Realitné právo:
Ochrana osobných údajov

Súčasná právna úprava v oblasti ochrany osobných údajov

Od 25.05.2018 vstúpilo do účinnosti **Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR)**. GDPR prinieslo niekoľko zmien, pričom toto nariadenie je ešte doplnené slovenským zákonom o ochrane osobných údajov č. 18/2018 Z. z., ktorý taktiež vstúpil do účinnosti 25.05.2018. Pri všetkých odkazoch na plnenie povinností prevádzkovateľa preto bude potrebné uvádzať ako relevantný predpis GDPR, okrem situácií, ktoré sú predmetom úpravy § 78 nového zákona č. 18/2018 Z. z. o ochrane osobných údajov.

Pôsobnosť GDPR

Účelom GDPR nie je regulácia spracúvania osobných údajov, ktoré spracúvajú pre svoju osobnú potrebu jednotlivci, napr. v rámci vedenia osobného adresára alebo korešpondencie. Inak sa GDPR vzťahuje na spracúvanie všetkých osobných údajov.

Osobný údaj

V zmysle GDPR je možné za osobný údaj považovať akýkoľvek údaj týkajúci sa fyzickej osoby, ktorú možno určiť priamo alebo nepriamo. Takto pomerne široko koncipovaná definícia umožňuje dozornému orgánu aplikovať vzťahujúce sa zákonné ustanovenia s prihliadnutím na špecifické okolnosti každého prípadu.

Osobným údajom teda rozumieme:

- **akúkoľvek informáciu**
- **týkajúcu sa**
- **identifikovanej a/alebo identifikovateľnej**
- **fyzickej osoby**

Tieto **4 zložky** musia byť splnené súčasne, aby bolo možné daný údaj klasifikovať ako osobný údaj, a tým pádom aplikovať aj GDPR. Pod priamou identifikáciou rozumieme presné určenie danej osoby, napr. na základe mena, priezviska a rodného čísla; pod nepriamou identifikáciou rozumieme identifikáciu napr. na základe dedukčnej alebo vylučovacej metódy.

Osobitná kategória osobných údajov sú tzv. „citlivé“ osobné údaje odhaľujúce najmä etnický pôvod, politické názory alebo údaje týkajúce sa zdravia. Nakoľko sa jedná o osobné údaje, ktoré by v prípade zneužitia mohli predstavovať závažnejší zásah do práv a právom chránených záujmov dotknutých osôb, GDPR stanovuje pre spracúvanie tejto kategórie osobných údajov prísnejšie kritériá. Medzi tieto kategórie patria osobné údaje odhaľujúce rasový alebo etnický pôvod, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách a taktiež spracúvanie genetických, biometrických údajov a údajov týkajúcich sa zdravia alebo sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

Osobnými údajmi sú aj adresa elektronickej pošty, telefónne číslo konkrétnej osoby a všetky ostatné informácie, ktoré sú spojiteľné s konkrétnou fyzickou osobou (údaje o kupovanej nehnuteľnosti, adresa, identifikačné údaje, číslo bankového účtu...)

Pozn.: rodné číslo nie je považované za osobitnú kategóriu osobných údajov

Právny základ spracúvania osobných údajov

Právny základ, resp. oprávnenie spracúvať osobné údaje je základným predpokladom zákonného postupu pri spracúvaní osobných údajov.

Právnym základom podľa GDPR môže byť:

- súhlas dotknutej osoby
- plnenie zmluvy, ktorej je dotknutá osoba zmluvnou stranou alebo v rámci predzmluvných vzťahov
- osobitný zákon, právne záväzný akt Európskej únie, medzinárodná zmluva, ktorou je SR viazaná
- ochrana životne dôležitých záujmov dotknutej alebo inej fyzickej osoby
- spracúvanie osobných údajov na splnenie úlohy realizovanej vo verejnom záujme
- oprávnený záujem prevádzkovateľa alebo tretej strany s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva dotknutej osoby

Poznámka: Je potrebné zrevidovať všetky osobné údaje, ktoré spoločnosť spracúva a zistiť, či na ich spracúvanie má právny základ. Najčastejšie je právnym základom súhlas dotknutej osoby (klienta) alebo s ňou uzatvorená zmluva, prípadne zákon pre údaje týkajúce sa pracovnoprávneho vzťahu alebo vedenie účtovníctva.

Subjekty zúčastňujúce sa procesu spracúvania osobných údajov

Jednou zo základných predpokladov správnej aplikácie GDPR je korektné vymedzenie postavenia jednotlivých subjektov, ktoré sú začlenené do procesu spracúvania. Tento základný predpoklad je dôležitý aj pre výkon práv osôb, ktorých osobné údaje sú spracúvané ako aj pre ostatné subjekty, ktorým z ich postavenia plynú určité povinnosti voči dozornému orgánu.

GDPR definuje ako:

- **dotknutú osobu** – každú fyzickú osobu, ktorej sa osobné údaje týkajú (zamestnanec, klient, záujemca o ponuku...)

- **prevádzkovateľa** – každého, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, podmienky ich spracúvania alebo ak ho za prevádzkovateľa ustanoví osobitný zákon (realitná kancelária, zamestnávateľ, realitný maklér pracujúci na živnosť...)

- **sprostredkovateľa** – každého, kto spracúva osobné údaje v mene prevádzkovateľa, v rozsahu a za podmienok dojednaných s prevádzkovateľom v zmluve alebo obdobnom právnom akte (účtovník, poskytovateľ marketingu, realitný maklér pracujúci na živnosť...),

- **tretiu stranu** – fyzická alebo právnická osoba a orgán verejnej moci a každý, kto nie je dotknutou osobou, prevádzkovateľom, jeho zástupcom alebo sprostredkovateľom (Sociálna poisťovňa, zdravotná poisťovňa...)
- **príjemcu** – každého, komu sú osobné údaje sprístupnené, pričom príjemcom môže byť aj tretia strana.

Dotknutá osoba a jej práva

Dotknutej osobe priznáva GDPR niekoľko práv, pričom niektoré boli upravené už predchádzajúcim zákonom (právo na prístup k osobným údajom) a niektoré sú obmenené, resp. úplne nanovo upravené.

Dotknutá osoba si môže u prevádzkovateľa uplatniť nasledovné práva

- právo na prístup k údajom
- právo na opravu
- právo na vymazanie (zabudnutie)
- právo na prenosnosť údajov
- právo namietať

Prevádzkovateľ

Prevádzkovateľ je subjektom nesúcim hlavnú časť zodpovednosti za spracúvanie osobných údajov v súlade s GDPR. Povinnosti prevádzkovateľa vyplývajú najmä z podmienok jeho činnosti a spracúvania osobných údajov. Každý prevádzkovateľ však musí disponovať spôsobilým právnym základom na výkon spracovateľských operácií, ktoré realizuje.

Sprostredkovateľ

Sprostredkovateľ spracúva osobné údaje v mene prevádzkovateľa na základe zmluvy, v ktorej si môžu bližšie dohodnúť podmienky výkonu jeho funkcie. S každým sprostredkovateľom musí prevádzkovateľ uzatvoriť zmluvu s nasledovnými náležitosťami:

- **deklarácia,** že osobné údaje sprostredkovateľ spracúva **iba na základe zdokumentovaných pokynov** prevádzkovateľa
- zabezpečenie toho, aby oprávnené osoby zachovávali **dôvernosť informácií** povinnosť dodržať podmienky prijať primerané **bezpečnostné opatrenia**
- **záväzok dodržať podmienky** zapojenia **ďalšieho sprostredkovateľa**
- **záväzok pomáhať prevádzkovateľovi** vhodnými technickými a organizačnými opatreniami pri plnení povinnosti reagovať na žiadosti o výkon práv dotknutej osoby
- záväzok pomôcť splniť si **povinnosť prijať primerané bezpečnostné opatrenia** na spracúvanie osobných údajov s prihliadnutím na povahu spracúvania a sprostredkovateľovi dostupné informácie
- záväzok po ukončení poskytovania služieb týkajúcich sa spracúvania všetky osobné **údaje vymazať alebo vrátiť prevádzkovateľovi**, ak tak umožňuje právo EÚ alebo osobitný predpis
- **záväzok poskytnúť** prevádzkovateľovi všetky vyššie uvedené informácie na preukázanie splnenia tejto povinnosti a umožnenie auditu, ako aj kontroly vykonávanej prevádzkovateľom alebo iným audítorom

Poznámka: poverenie sprostredkovateľa už nie je nevyhnutné vykonať písomnou zmluvou. Bude však potrebné existujúce zmluvy dodatkovať, alebo uzatvoriť nové tak, aby obsahovali všetky predpísané náležitosti.

Zodpovedná osoba

Prevádzkovateľ je povinný zodpovednú osobu vymenovať iba, ak je splnený aspoň jeden predpoklad z nasledovného:

- prevádzkovateľ spracúva osobné údaje ako orgán verejnej moci alebo verejnoprávny subjekt hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu
- hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií osobných údajov vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky

Pre všetkých ostatných prevádzkovateľov nie je povinnosť určiť zodpovednú osobu. Predpoklady výkonu funkcie zodpovednej osoby sú jej odborné kvality, a to najmä jej odborné znalosti z oblasti práva a postupov v oblasti ochrany osobných údajov. Táto osoba môže byť interný zamestnanec prevádzkovateľa, ale aj externá zodpovedná osoba. Zodpovedná osoba už nebude povinná absolvovať skúšku na Úrade na ochranu osobných údajov SR.

Informačná povinnosť prevádzkovateľa

Ak sa od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, je prevádzkovateľ povinný poskytnúť dotknutej *oso*be pri ich získavaní

- identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený,
- kontaktné údaje zodpovednej osoby, ak je určená, účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov,
- oprávnené záujmy prevádzkovateľa alebo tretej strany, ak sa osobné údaje spracúvajú podľa na tomto právnom základe,
- identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje,
- informáciu o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii, identifikáciu tretej krajiny alebo medzinárodnej organizácie, informáciu o existencii alebo neexistencii rozhodnutia Európskej komisie o primeranosti alebo odkaz na primerané záruky alebo vhodné záruky a prostriedky na získanie ich kópie alebo informáciu o tom, kde boli sprístupnené.

Okrem informácií podľa predchádzajúceho odseku je prevádzkovateľ povinný pri získavaní osobných údajov poskytnúť dotknutej osobe informácie o

- dobe uchovávania osobných údajov; ak to nie je možné, informácie o kritériách jej určenia,
- práve požadovať od prevádzkovateľa prístup k osobným údajom týkajúcich sa dotknutej osoby,
- práve na opravu osobných údajov, o práve na vymazanie osobných údajov alebo o práve na obmedzenie spracúvania osobných údajov, o práve namietať spracúvanie osobných údajov,
- ako aj o práve na prenosnosť osobných údajov,
- práve kedykoľvek svoj súhlas odvolať,
- práve podať sťažnosť dozornému orgánu,
- tom, či je poskytovanie osobných údajov zákonnou požiadavkou alebo zmluvnou požiadavkou alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, a o tom, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj o možných následkoch neposkytnutia osobných údajov,
- existencii automatizovaného individuálneho rozhodovania vrátane profilovania; v týchto v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.

Ak osobné údaje neboli získané od dotknutej osoby, prevádzkovateľ je povinný dotknutej osobe poskytnúť

- identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený,
- kontaktné údaje zodpovednej osoby, ak je určená,
- účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov,
- kategórie spracúvaných osobných údajov,
- identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje,
- informáciu o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii, identifikáciu tretej krajiny alebo medzinárodnej organizácie,
- informáciu o existencii alebo neexistencii rozhodnutia Komisie o primeranosti alebo odkaz na primerané záruky alebo vhodné záruky a prostriedky na získanie ich kópie alebo informáciu o tom, kde boli sprístupnené

Okrem informácií podľa predchádzajúceho odseku je prevádzkovateľ povinný poskytnúť dotknutej osobe informácie o

- dobe uchovávania osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia,
- oprávnených záujmoch prevádzkovateľa alebo tretej strany, ak sa spracúvajú osobné údaje podľa tohto právneho základu,
- práve požadovať od prevádzkovateľa prístup k osobným údajom týkajúcich sa dotknutej osoby,
- o práve na opravu osobných údajov,
- o práve na vymazanie osobných údajov
- alebo o práve na obmedzenie spracúvania osobných údajov,
- o práve namietať spracúvanie osobných údajov,
- o práve na prenosnosť osobných údajov,
- práve kedykoľvek svoj súhlas odvolať,
- práve podať sťažnosť dozornému orgánu,
- zdroji, z ktorého pochádzajú osobné údaje, prípadne informácie o tom, či pochádzajú z verejne prístupných zdrojov,
- existencii automatizovaného individuálneho rozhodovania vrátane profilovania podľa čl. 22 ods. 1 a 4; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použitom postupe, ako aj o význame automatizovaného individuálneho rozhodovania a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.

Prevádzkovateľ je povinný poskytnúť vyššie uvedené informácie

- najneskôr do jedného mesiaca po získaní osobných údajov, pričom zohľadní konkrétne okolnosti, za ktorých sa osobné údaje spracúvajú,
- najneskôr v čase prvej komunikácie s touto dotknutou osobou, ak sa osobné údaje majú použiť na komunikáciu s dotknutou osobou, alebo
- najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú, ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi.

Poznámka: rozsah informačnej povinnosti je značne rozsiahly a je to jedna zo základných povinností prevádzkovateľa. V praxi sa zvykne plniť prostredníctvom všeobecných obchodných podmienok pripojených k zmluve alebo súhlasu, alebo odkazom na webovú stránku, kde sú tieto informácie zverejnené

Bezpečnosť

Prevádzkovateľ a sprostredkovateľ sú povinní prijať so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej tomuto riziku, pričom uvedené opatrenia môžu zahŕňať najmä

- pseudonymizáciu a šifrovanie osobných údajov,
- zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov,
- proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu,
- proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.

Pri posudzovaní primeranej úrovne bezpečnosti sa **prihliada na riziká,** ktoré predstavuje spracúvanie osobných údajov, a to najmä náhodné zničenie alebo nezákonné zničenie, strata, zmena alebo neoprávnené poskytnutie prenášaných osobných údajov, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo neoprávnený prístup k takýmto osobným údajom.

Splnenie vyššie uvedených povinností možno aj **schváleným kódexom správania** alebo **certifikátom** podľa príslušných ustanovení GDPR.

Bežní prevádzkovatelia preukazujú splnenie povinnosti prijať primerané bezpečnostné opatrenia prostredníctvom interných smerníc spoločnosti, ktoré riešia prístupové práva zamestnancov, správanie sa na pracovisku a mimo neho, pravidlá práce s osobnými údajmi mimo pracovisko, pravidlá pri spôsobení bezpečnostného incidentu, atď.

Poznámka: už nie je povinnosť vypracovávať bezpečnostný projekt. Je ho však možné použiť pri spracovávaní bezpečnostných opatrení podľa GDPR. Prevádzkovateľ a sprostredkovateľ budú musieť hlavne preukázať primeranosť prijatých bezpečnostných opatrení.

Posúdenie vplyvu na ochranu osobných údajov

Ak typ spracúvania osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účel spracúvania osobných údajov, môže viesť k vysokému riziku pre práva fyzických osôb, prevádzkovateľ je povinný pred spracúvaním osobných údajov vykonať posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziko, postačí jedno posúdenie.

Posúdenie vplyvu na ochranu osobných údajov sa vyžaduje najmä, ak ide o

- systematické a rozsiahle hodnotenie osobných znakov alebo charakteristík týkajúcich sa dotknutej osoby, ktoré je založené na automatizovanom spracúvaní osobných údajov vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa dotknutej osoby alebo s podobne závažným vplyvom na ňu,
- spracúvanie vo veľkom rozsahu osobitných kategórií osobných údajov alebo osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku, alebo
- systematické monitorovanie verejne prístupných miest vo veľkom rozsahu.

Predchádzajúca konzultácia

Prevádzkovateľ je povinný s úradom uskutočniť konzultáciu pred spracúvaním osobných údajov, ak je z posúdenia vplyvu na ochranu osobných údajov zrejmé, že spracúvanie osobných údajov povedie k vysokému riziku pre práva fyzických osôb, ak prevádzkovateľ neprijme opatrenia na zmiernenie tohto rizika.

Oznámenie porušenia ochrany osobných údajov úradu

Prevádzkovateľ je povinný oznámiť úradu porušenie ochrany osobných údajov **do 72 hodín po tom, ako sa o ňom dozvedel**; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby (v tomto prípade nie je potrebné oznamovať porušenie vôbec).

Oznámenie musí obsahovať najmä

- opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
- kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
- opis pravdepodobných následkov porušenia ochrany osobných údajov,
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

Oznámenie porušenia ochrany osobných údajov dotknutej osobe

Prevádzkovateľ je povinný **bez zbytočného odkladu** oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby.

Oznámiť je potrebné

- kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
- opis pravdepodobných následkov porušenia ochrany osobných údajov,
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

Oznámenie podľa vyššie uvedeného sa nevyžaduje, ak

- prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a uplatnil ich na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä šifrovanie alebo iné opatrenia, na základe ktorých sú osobné údaje nečitateľné pre osoby, ktoré nie sú oprávnené mať k nim prístup,
- prevádzkovateľ prijal následné opatrenia na zabezpečenie vysokého rizika porušenia práv dotknutej osoby,

- by to vyžadovalo neprimerané úsilie; prevádzkovateľ je povinný informovať verejnosť alebo prijať iné opatrenie na zabezpečenie toho, že dotknutá osoba bude informovaná rovnako efektívnym spôsobom.

Registrácia a osobitná registrácia informačných systémov

Tieto povinnosti boli zrušené s účinnosťou od 25.05.2018 a neboli nahradené žiadnou obdobnou povinnosťou.

Povinnosť vedenia záznamov o spracovateľských činnostiach

Táto povinnosť sa vzťahuje iba na prevádzkovateľov, ktorí majú viac ako 250 zamestnancov a nie je pravdepodobné, že spracúvanie povedie k riziku pre dotknuté osoby.

Súvisiace predpisy

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov

- Zákon č. 18/2018 Z. z. ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Záver

Za účelom zosúladenia podmienok, za ktorých prevádzkovateľ spracúva osobné údaje s požiadavkami GDPR, je potrebné najmä

- zrevidovať, či prevádzkovateľ má na všetky spracúvané osobné údaje právny základ (súhlas, zmluva, zákon...)
- skontrolovať, či pri získavaní osobných údajov prevádzkovateľ poskytuje dotknutým osobám požadované informácie o spracúvaní osobných údajov
- analyzovať všetky subjekty, ktorým poskytuje prevádzkovateľ osobné údaje a identifikovať, či je možné tieto údaje poskytovať (či je na to právny základ) a pokiaľ sa jedná o sprostredkovateľa (napríklad externý účtovník, poskytovateľ marketingu, poskytovateľ cloud úložiska...) zistiť, či s ním uzatvorená zmluva má všetky náležitosti podľa GDPR
- spracovať interné smernice (alebo inak nazvané pravidlá), na základe ktorých spoločnosť prijme primerané bezpečnostné opatrenia na ochranu spracúvaných osobných údajov