Právní rámec

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů; dále jen jako „GDPR"), které nabývá účinnosti 25. května 2018 a **Zákon č. 110/2019 Sb., o zpracování osobních údajů** a o změně některých zákonů, ve znění pozdějších předpisů, který nabyl účinnosti 24. dubna 2019, představuje základ legislativní úpravy rámci ochrany osobních údajů v Evropské unii a samozřejmě i v ČR.

Dále ochranu osobních údajů upravují i některé další právní předpisy, např.

- Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108, vyhlášená pod č. 115/2001 Sb. m. s.
- Zákon č. 277/2009 Sb., o pojišťovnictví, ve znění pozdějších předpisů
- Zákon č. 170/2018 Sb., o distribuci pojištění a zajištění, ve znění pozdějších předpisů
- Zákon č. 37/2004 Sb., o pojistné smlouvě a o změně souvisejících zákonů, ve znění pozdějších předpisů
- Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů
- Zákon č. 164/2013 Sb., o mezinárodní spolupráci při správě daní a o změně dalších souvisejících zákonů
- Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů
- Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
- Zákon České národní rady č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů
- Zákon České národní rady č. 589/1992 Sb., o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, ve znění pozdějších předpisů
- Právní předpisy v oblasti pracovního práva a zaměstnanosti
- Právní předpisy v oblasti sociálního zabezpečení a zdravotního pojištění
- Právní předpisy v oblasti účetnictví, daní a kontrolní činnosti

Základní pojmy

Základními pojmy GDPR v kontextu pojišťovací činnosti jsou:

Osobní údaj (OÚ) – jakákoliv informace, která se týká konkrétní fyzické osoby (subjektu údajů), ať už jde o identifikační a kontaktní údaje (např. jméno, příjmení, datum narození, adresa pobytu, rodné číslo, IČO/DIČ, telefonní číslo, e-mail, údaje o poloze, popisné údaje vypovídající o fyziologii člověka (např.
výška, váha, velikost boty), informace z fotografií a kamerových záznamů, sociodemografické údaje (věk, pohlaví, rodinný stav, vzdělání, zaměstnání, příjmy a výdaje, počet dětí) nebo údaje o jeho chování a preferencích.

Zvláštní kategorie osobních údajů (dříve citlivé osobní údaje) – některé osobní údaje zvlášť rizikové z pohledu možných zásahů do garantovaných práv a svobod fyzických osob, například údaje o zdravotním stavu, údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, genetické či biometrické údaje.

Subjekt údajů – každá fyzická osoba, jejíž OÚ jsou zpracovávány.

Zpracování – jakékoli nakládání s osobními údaji, např. shromáždění, zaznamenání, zpřístupnění, uložení, uspořádání, vyhledání, pozměnění, použití, šíření atd. Mezi typické příklady jsou např. vedení spisové evidence (elektronické i listinné), evidence pojistných událostí, dokumentace v souvislosti s požadavky AML předpisů aj., a to jak v rámci klientské agendy, tak i administrativních činností pojišťovny (např. personalistika).

Správce – jakákoli fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; v případě pojišťovací činnosti je to pojišťovna.

Zpracovatel – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává pro správce osobní údaje, pokud ho tím správce pověří, a pouze ve správcem stanoveném rozsahu a ke stanoveným účelům; není vyloučeno, že jedna osoba bude zároveň správcem (například ve vztahu ke svým zaměstnancům) i zpracovatelem (ve vztahu k jinému správci).

Společní správci – správci, kteří společně stanoví účely a prostředky zpracování osobních údajů.

Příjemce – jakýkoli subjekt, kterému jsou osobní údaje poskytnuty (není rozhodující, zda přímo správcem, nebo zpracovatelem na pokyn správce), v některých případech se za příjemce nepovažují orgány veřejné moci.

Právo vznést námitku – je-li zpracování založeno na oprávněném zájmu správce, případně prováděno ve veřejném zájmu nebo při výkonu veřejné moci, má subjekt údajů právo kdykoli proti takovémuto zpracování vznést námitku, subjekt údajů má právo vznést námitku také proti zpracování za účelem přímého marketingu a správce má v tomto případě povinnost dotčené OÚ dále nezpracovávat.

ÚOOÚ – Úřad pro ochranu osobních údajů, kontrolní a dozorový úřad dle GDPR v ČR, se sídlem, Pplk. Sochora 27, 170 00, Praha 7, telefon: +420 234 665 111, web: www.uoou.cz.

Záznamy o činnostech zpracování – každý správce osobních údajů je povinen vést záznamy o činnostech zpracování osobních údajů, za něž zodpovídá. GDPR předepisuje formální vedení záznamů o činnostech zpracování především pro velké organizace (nad 250 zaměstnanců). Nicméně, vzhledem k tomu, že záznamy musí vést i každý správce a zpracovatel (bez ohledu napočet zaměstnanců), pokud

a) prováděné zpracování OÚ pravděpodobně představuje riziko pro práva a svobody subjektů údajů,
b) zpracování OÚ není příležitostné, nebo
c) zpracování zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů, bude se povinnost vést tyto formalizované záznamy týkat všech pojišťoven. Přitom musí zohlednit kontext, citlivost a rozsah vedených osobních údajů, aby byly schopny prokázat soulad s GDPR při případné kontrole ze strany ÚOOÚ

DPO – pověřenec pro ochranu osobních údajů (z angl. data protection officer); DPO je jakýmsi interním auditorem zpracování a ochrany osobních údajů; dohlíží nad tím, že osobní údaje jsou zpracovávány a chráněny v souladu s GDPR. Povinnost jmenovat DPO není plošná (lze ho však ustavit dobrovolně). Pojišťovna ho mít musí.

Analýza rizik – posouzení zpracování osobních údajů s cílem zjistit, jak závažná rizika plynou ze zpracování pro práva a svobody fyzických osob, a na základě toho přijmout opatření, která tato rizika minimalizují.

DPIA – posouzení vlivu na ochranu osobních údajů (z angl. data protection impact assessment) - formalizovaná riziková analýza, jejímž úkolem je zjistit, zda i přes vysoká rizika zpracování osobních údajů, zjištěná v rámci zpracování záznamů o činnostech zpracování, lze tyto údaje legálně zpracovávat za použití opatření, která sníží vysoká rizika na přijatelnou úroveň.

Hlášení bezpečnostních incidentů – GDPR obsahuje povinnost správce hlásit porušení zabezpečení, integrity a ztrátu osobních údajů ÚOOÚ bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o nich dozvěděl; z této povinnosti jsou vyloučeny pouze incidenty s nízkou rizikovostí pro subjekty osobních údajů. Navíc správci musí oznámit toto porušení neprodleně všem dotčeným subjektům údajů, pokud je pravděpodobné, že příslušné porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob.