko pre práva a slobody dotknutých osôb.
- implementácia nápravných opatrení
- obnova dostupnosti osobných údajov (účinné je preto zálohovanie)
- prevencia.

29. Vykonávam cezhraničné spracúvanie ale prenosy osobných údajov do tretích krajín? Voľný pohyb osobných údajov medzi Slovenskou republikou a členskými štátmi EÚ sa zaručuje; základným predpokladom spracúvania osobných údajov pri akejkoľvek spracovateľskej operácii s osobnými údajmi, tak v rámci EÚ ako i mimo nej, je splnenie princípu zákonnosti, teda musí byť založené na legálnom právnom základe podľa čl. 6 ods. 1 Nariadenia/§ 13 ods. 1 zákona č. 18/2018 Z. z.

30. Dobrovoľná možnosť certifikácie, akreditácie, zavedenie kódexu správania

UPOZORNENIE: Tento postup nie je univerzálne použiteľný. Záleží od zložitosti jednotlivých procesov a objemu spracúvaných osobných údajov.

Materiál nie je právne záväzný, má len odporúčací charakter nakoľko prostredie každého prevádzkovateľa, či sprostredkovateľa je jedinečné a vyžaduje zohľadnenie konkrétnych odlišností.