JURÁŠ
CHOVANCOVÁ
DAVID
advokáti v.o.s.

OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

GDPR

Základní informace

1. Právní rámec

Oblast zpracování a ochrany osobních údajů je v České republice v současné době upravena zákonem č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOÚ“), který plně implementoval směrnici Evropského parlamentu a Rady č. 95/46/ES ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu údajů.

ZOOÚ bude v plném rozsahu nahrazen Nařízením Evropského parlamentu a rady (EU) 2016/679 ze dne 27.4.2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“), **a to ke dni 25.5.2018**. Vzhledem k tomu, že nařízení je přímo aplikovatelné v členských státech EU, není nutné, aby došlo k implementaci do obecně závazného právního předpisu.

GDPR však nechává v některých oblastech možnost právní úpravy jednotlivými členskými státy. V této souvislosti je nyní v poslanecké sněmovně návrh tzv. adaptačního zákona – zákon o zpracování osobních údajů, který bude některá práva a povinnosti založená GDPR upravovat.

Současná právní úprava ochrany osobních údajů zakotvená v ZOOÚ obsahuje a upravuje většinu institutů a povinností, které GDPR vyžaduje, a to s ohledem na to, že implementovala směrnice ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu osob a GDPR na tuto směrnice navazuje.

Druhý moment, který je nutné vnímat je skutečnost, že dle GDPR se bude postupovat pouze tehdy, dochází-li ke zpracování osobních údajů. Půjde-li o ochranu soukromí v širším slova smyslu, bude se nadále postupovat dle právní úpravy obsažené v občanském zákoníku.

2. Významné definice a pojmy

Osobní údaj

- jeho definice se nemění a zůstává ve stejném rozsahu, jak je uvedena v ZOOÚ. Není na místě citovat znění tohoto ustanovení, ve stručnosti je osobním údajem jakýkoliv údaj, na základě kterého je možné identifikovat fyzickou osobu; za zmínku např. stojí to, že nově se ve výčtu již konkrétně objevují i lokační údaje (GPS) a síťový identifikátor (IP);
- v této souvislosti je nutné zmínit, že ochrana se nevztahuje na údaje právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby a dále na osobní údaje zesnulých osob.

Zvláštní kategorie osobních údajů

- jedná se pouze o nový název pro dnes známou kategorii tzv. citlivých údajů, kdy její definice opět odpovídá definici citlivých údajů obsažených v ZOOÚ, do výčtu jsou doplněny genetické a biometrické údaje; *příkladmo jde o osobní údaje, které vypovídají o rasovém či etnickém původu, zdravotním stavu atd.*

Správce osobních údajů

- fyzická nebo právnická osoba, která zpracovává osobní údaje a určuje účel a prostředky zpracování osobních údajů;

Zpracovatel osobních údajů
- fyzická nebo právnická osoba, která zpracovává osobní údaje pro správce.

Z hlediska praxe je zcela běžné, že správce osobních údajů využívá zpracovatele osobních údajů. Mezi správcem a zpracovatelem musí při zpracování osobních údajů existovat písemné ujednání, zpravidla součástí smlouvy, které vymezí pro zpracovatele podmínky zpracování osobních údajů. GDPR zakazuje řetězení zpracovatelů osobních údajů bez souhlasu správce.

3. Zásady zpracování osobních údajů

GDPR je postaveno na novém základním principu, kterým je **princip odpovědnosti**, který vyjadřuje to, že právě správce je ta osoba, která odpovídá za dodržování GDPR a zároveň je povinen doložit soulad zpracování osobních údajů s GDPR.

Při jakémkoliv zpracování osobních údajů musí správce dodržovat zásady zpracování osobních údaj, které fakticky vyjadřují podmínky pro zpracování osobních údajů a jedná se o:

a) zákonnost, korektnost a transparentnost
- tato zásada odráží jednak povinnost správce provádět zpracování zákonným způsobem, tj. na základě právem předvídaných právních důvodů, k tomu viz. níže,
- správce nesmí zastírat důvod zpracování, tj. subjekt údajů by měl mít relevantní informace o zpracování.

b) omezení účelu
- osobní údaje mohou být shromažďovány a zpracovány pro výslovně vyjádřené a legitimní účely; tj. správce si určí, z jakého důvodu bude osobní údaje zpracovávat a pouze za takto vymezeným účelem tyto údaje zpracovávat,
- účel zpracování může vyplývat přímo ze zákona nebo je zřejmý z plnění smlouvy, pokud jde o ostatní účely, je nutné je vymezit tak, aby bylo zřejmé, jaká zpracování na základě nich budou probíhat. To vše musí učinit správce dříve, než začne shromažďovat a zpracovávat osobní údaje.

c) minimalizace údajů
Správce může zpracovávat pouze ty osobní údaje, které jsou vzhledem k účelu zpracování relevantní, a pouze v rozsahu, který je pro naplnění účelu nezbytný.

d) přesnost
Osobní údaje zpracovávané správcem mají odpovídat skutečnosti a v případě potřeby by měly být aktualizovány. Skutečnost, že údaje mají být přesné neznamená, že musí být pravdivé, tj. správce nebude odpovídat za to, že mu subjekt údajů sdělí nepravdivé údaje. Taktéž platí, že sám správce není povinen vyhledávat nepřesné údaje, pokud však správce zjistí, že zpracovává nepřesné údaje, měl by učinit vhodná opatření k jejich nápravě a takto nepřesné osobní údaje dále nezpracovávat.

e) omezení uložení
Tato zásada odráží povinnost správce uchovávat osobní údaje pouze po dobu, která je nezbytná pro účely, pro které jsou zpracovány.

f) integrita a důvěrnost
Správce je povinen při zpracovávání osobních údajů přijmout náležité zabezpečení, a to pomocí vhodných technických a organizačních opatření.

4. Právní důvody zpracování

Jak již bylo shora uvedeno, pro zpracování osobních údajů platí základní zásada a to zákonnost, která vyjadřuje tu skutečnost, že správce může provádět zpracování osobních údajů pouze na základě stanoveného právního důvodu. GDPR stanovuje, že zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek:

a) subjekt údajů **udělil souhlas** se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
b) zpracování je nezbytné pro **splnění smlouvy**, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
c) zpracování je nezbytné pro **splnění právní povinnosti**, které se na správce vztahuje;
d) zpracování je nezbytné pro **ochranu životně důležitých zájmů subjektu údajů** nebo jiné fyzické osoby;
e) zpracování je nezbytné pro **splnění úkolu prováděného ve veřejném zájmu** nebo při výkonu veřejné moci, kterým je správce pověřen;
f) zpracování je nezbytné **pro účely oprávněných zájmů příslušného správce** či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadujících ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

Není vyloučeno, že správce může mít souběžně více právních důvodů pro zpracování. Pokud však nastane situace, že správci tento právní důvod odpadne, musí následovat likvidace osobních údajů.

GDPR přináší zpřísnění podmínek pro udělení souhlasu pro zpracování osobních údajů subjektu, kdy takový souhlas

- musí být svobodný – dobrovolný, informovaný a obsahují jednoznačný projev vůle subjektu údajů,
- správce musí být schopen doložit, že mu takový souhlas byl udělen,
- souhlas musí být psán srozumitelně a jednoduše, je například vyloučeno, aby byl součástí VOP, je-li v textu smlouvy, měl by být oddělen od ostatního textu, se zdůrazněním, že je o souhlas se zpracováním osobních údajů,
- u souhlasu musí správce vždy počítat s tím, že jej může subjekt údajů kdykoliv odvolat.

5. Práva subjektu údajů

Důvodem zavedení těchto institutů je vyvážení vztahu mezi správcem a subjektem údajů, jehož údaje jsou zpracovávány. Většinu těchto práva obsahuje ZOOÚ, nově se přidává právo na přenositelnost.

a) informovanost subjektu
Povinnost správce informovat subjekt údajů o rozsahu zpracování osobních údajů je odrazem zásady transparentnosti, tj. subjekt údajů by měl získat minimální údaje o totožnosti správce, účelu zpracování, vymezení oprávněného zájmu, pokud je tento podkladem pro zpracování, příjemci údajů, pokud je správce dál předává, době uložení, právech subjektu, odvolání souhlasu, existence práva na stížnost.

b) právo na přístup
Jedná se o právo subjektu údajů získat od správce potvrzení, zda zpracovává jeho osobní údajů a pokud ano, má právo žádat o sdělení pro jaké účely, kategorie dotčených osobních údajů, příjemci, době uložení. Nadto má právo získat i kopii zpracovaných osobních údajů.

c) právo na opravu
Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.

d) právo na výmaz („právo být zapomenut“)
Uvedené odráží právo subjektu údajů, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost bez zbytečného odkladu vymazat, pokud je dán některý z důvodů uvedených v čl. 17 odst. 1 GDPR, zejména nejsou potřebné pro účely, pro které byly shromážděny, subjekt odvolá souhlas, vznese námitky, byly zpracovány protiprávně.

Výjimka je stanovena pro případ, kdy správce nemusí osobní údaje vymazat, pokud osobní údaje správce potřebuje pro výkon nebo obhajobu právních nároků.

Pokud by na základě některé z výjimek uvedených v čl. 17 odst. 3 GDPR správce odmítl provést výmaz, je povinen do jednoho měsíce od doručení žádosti o tomto odmítnutí subjekt údajů informovat, užití výjimky řádně odůvodnit a poučit subjekt údajů o právu podat stížnost u dozorového úřadu (čl. 77 GDPR) nebo se proti takovému odmítnutí bránit u soudu (čl. 79 GDPR).

e) právo na omezení zpracování
Subjekt údajů má právo na to, aby správce omezil zpracování osobních údajů, které se ho týkají, za předpokladu, že jsou splněny podmínky uvedené v čl. 18 odst. 1 GDPR, tj.

- subjekt popírá přesnost osobních údajů, a to na dobu potřebnou tomu, aby správce mohl přednost osobních údajů ověřit,
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití,
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků.

f) právo na přenositelnost údajů
Jedná se novou právní úpravu, jejímž cílem je umožnit převádění osobních údajů mezi správci. Právo na přenositelnost se projevuje dvěma způsoby:

a) jako právo subjektu údajů získat, tedy zejména stáhnout od správce své osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu, a
b) jako právo na přímé poskytnutí osobních údajů původním správcem správci jinému.

Právo na přenositelnost údajů lze uplatnit pouze pokud je zpracování osobních údajů prováděno automatizovaně a zároveň je založeno na souhlasu dle čl. 6 odst. 1 písm. a) GDPR nebo čl. 9 odst. 2 písm. a) nebo na smlouvě podle čl. 6 odst. 1 písm. b) GDPR.

g) právo vznést námitku
Právo vznést námitku směřuje na situace, kdy subjekt údajů neměl možnost ovlivnit to, že jsou jeho údaje zpracovány, a zároveň se nejedná o plnění právní povinnosti nebo životně důležitý zájem, kdy je tato nemožnost obhajitelná. Subjekt údajů má takto možnost vznést tři druhy námitek proti zpracování:

a) zpracování na základě právního titulu oprávněného zájmu a plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci,
b) zpracování pro účely přímého marketingu na základě právního titulu oprávněného zájmu. Jakmile subjekt údajů tuto námitku vznese, musí správce přestat osobní údaje subjektu údajů pro účely přímého marketingu zpracovávat, a
c) zpracování pro účely vědeckého či historického významu nebo pro statistické účely.

Správce má povinnost subjekt údajů výslovně upozornit, že má právo podat námitku proti zpracování na základě oprávněného zájmu či plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci a námitku proti zpracování pro účely přímého marketingu. Upozornění musí provést nejpozději v okamžiku první komunikace se subjektem údajů a musí být uvedeno zřetelně a odděleně od jakýchkoli jiných informací.

Pokud správce obdrží žádost dle čl. 15 až 22 GDPR musí ji zpracovat, posoudit a odpovědět na ni bez zbytečného odkladu. Nejpozději musí správce informovat žadatele o přijatých opatřeních, odmítnutí nebo prodloužení lhůty **do jednoho měsíce poté, co je mu žádost doručena,** kterou lze ve výjimečných případech prodloužit (čl. 12 odst. 3 GDPR).

Pokud správce vyhodnotí, že žádost nesplňuje předpoklady pro její kladné vyřízení, dle požadavků stanovených v čl. 15 až 22 GDPR může žádost odmítnout. V takovém případě však musí do jednoho měsíce od obdržení žádosti subjektu údajů informovat o důvodech odmítnutí a zároveň jej musí poučit o možnosti podat stížnost u dozorového úřadu dle čl. 77 GDPR a o právu žádat o soudní ochranu dle čl. 79 GDPR.

6. Ohlašování případů porušení zabezpečení osobních údajů

Správce je povinen dle čl. 33 GDPR ohlásit dozorovému úřadu, kterým je Úřad pro ochranu osobních údajů, jakékoli porušení zabezpečení osobních údajů, a to bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. Správce není povinen ohlášení provádět, pokud je nepravděpodobné, že by porušení mělo za následek riziko pro práva a svobody fyzických osob, vždy je však povinen porušení zabezpečení zdokumentovat.

Porušením zabezpečení osobních údajů se rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. V případě, že porušení zabezpečení představuje vysoké riziko pro práva a svobody subjektu údajů, vzniká správci povinnost oznámit tuto událost subjektu údajů.

7. Ostatní

Kromě shora uvedeného přináší GDPR pro správce i další povinnosti. Na místě je nutné určitě zmínit:

a) povinnost správce vést **záznamy o činnostech zpracování** ve smyslu čl. 30 GDPR. Náležitosti těchto záznamů jsou stanoveny v čl. 30 odst. 1 písm. a) až g) GDPR. Záznamy musí být vyhotovovány písemně, přičemž za písemnou formu se považuje i forma elektronická. Povinnost vést záznamy se vztahuje i na zpracovatele, a to v rozsahu dle čl. 30 odst. 2 GDPR.

   Povinnost vést záznamy se nevztahuje na podniky a organizace zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštní kategorie údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10 GDPR.

b) povinnost provádět **posouzení vlivu na ochranu osobních údajů** v rozsahu dle čl. 35 odst. 7 GDPR, které se vztahuje na:

   aa) zpracování popsané v čl. 35 odst. 3 písm. a), b) nebo c) GDPR,
   ab) zpracování, které označil za rizikové dozorový úřad v souladu s čl. 35 odst. 4 GDPR,
   ac) zpracování, u kterého existuje pravděpodobnost, že bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

   Pro každou zamýšlenou operaci zpracování tak správce musí provést prvotní posouzení, zda nespadá do některého z výše uvedených případů. K tomu lze samozřejmě opět doporučit písemné zdokumentování tohoto, že správce toto prvotní posouzení provedl.

c) povinnost správce konzultovat s dozorujícím úřadem, a to před zpracováním, pokud z posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR vyplyne, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika.

   Konzultace s dozorujícím úřadem se provádí na základě žádosti, kdy správce musí dozorujícímu úřadu poskytnout informace v rozsahu uvedeném v čl. 36 odst. 3 GDPR. O výsledku posouzení informuje dozorující úřad správce do osmi týdnů od obdržení žádosti (lhůtu může dozorující úřad prodloužit).

d) povinnost jmenovat **pověřence pro ochranu osobních údajů,** kterou mají ty organizace, kterou splní alespoň jednu z podmínek uvedených v čl. 37 odst. 1 GDPR.