Česká asociace pojišťoven

Samoregulační standardy

České asociace pojišťoven k uplatňování obecného nařízení o ochraně osobních údajů (GDPR) v pojišťovnictví

Účinné od 1. srpna 2020

Obsah

A

Obecná ustanovení

Preambule

Pojišťovny pro řádný a korektní výkon své činnosti potřebují velké množství osobních údajů, jež jsou v rámci jejich činnosti zpracovávány. I když je pojišťovací odvětví vysoce legislativně regulovaným oborem, členské pojišťovny ČAP se rozhodly zdůraznit význam připisovaný ochraně soukromí a bezpečnosti osobních údajů přijetím těchto Samoregulačních standardů ČAP (dále jen „**Standardy**“) k aplikaci 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 „**GDPR**“).[1]

Za tímto účelem ČAP ve spolupráci se svými členy vypracovala a přijala následující Standardy, které přispívají k řádnému uplatňování GDPR a zároveň reflektují specifickou povahu pojišťovnictví a konkrétní potřeby členů ČAP při zpracovávání osobních údajů. Tyto Standardy jsou koncipovány jednotně pro všechny přistoupivší členy s cílem upřesnit uplatňování GDPR. Standardy představují obecně pojatou minimální míru ochrany subjektů údajů, kdy není bráněno jednotlivým členům zvolit v konkrétních případech vyšší míru ochrany zpracování osobních údajů na základě jejich specifických potřeb a postupů.

Jejich účelem není nahradit právní úpravu GDPR ani doporučené postupy a výkladová stanoviska Úřadu pro ochranu osobních údajů, WP29 či EDPB. Standardy mají sloužit jako jejich doplněk a obecné interpretační vodítko při aplikaci jednotlivých zásad ochrany osobních údajů a jednotlivých povinností upravených GDPR v prostředí pojišťovnictví.

Standardy jsou určeny členům ČAP, kteří ke Standardům přistoupili, a jejich zaměstnancům, kteří zpracovávají osobní údaje. Dobrovolné přistoupení k Standardům je vyjádřením závazku kompatibility s jejich obsahem a zároveň je vyjádřením dobré vůle zúčastněných pojišťoven, jež veřejně proklamují respekt k ochraně osobnosti, důvěrnosti a bezpečnosti osobních údajů, plné míře informovanosti klienta, zvýšení jeho ochrany a rozvoji finančního trhu. Pojišťovny, které k Standardům přistoupily, o této skutečnosti vhodným způsobem informují své klienty.

Standardy se vztahují na zpracování osobních údajů klientů a pojišťovacích zprostředkovatelů, které pojišťovny zpracovávají při výkonu pojišťovací činnosti a souvisejících činností, na území České republiky. Jiná zpracování, která jsou vlastní v zásadě každému správci (např. zpracování osobních údajů zaměstnanců), nejsou předmětem těchto Standardů. Kde je ve Standardech uváděna pojišťovna, se uvedená práva a povinnosti obdobně použijí i na členské zajišťovny při zajišťovací činnosti.

[1] http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS

Seznam definic a zkratek

Ve Standardech jsou používány příslušné termíny s následujícím významem:

1) **„citlivé údaje“:** osobní údaje, které tvoří zvláštní kategorii osobních údajů dle čl. 9 odst. 1 GDPR;

2) **„dozorový úřad“:** nezávislý orgán veřejné moci zřízený členským státem podle čl. 51 GDPR; v ČR Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“);

3) **„EDPB“:** Evropský sbor pro ochranu osobních údajů, který nahradil WP29;

4) **„EHP“:** Evropský hospodářský prostor;

5) **„EU“:** Evropská unie;

6) **„GDPR“:** 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);

7) **„plně automatizované rozhodování“:** rozhodnutí založené výhradně na automatizovaném zpracování (zpracování bez lidského zásahu), včetně profilování, které má pro subjekt údajů právní nebo obdobné účinky a které tak spadá pod čl. 22 GDPR;

8) **„přímý marketing“:** cílená a adresná komunikace spočívající v přímém kontaktu mezi pojišťovnou a klientem, na základě které je učiněna nabídka produktů nebo služeb. Jedná se např. o aktivní telemarketing, odpovědní zásilky či e-mail a SMS;

9) **„skupina podniků“:** skupina zahrnující řídící podnik a jím řízené podniky; kdy podnikem je jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, které běžně vykonávají hospodářskou činnost, tj. např. i pojišťovna. Tradičně se jedná o finanční skupiny, jejichž je pojišťovna součástí;

10) **„správce“:** obecně jakákoli fyzická nebo právnická osoba naplňující znaky čl. 4 bodu 7 GDPR. V případě Standardů se za správce vesměs považuje příslušná pojišťovna;

11) **„stížnost“:** podání subjektu osobních údajů obsahující zřetelný projev nespokojenosti či kritické vyjádření k oblasti zpracování osobních údajů;

12) **„subjekt údajů“:** fyzická osoba, jejíž osobní údaje jsou zpracovávány. Pro účely těchto Standardů a pojišťovací činnosti se většinou bude jednat o pojištěného, pojistníka, obmyšleného, poškozeného anebo zájemce o pojištění;

13) **„třetí země“:** stát, který není členem EHP;

14) **„WP29“:** pracovní skupina článku 29 ustanovena směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, která účinností GDPR pozbyla platnost, a nahrazena EDPB;

15) **„zákon č. 480/2004 Sb.“:** zákon č. 480/2004 Sb., o některých službách informační společnosti, jenž transponoval směrnici Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu. Přijetím GDPR není uplatňování této úpravy dotčeno. Obě úpravy existují vedle sebe. Zákon č. 480/2004 Sb. se nedotýká tzv. živých telefonických hovorů. V případě zasílání obchodních sdělení pojišťovna musí naplnit současně požadavky zákona č. 480/2004 Sb. a též mít k takovému zpracování osobních údajů potřebný účel a právní základ dle GDPR. Případný souhlas dle zákona č. 480/2004 Sb. však není souhlasem dle GDPR a nemusí proto naplnit podmínky GDPR;

16) **„zákon o AML“:** zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu;

17) **„zákon o distribuci pojištění a zajištění“:** zákon č. 170/2018 Sb., o distribuci pojištění a zajištění;

18) **„zákon o zpracování osobních údajů“:** zákon č. 110/2019 Sb., o zpracování osobních údajů.

Další výrazy použité v textu Standardů odpovídají svým významem významu, který je jim přisuzován GDPR.

B

Požadavky na zpracování osobních údajů v pojišťovnictví

1

1.1 Základní principy zpracování osobních údajů

1.1.1 Pojišťovna se při zpracovávání osobních údajů řídí následujícími principy:

a) Veškeré osobní údaje pojišťovna zpracovává vždy zákonně, korektně, transparentně a odpovědně (uvedené principy jsou blíže vysvětleny v bodech 1.1.2 a následujících Standardů níže).

b) Zpracování je účelově omezené, což znamená, že pojišťovna zpracovává osobní údaje pouze pro určité, výslovně vyjádřené a legitimní účely, přičemž osobní údaje nejsou dále zpracovávány způsobem, který je s těmito účely neslučitelný (viz bod 1.3 Standardů níže).

c) V rámci zásady minimalizace údajů pojišťovna zpracovává přiměřené, relevantní a na nezbytný rozsah omezené osobní údaje ve vztahu k účelu, pro který jsou zpracovávány.

d) Pojišťovna zpracovává přesné a aktualizované osobní údaje. Pokud jsou osobní údaje nepřesné, pojišťovna zajistí jejich opravu či případně výmaz, k čemuž může požadovat nezbytnou součinnost (viz bod 1.1.5 Standardů níže).

e) Pojišťovna nezpracovává osobní údaje, pokud pomine účel (právní titul) stanovený pro jejich zpracování (viz kapitola 2 Standardů).

f) Pojišťovna zpracovává osobní údaje způsobem, který zajistí náležité zabezpečení a ochranu osobních údajů (viz kapitola 4 Standardů).

1.1.2 Princip zákonnosti

Aby bylo zpracování zákonné, musí pojišťovna zpracovávat osobní údaje na základě některého z právních titulů uvedených v čl. 6 GDPR a pouze v odpovídajícím rozsahu pro stanovený účel zpracování. Pro pojišťovací činnosti jsou relevantní zejména právní základy zpracování nezbytné pro splnění smlouvy či její uzavření, zpracování nezbytné pro splnění zákonné povinnosti správce, zpracování nezbytné pro účely oprávněného zájmu anebo zpracování na základě souhlasu subjektu údajů (jejich přehled viz bod 1.4 Standardů níže). V případě citlivých údajů je vedle stanovení právního základu dle čl. 6 GDPR potřeba zároveň naplnit i jednu z podmínek uvedených v čl. 9 GDPR (jejich přehled viz bod 1.5 Standardů níže).

1.1.3 Princip korektnosti a transparentnosti

Pojišťovna transparentně informuje subjekt údajů, které osobní údaje o něm zpracovává, v jakém rozsahu a jakým způsobem, jaká práva má v souvislosti se zpracováním těchto osobních údajů, a napomáhá výkonu těchto jeho práv. Subjekt údajů by měl být dále informován o provádění automatizovaného rozhodování a o jeho důsledcích. Pojišťovna upozorní subjekt údajů na rizika, pravidla a záruky zpracování osobních údajů a na práva subjektu údajů, která je možno v této souvislosti uplatnit. Všechny informace určené subjektu údajů poskytuje pojišťovna stručně, snadno přístupným způsobem a srozumitelně (k informační povinnosti viz bod 1.8 Standardů níže).

1.1.4 Princip odpovědnosti

Pojišťovna odpovídá za dodržení principů uvedených v bodu 1.1.1 Standardů výše při zpracování osobních údajů a je schopna soulad s nimi doložit. Za tímto účelem pojišťovna zavede vhodná opatření, která pravidelně aktualizuje a je schopna demonstrovat jejich existenci a aplikaci. Taková opatření jsou uvedena v kapitolách 4 a 5 Standardů.

Pojišťovna jako správce osobních údajů je odpovědná za újmu, kterou způsobí zpracováním, jež je v rozporu s GDPR. Zpracovává-li pojišťovna osobní údaje v pozici zpracovatele, je za újmu způsobenou zpracováním odpovědná pouze v případě, že nesplní povinnosti stanovené právními předpisy pro zpracovatele nebo pokud jednala nad rámec pokynů správce či v rozporu s nimi. Pojišťovna v pozici správce či zpracovatele může být odpovědnosti za újmu zproštěna, pokud prokáže, že vynaložila veškerou péči, aby předešla události, která ke vzniku újmy vedla.

1.1.5 Přesnost a aktuálnost zpracování osobních údajů

Pro řádný výkon pojišťovací činnosti je maximálně podstatné, aby pojišťovna disponovala přesnými a aktuálními osobními údaji subjektů údajů. Objeví-li se při nebo po uzavření smlouvy konkrétní indikace, že byly poskytnuty nepřesné či nekompletní osobní údaje, nebo došlo k jejich změně, pojišťovna učiní nezbytný výmaz nebo opravu za účelem odstranění nedostatků. K tomuto pojišťovna může vyžadovat maximální součinnost subjektu údajů.

PŘÍKLAD

Neohlášení změny příjmení např. z důvodu změny osobního stavu klienta může mít vliv na rychlost a efektivnost pojistného plnění a řešení pojistné události, neboť nejprve bude pojišťovna muset provést identifikaci subjektu údajů, a to např. cestou dožádání oddacího listu.

1.1.6 Zásada minimalizace a účelového omezení

Zpracování osobních údajů musí odpovídat účelu jejich shromáždění. Osobní údaje lze zpracovávat pouze pro určité a oprávněné účely, o jejichž existenci byl subjekt údajů řádně informován a které jsou v souladu s právními předpisy. Pojišťovny zpracovávají osobní údaje v rozsahu nezbytném k naplnění takového účelu.

Osobní údaje nelze zpracovat způsobem, který je v rozporu s účelem jejich zpracování, ani v rozsahu přesahujícím potřeby a požadavky takového účelu.

1.2 Kategorie osobních údajů

1.2.1 V rámci pojišťovací činnosti pojišťovny zpracovávají různé kategorie osobních údajů. Těmito kategoriemi jsou zejména:

a) identifikační a kontaktní údaje (např. jméno a příjmení, datum narození, rodné číslo, adresa, telefon, e-mail, státní příslušnost);

b) osobní údaje týkající se rozsudků v trestních věcech a trestných činů (např. údaje o trestní bezúhonnosti pojišťovacího zprostředkovatele);

c) údaje pro účely underwritingu (např. povolání, vzdělání, provozované sporty a koníčky);

d) údaje vztahující se k předmětu pojištění (např. velký technický průkaz pojištěného vozidla);

e) údaje pro zjištění potřeb a požadavků klienta (na základě § 77 zákona o distribuci pojištění

a zajištění je pojišťovna povinna před sjednáním anebo podstatnou změnou pojištění získat od klienta informace týkající se jeho požadavků, cílů a potřeb, zejména informace o okolnostech vedoucích klienta ke sjednání pojištění a nastavení jeho konkrétních parametrů);

f) údaje potřebné pro test vhodnosti (na základě § 78 zákona o distribuci pojištění a zajištění je pojišťovna povinna před sjednáním anebo podstatnou změnou rezervotvorného pojištění poskytnout klientovi radu týkající se vhodnosti těchto právních jednání pro klienta. Mezi požadované údaje patří finanční situace klienta, znalosti a zkušenosti klienta v oblasti investic, riziková tolerance klienta a jeho schopnost nést ztráty, právní vztahy klienta týkající se dalších produktů finančního trhu);

g) citlivé údaje sloužící především k provedení underwritingu). Pro účely Standardů půjde v rámci pojišťovací činnosti zejména o tyto citlivé údaje:

- **„genetické údaje“:** osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotyčné fyzické osoby;
- **„biometrické údaje“:** osobní údaje vyplývající z konkrétního technického zpracování a týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují nebo potvrzují jedinečnou identifikaci, např. zobrazení obličeje nebo daktyloskopické údaje;
- **„údaje o zdravotním stavu“:** osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;

h) údaje z monitoringu (např. údaje získané na základě záznamů z jednání, záznamů telefonických hovorů, záznamů o využívání on-line služeb, záznamů o komunikaci s klienty a prohlížení webu pojišťovny, údaje o zasílaných obchodních sděleních, údaje z mobilních aplikací);

i) údaje zpracovávané v souvislosti s plněním pojistné smlouvy a využíváním služeb (např. údaje o sjednání a využívání služeb či o nastavení smluv a parametrech pojištění, předané informace k řešení pojistné události, údaje získané během likvidace).

1.3 Účely zpracování v pojišťovnictví

1.3.1 Pojišťovna zpracovává osobní údaje a jejich kategorie pro účely vyplývající z její činnosti. Pojišťovna se zavazuje stanovit účely zpracování osobních údajů v souladu s právními předpisy a takto stanovené účely respektovat.

Pojišťovna zpracovává osobní údaje pro různé účely, jejichž obecný přehled je uveden dále, přičemž pro každý účel potřebuje právní základ zpracování osobních údajů (právní základy použitelné v pojišťovnictví jsou uvedené v bodu 1.4. Standardů níže). Pojišťovna může jedny osobní údaje či jednu kategorii osobních údajů zpracovávat pro různé účely. Pojišťovna stanoví již v okamžiku shromažďování nebo nakládání s osobními údaji konkrétní, jednoznačné a legitimní účely, pro které budou osobní údaje zpracovávány.

a) V souladu se zásadou minimalizace údajů pojišťovna zpracovává osobní údaje pouze v rozsahu přiměřeném, relevantním a omezeném na to, co je nezbytné z hlediska účelů jejich zpracování.

PŘÍKLAD

Není důvodné od klienta vyžadovat předložení výpisu z trestního rejstříku pro účely sjednání smlouvy o havarijním pojištění.

b) Pojišťovna zpracovává osobní údaje pro stanovený účel (účely). Osobní údaje poskytnuté pro jeden účel nelze v souladu s principem účelového omezení dle bodu 1.1.1 Standardů bez dalšího užívat k jinému účelu.

Pokud pojišťovna zjistí, že potřebuje zpracovávat osobní údaje i pro jiné účely, než jsou ty, pro které osobní údaje původně shromáždila, může tak učinit pouze,

- pokud to umožňuje právní předpis EU nebo ČR,
- byl-li k tomu udělen souhlas subjektu údajů,
- je zpracování pro jiný účel slučitelné s účely, pro které byly osobní údaje shromážděny. V takovém případě pojišťovna vždy mimo jiné zohlední jakoukoli vazbu mezi těmito účely, povahu osobních údajů (zejména, zda se nejedná o citlivé údaje), okolnosti, za nichž byly údaje shromážděny, možné důsledky zamýšleného dalšího zpracování pro subjekty údajů a existenci vhodných záruk jako např. šifrování nebo pseudonymizace.

Před uvedeným dalším zpracováním pojišťovna poskytne subjektu údajů informace o tomto jiném účelu a jeho právech, ledaže již subjekt údajů takové informace má.

PŘÍKLAD I

E-mailová adresa klienta (anebo telefonní číslo pro SMS komunikaci), která byla klientem pojišťovně poskytnuta při uzavření smlouvy pro účely jejího plnění, nesmí být bez dalšího užita k takovým marketingovým účelům, u kterých je vyžadován jako právní základ souhlas (tedy se nejedná o přímý marketing, neboť tam je právním základem oprávněný zájem a souhlas klienta není třeba). Pojišťovna musí v takovém případě obdržet předchozí souhlas klienta se zpracováním osobních údajů – e-mailové adresy – pro účely těchto nepřímých marketingových a obchodních sdělení (např. nabídek služeb třetích stran).

PŘÍKLAD II

Skutečnost, že pojišťovna některé údaje získá z veřejně dostupných zdrojů, neznamená automaticky, že účel jejich dalšího zpracování je slučitelný s účelem, pro který byly osobní údaje původně zveřejněny. Vždy je nezbytné pečlivě zvážit veškeré výše uvedené podmínky slučitelnosti zpracování.

V případech důvodného podezření pojišťovny na podvodné či protiprávní jednání bude nový účel – prevence a vyšetřování pojistných podvodů a jiné protiprávní činnosti – zpracování osobních údajů získaných z veřejných zdrojů s největší pravděpodobností vyhodnocen jako slučitelný s původním účelem, jímž bylo jejich zveřejnění ke zpracování nezbytnému pro účely oprávněných zájmů pojišťovny či třetí strany spočívajících zejména v ochraně právních nároků. To však platí kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující zvýšenou ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

1.3.2 Pojišťovna zpracovává osobní údaje zejména za následujícími účely:

a) výkon pojišťovací a zajišťovací činnosti a činností z nich vyplývajících:
   - jednání o smluvním vztahu, které se týká kromě samotného uzavření pojistné smlouvy i přípravy modelací a návrhů;
   - zjišťování potřeb a požadavků klienta a další údaje potřebné pro test vhodnosti (např. finanční situace klienta, jeho znalosti a zkušenosti v oblasti investic); tyto údaje jsou nezbytné pro splnění zákonné povinnosti poskytnout doporučení, resp. radu klientovi, aby se mohl řádně rozhodnout, zda sjedná nebo změní pojištění a zda je to pro něj vhodné;
   - upisování a ocenění pojistného rizika a stanovení pojistného v odpovídající výši;
   - rozložení pojistného rizika formou sjednání zajištění či soupojištění a předávání osobních údajů zajišťovnám;[2]
   - správa pojištění a ukončení pojistné smlouvy;

[2] V případě rozložení pojistného rizika formou zajištění a předávání osobních údajů zajišťovně jsou aplikovány obdobné právní základy jako v případě zpracování osobních údajů pojišťovnami, a to v závislosti na okamžiku a účelu jejich zpracování. Pro předání osobních údajů zajišťovně není nezbytný samostatný souhlas subjektu údajů, neboť v právních základech použitých pro zpracování pojišťovnami je zahrnuto i případné předání příslušným zajišťovnám. Obdobné se použije i v případě citlivých údajů, viz bod 1.5.1 Standardů.

- plnění závazků z pojistné smlouvy, šetření pojistných událostí, poskytování plnění z pojistných smluv a poskytování asistenčních služeb;
- příprava statistik a pojistněmatematických studií pro potřebu cenotvorby;
- hodnocení a řízení rizik různými metodami, včetně profilování a scoringu;
- ověření podmínek rozhodných pro stanovení výše pojistného za pojištění odpovědnosti za újmu způsobenou provozem vozidla u České kanceláře pojistitelů;

PŘÍKLAD I

Pokud zajistitel obdrží osobní údaje od pojišťovny v rámci zajištění, je samostatným správcem těchto osobních údajů. Zajistitel zabezpečí informování subjektů údajů o zpracování osobních údajů buď sám napřímo, nebo prostřednictvím příslušné pojišťovny.

PŘÍKLAD II

Pokud pojišťovna v rámci zajištění předává či může předat osobní údaje zajistiteli, informuje subjekty údajů o možnosti předání osobních údajů na zajistitele. Pro předání citlivých údajů pojišťovnou na zajistitele je právním titulem souhlas subjektu údajů.

b) plnění požadavků dozorových a jiných státních orgánů a plnění zákonných povinností vyplývajících ze zvláštních právních předpisů;[3]

c) ochrana práv a právem chráněných zájmů pojišťovny (např. vymáhání pohledávek a regresů);

d) prevence a odhalování pojistných podvodů a jiných protiprávních jednání;

e) interní potřeby pojišťovny, tedy vnitřní administrativní potřeby pojišťovny;

f) vznik, správa a ukončení vztahů se zprostředkovateli a obchodními partnery;

g) nabízení vlastních služeb (přímý marketing);

h) oslovování potenciálních klientů;

i) nabízení produktů a služeb třetích stran a předávání osobních údajů třetím stranám (zejména v rámci skupiny podniků) pro tento účel;

j) předávání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely;

k) hodnocení kvality nabízených služeb.

1.4 Právní základy zpracování

1.4.1 Zpracování je zákonné, pouze pokud je prováděno v odpovídajícím rozsahu za splnění nejméně jedné z podmínek (právních základů) zpracování dle čl. 6 odst. 1 GDPR. Pro účely v pojišťovnictví uvedené výše se zejména uplatní tyto právní základy:

a) zpracování je **nezbytné pro plnění smlouvy**, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů (čl. 6 odst. 1 písm. b) GDPR);

b) zpracování je **nezbytné pro plnění právní povinnosti**, která se na správce vztahuje (čl. 6 odst. 1 písm. c) GDPR);

c) 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 vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě (čl. 6 odst. 1 písm. f) GDPR);

d) subjekt údajů udělil **souhlas** se zpracováním svých osobních údajů pro jeden či více konkrétních účelů (čl. 6 odst. 1 písm. a) GDPR).

Souhlas subjektu údajů je pouze jedním z právních základů použitelných pro zpracování osobních údajů. Pojišťovna využívá právní základ souhlasu pouze v případech, kdy nemůže využít žádný z dalších právních základů zpracování osobních údajů rozvedených dále.

[3] Jedná se především o zákon č. 277/2009 Sb., o pojišťovnictví, zákon č. 168/1999 Sb., o pojištění odpovědnosti za újmu způsobenou provozem vozidla, zákon o AML, zákon č. 164/2013 Sb., o mezinárodní spolupráci při správě daní, daňové předpisy, zákon o distribuci pojištění a zajištění apod.

1.4.2 Zpracování nezbytné pro plnění smlouvy nebo pro provedení opatření přijatých před uzavřením smlouvy

1.4.2.1 Pojišťovna zpracovává osobní údaje již od doby jednání o uzavření pojistné smlouvy s klientem a dále v případě uzavření smlouvy po celou dobu trvání pojištění. Tento právní základ se použije jenom pro zpracování osobních údajů subjektu údajů, který je smluvní stranou pojistné smlouvy, která s ním byla nebo má být uzavřena.
Ke zpracování osobních údajů na základě tohoto právního základu tak dochází zejména v situacích:

a) jednání o uzavření pojistné smlouvy a hodnocení pojistného rizika;

b) uzavření pojistné smlouvy a její správy;

c) zaznamenávání telefonických hovorů a elektronické komunikace pro účel uzavření smlouvy a plnění smluvních povinností z ní;

PŘÍKLAD

Hovory týkající se konkrétní smlouvy nebo pojistné události, stížnosti na postup pojišťovny ve věcech týkajících se uzavřené pojistné smlouvy, hovory potenciálních klientů k obdržení informací před uzavřením pojistné smlouvy apod.

d) šetření pojistných událostí;

e) poskytování plnění z pojistné smlouvy.

1.4.2.2 Na právním základě plnění smlouvy pojišťovna zpracovává zejména tyto kategorie údajů:

a) identifikační a kontaktní údaje klienta (např. jméno, příjmení, adresa pobytu, rodné číslo, telefonní číslo, e-mail);

b) osobní údaje vztahující se k předmětu pojištění (např. velký technický průkaz pojištěného vozidla);

c) citlivé osobní údaje (např. údaje o zdravotním stavu), jejichž zpracování musí též naplnit podmínky čl. 9 GDPR (viz bod 1.5 Standardů níže);

d) údaje pro účely underwritingu (např. povolání, vzdělání, provozované sporty a koníčky);

e) osobní údaje získané při poskytování plnění a využívání služeb, zejména při šetření pojistné události a poskytování pojistného plnění (např. popis případu, detaily poškození a výdajů, lokalizační údaje, údaje o bankovním účtu).

1.4.3 Zpracování nezbytné pro splnění právní povinnosti

1.4.3.1 Pojišťovna při provozování pojišťovací činnosti musí zpracovávat osobní údaje pro plnění právních povinností, které jí ukládají právní předpisy ČR nebo EU.

Mezi zpracování osobních údajů na základě plnění právních povinností patří zejména:

a) zjišťování požadavků a potřeb klienta a finančních údajů v rámci testu vhodnosti pro účely poskytování doporučení a rady;[4]

b) uchovávání dokumentů a záznamů z jednání;[5]

c) poskytování součinnosti České národní bance, soudům, orgánům činným v trestním řízení, exekutorům, notářům, insolvenčním správcům a dalším orgánům veřejné moci dle příslušných právních předpisů;[6]

d) uplatňování opatření proti legalizaci výnosů z trestné činnosti a financování terorismu za účelem zabránění zneužívání finančního systému pojišťovny;[7]

e) plnění povinností vyplývajících z uplatňování mezinárodních sankcí;[8]

f) zpracování osobních údajů pojišťovnou nebo Českou kanceláří pojistitelů v souvislosti s plněním povinností u pojištění odpovědnosti z provozu vozidla včetně vedení zákonných evidencí údajů a související předávání České kanceláři pojistitelů;[9]

[4] Zákon o distribuci pojištění a zajištění.

[5] Zákon o distribuci pojištění a zajištění.

[6] Např. zákon č. 277/2009 Sb., o pojišťovnictví, zákon č. 141/1961 Sb., trestní řád, zákon č. 120/2001 Sb., exekuční řád.

[7] Zákon o AML.

[8] Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí.

[9] Zákon č. 168/1999 Sb., o pojištění odpovědnosti za újmu způsobenou provozem vozidla a o změně některých souvisejících zákonů (zákon o pojištění odpovědnosti z provozu vozidla).

g) vzájemné informování a sdílení informací mezi pojišťovnami za účelem prevence a odhalování pojistného podvodu a dalšího protiprávního jednání;[10]

h) shromažďování informací týkajících se osob, na které se v jiném státě vztahují daňové povinnosti, a předávání těchto údajů příslušným orgánům finanční správy.[11]

1.4.4 Zpracování nezbytné pro účely oprávněných zájmů

1.4.4.1 Pojišťovna zpracovává osobní údaje na právním základě oprávněného zájmu pojišťovny či třetí strany, převažuje-li tento zájem pojišťovny nad oprávněnými zájmy, základními právy a svobodami subjektu údajů.

Ke zpracování osobních údajů na základě tohoto právního základu tak dochází zejména v následujících situacích:

a) zpracování údajů nesmluvních stran,

PŘÍKLAD

Pojišťovna zpracovává na tomto právním základě osobní údaje subjektů údajů, které nejsou stranou pojistné smlouvy. Jedná se zejména o pojištěné osoby, a to v rámci individuálního i skupinového pojištění, dále o osoby obmyšlené, oprávněné, poškozené a další osoby, jejichž osobní údaje jsou nezbytné k výkonu pojišťovací činnosti.

b) zpracování pro účely přímého marketingu,

PŘÍKLAD

Pojišťovna zpracovává na tomto právním základě osobní údaje pro účely přímého marketingu, který zahrnuje zejména nabízení produktů pojišťovny, jíž je subjekt údajů klientem.

Naopak se právní základ oprávněného zájmu neuplatní na předávání osobních údajů třetím stranám za účelem zasílání marketingových sdělení, s kterými nemá subjekt údajů relevantní existující vztah, nebo na zasílání marketingových sdělení třetích osob, zde je potřeba souhlas subjektu údajů s tímto účelem zpracování (nepřímý marketing).

c) ochrana práv a právem chráněných zájmů pojišťovny,

PŘÍKLAD

Pojišťovna zpracovává osobní údaje k ochraně svých práv a právních nároků v nezbytně nutném rozsahu v rámci soudních řízení či řízení před orgány mimosoudního řešení sporů, při vymáhání dlužného pojistného, regresních postizích a vymáhání dalších pohledávek.

d) prevence a odhalování pojistných podvodů a jiných protiprávních jednání,

e) nahrávání telefonických hovorů,

PŘÍKLAD

Za účely oprávněných zájmů uvedených pod písm. a), c) a d) pojišťovna nahrává telefonické hovory a zpracovává osobní údaje z těchto záznamů. Záznamy hovorů jsou uloženy a chráněny způsobem, jenž zajišťuje, že nejsou dostupné neoprávněným osobám, a současně pojišťovna přijala nezbytná opatření zabraňující neoprávněnému nakládání s takto uloženými osobními údaji. Pojišťovna může poskytnout záznamy orgánům činným v trestním řízení pouze na základě zákona a v jeho mezích.

f) předání osobních údajů v rámci skupiny podniků, jejíž je pojišťovna součástí, pro její vnitřní administrativní účely, ne však za účelem marketingu (bod 1.6.1.1 Standardů) nebo za účelem některých pokročilých marketingových analýz (bod 1.6.1.2 Standardů), kde je vyžadován jako právní základ souhlas subjektu údajů,

g) zpracování osobních údajů pro provedení auditů, vnitropodnikových nařízení a pro vnitřní administrativní účely,

h) zpracování osobních údajů pro přerozdělení rizik zajištěním nebo soupojištěním.

[10] § 129b zákona č. 277/2009 Sb., o pojišťovnictví.

[11] Zákon č. 164/2013 Sb., o mezinárodní spolupráci při správě daní a o změně dalších souvisejících zákonů.

1.4.5 Zpracování na základě souhlasu subjektu údajů

1.4.5.1 Souhlas je pouze jedním z právních základů zpracování osobních údajů. Souhlas se zpracováním osobních údajů je pojišťovnou vyžadován pouze v situacích, kdy není možné provádět zpracování osobních údajů na základě jiného právního základu.

1.4.5.2 Pojišťovna umožňuje subjektu údajů udělit souhlas se zpracováním osobních údajů zejména[12] při zpracování osobních údajů pro účely jiného než tzv. přímého marketingu (tj. případy, kdy se marketing může spolehnout na právní základ oprávněného zájmu, viz bod 1.4.4.1 Standardů výše).

PŘÍKLAD

Oslovování potenciálních klientů

Prostřednictvím elektronické pošty pojišťovna realizuje oslovování subjektů údajů, které nejsou klienty pojišťovny, a to na základě jejich předchozího souhlasu, který byl udělen přímo pojišťovně (např. potenciální klient vyplní on-line formulář dostupný na webu) nebo získán prostřednictvím doporučující osoby (např. potenciální klient udělí svůj souhlas na formuláři, který doporučující předá pojišťovně). Souhlas může být udělen i ústně, pojišťovna však musí být schopna ústní souhlas prokázat (např. svědeckou výpovědí nebo záznamem telefonního hovoru).

Nicméně ve chvíli, kdy potenciální klient požádá o zpracování nabídky pojištění (např. přípravy návrhů ve formě kalkulací, modelů a variant řešení, hodnocení pojistného rizika), se již jedná o právní základ zpracování nezbytné pro uzavření smlouvy realizované na žádost subjektu údajů (viz bod 1.4.2 Standardů výše). V tu chvíli se potenciální klient stává klientem a souhlas pro další marketingové nabídky pojišťovny klientovi není vyžadován.

1.4.5.3 Ve specifických situacích pojišťovna umožňuje subjektu údajů udělit výslovný souhlas se zpracováním osobních údajů. Výslovný souhlas nelze dovozovat z jiného jednoznačného vyjádření subjektu údajů. Pojišťovna umožňuje subjektu údajů udělit výslovný souhlas zejména v následujících situacích:

a) plně automatizované individuální rozhodování dle čl. 22 GDPR, včetně profilování, pokud se nepoužije jiný právní titul (viz bod 3.7 Standardů níže).

PŘÍKLAD

Pojišťovna umožňuje subjektu údajů udělit výslovný souhlas s automatizovaným rozhodováním včetně profilování (scoring klienta) například v případě pojištění osob, kdy sjednávací systém zcela automaticky vyhodnotí informace o zdravotním stavu uvedené do zdravotního dotazníku v rámci přípravy modelace pojištění nebo v rámci uzavírání pojistné smlouvy a na základě obdržených údajů stanoví přirážku za zdravotní stav k pojistnému.

1.4.5.4 Platně projevený souhlas se zpracováním osobních údajů, včetně výslovného souhlasu, musí splňovat všechny následující podmínky pro jeho udělení:

a) Svobodný

Souhlas se poskytuje k určitému účelu. Pojišťovna nemůže podmiňovat poskytnutí svých služeb souhlasem se zpracováním osobních údajů, které nejsou pro poskytnutí takové služby nezbytné. Souhlas je svobodně udělen, pokud subjekt údajů může souhlas se zpracováním osobních údajů odmítnout nebo následně odvolat, aniž by to pro něj mělo škodlivé následky. Pokud existuje jiný právní základ zpracování, souhlas se nepoužije.

PŘÍKLAD I

Uzavření pojistné smlouvy nelze podmínit udělením souhlasu se zpracováním osobních údajů pro účely nepřímého marketingu.

PŘÍKLAD II

Správu pojistné smlouvy nelze podmínit udělením souhlasu se zpracováním osobních údajů, neboť se použije právní základ „zpracování nezbytné pro splnění smlouvy" (viz výše) a souhlas tak není třeba a podmínění správy pojistné smlouvy souhlasem se zpracováním osobních údajů není nezbytné.

[12] Pojišťovny často vyžadují souhlas i ke zpracování citlivých údajů, jak je vysvětleno níže v bodě 1.5.1 Standardů. Na tento souhlas se uplatní stejné požadavky, jako jsou uvedené v bodě 1.4.5.3 Standardů.

Pokud pro zpracování osobních údajů neexistuje jiný právní základ pro zpracování (viz výše přehled ostatních právních základů v pojišťovnictví), lze pro zpracování osobních údajů vyžadovat souhlas.

Zejména v případě citlivých údajů může být pro zpracování těchto údajů vyžadován souhlas (viz bod 1.5 Standardů níže). Pojišťovna musí v takovém případě vždy zvážit, zda existuje přímá spojitost mezi určitými osobními údaji a potřebou jejich zpracování pro uzavření nebo plnění dané smlouvy (poskytnutí služby). Pojišťovna v takovém případě informuje subjekt údajů o smluvním požadavku osobní údaje poskytnout, o jejich nezbytnosti pro uzavření smlouvy a možných důsledcích, nebude-li tak učiněno. Vyžadování takového souhlasu není v rozporu s čl. 7 odst. 4 GDPR, jelikož zpracování citlivých údajů je nezbytně nutné již pro samotné uzavření a plnění smlouvy a nejedná se o zpracování, které by pro uzavření či plnění smlouvy nebylo nezbytné.

PŘÍKLAD

Souhlas se zpracováním zdravotních údajů u životního pojištění (mimo případy naplnění odchylky určení a obhajoba právních nároků, kdy není souhlas potřeba – vysvětleno v bodu 1.5 Standardů níže) naplňuje uvedenou podmínku nezbytnosti, neboť bez potřebných údajů o zdravotním stavu a možnosti jejich zpracování nemůže pojišťovna uzavřít s klientem smlouvu o životním pojištění.

Uvedené se netýká tzv. „obyčejných necitlivých" osobních údajů subjektu údajů, který je stranou pojistné smlouvy, jelikož pro ty je možné využít právní základ nezbytnosti pro plnění smlouvy (viz bod 1.4.2 Standardů výše). Takový právní základ však nebyl zakotven v GDPR pro citlivé údaje, a proto je jejich zpracování pro uzavření příslušných pojistných smluv podmiňováno souhlasem subjektů údajů.

b) Jednoznačný

Udělený souhlas je jednoznačným projevem vůle, pokud:

- je text souhlasu oddělitelný od ostatních smluvních ujednání, zejména vizuálně, aby jej subjekt údajů mohl efektivně a jednoduše zaznamenat;

PŘÍKLAD

Souhlas se zpracováním osobních údajů není neoddělitelnou součástí pojistných podmínek.

- je projeven vědomě, aktivně a

PŘÍKLAD

Souhlas se zpracováním osobních údajů je projeven podpisem listiny, zaškrtnutím příslušného pole, písemným prohlášením, ústním prohlášením, popř. jiným dostatečně zjevným a prokazatelným způsobem. Pokud subjekt údajů souhlas neudělí, pojišťovna jeho osobní údaje pro tento účel zpracovávat nebude. V případech, kdy GDPR souhlas vyžaduje, není možné nadále využívat opt-out souhlasy, tj. předem zaškrtnutá políčka, která subjekt údajů musel aktivně vyškrtnout, pokud nesouhlasil, aby jeho osobní údaje byly zpracovávány.

- je s ohledem na naléhavost situace a zájem subjektu údajů prokazatelně udělen prostřednictvím jakéhokoli dokumentovatelného prostředku, kterými jsou např. podpis na listině, e-mail, fax, SMS, telefonický hovor.

PŘÍKLAD

Subjekt údajů projevil zájem o uzavření pojistné smlouvy na dálku prostřednictvím telefonního hovoru a při sjednání smlouvy projevil souhlas se zpracováním osobních údajů za účelem nabízení služeb třetích osob, dalších členů skupiny podniků a spolupracujících obchodních partnerů. Tento ústní souhlas má pojišťovna zdokumentovaný (nahraný).

c) Granularita, určitý a konkrétní

Ke každému z účelů zpracování osobních údajů, kde je právním základem souhlas subjektu údajů, vyžaduje pojišťovna ideálně samostatný souhlas pro každý z těchto účelů. Jeden souhlas může být udělen pro zpracování více kategorií osobních údajů a zahrnovat více skutečných operací/kroků zpracovávání, pokud tyto operace sledují stejný účel. Pokud pojišťovna hodlá využít

osobní údaje pro jiný účel, pro který je potřeba souhlas, musí obdržet ideálně před započetím jejich zpracovávání nový souhlas pro tento účel.

PŘÍKLAD

Ke zpracování osobních údajů pro zařazení do soutěží a pro předávání údajů třetí osobě, tj., kde je oboje na právním základu souhlasu, jde o dva souhlasy. Pojišťovna nepožaduje v tomto případě pouze jeden souhrnný souhlas, neboť jde o dva účely zpracování.

Souhlas není vyžadován pro předání osobních údajů v rámci skupiny podniků z důvodu vnitřních administrativních účelů skupiny, kde dochází ke zpracování na základě oprávněného zájmu (bod 1.4.4.1 písm. f) Standardů). Pro jiné než vnitřní administrativní účely skupiny podniků je vyžadován souhlas. Jedná se např. o předání osobních údajů v rámci skupiny podniků za účelem marketingu (bod 1.6.1.1 Standardů) nebo za účelem některých pokročilých marketingových analýz (bod 1.6.1.2 Standardů).

d) Informovaný

Subjekt údajů je informován, k jakým účelům zpracování poskytuje svůj souhlas, a dále o svých právech, jakož i např. o právu odvolat souhlas (více o informační povinnosti viz bod 1.8 Standardů).

e) Odvolatelný

Subjekt údajů má právo svůj souhlas kdykoli odvolat, a to stejným způsobem, jakým jej poskytl. V případě odvolání souhlasu by měla pojišťovna být bez ohledu na formu udělení souhlasu schopna prokázat, zda a kdy byl souhlas subjektem odvolán.

PŘÍKLAD

Pokud byl souhlas udělen elektronicky, musí mít subjekt údajů možnost tento souhlas i odvolat elektronickou cestou a nemůže být vyžadováno písemné odvolání souhlasu.

Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu před jeho odvoláním. Odvolání souhlasu se děje vždy k určitému účelu, pro který byly osobní údaje zpracovávány.

Odvolání souhlasu neznamená vždy povinnost pojišťovny osobní údaje zlikvidovat, neboť pojišťovně může příslušet jiný právní základ, pro který může pojišťovna nadále držet či aktivně zpracovávat osobní údaje pro jiný účel (např. ochrana práv a právem chráněných zájmů pojišťovny nebo plnění právních povinností).

Odvolání souhlasu, stejně jako jeho neposkytnutí v prvé řadě nesmí jít k tíži subjektu údajů nebo mít pro něj příliš zatěžující důsledky.

PŘÍKLAD

Pokud klient odvolá souhlas se zpracováním osobních údajů pro marketingové účely, nemůže to vést k ukončení celé pojistné smlouvy či odmítání pojišťovny nadále poskytovat plnění dle pojistné smlouvy.

Pokud však subjekt údajů odvolá souhlas v případě, kdy je zpracování takových osobních údajů nezbytné pro uzavření nebo plnění smlouvy, není pojišťovna v prodlení ani povinna konat, dokud neobdrží požadovaný souhlas se zpracováním osobních údajů.

PŘÍKLAD

Subjekt údajů udělí výslovný souhlas se zpracováním údajů o zdravotním stavu pro účely uzavření pojistné smlouvy životního pojištění. Tento souhlas ještě před uzavřením smlouvy odvolá. Pojišťovna není nucena uzavřít s klientem smlouvu životního pojištění, dokud subjekt údajů znovu neposkytne souhlas se zpracováním osobních údajů, a toto neuzavření není považováno za jinak zakázaný škodlivý důsledek odvolání souhlasu.

1.5 Zvláštní případy zpracování

1.5.1 Citlivé údaje

Citlivé údaje jsou v GDPR nazývány jako zvláštní kategorie osobních údajů, kterými jsou v pojišťovnictví primárně údaje o zdravotním stavu, genetické údaje a biometrické údaje zpracovávané při uzavírání pojistné smlouvy.

S ohledem na jejich povahu jsou hodny zvláštní ochrany. Ta tkví v tom, že vyjma klasického určení účelů a k tomu souvisejícího právního základu v čl. 6 GDPR (popsané v bodě 1.4 Standardů výše) musí být též nalezena jedna z taxativně vymezených výjimek dle čl. 9 odst. 2 GDPR pro jejich zpracování. V pojišťovnictví těmito výjimkami jsou zejména:

a) výslovný souhlas subjektu údajů (čl. 9 odst. 2 písm. a) GDPR) – viz ad a) níže anebo

b) zpracování (bez souhlasu subjektu údajů) nezbytné pro určení, výkon nebo obhajobu právních nároků (čl. 9 odst. 2 písm. f) GDPR) – viz ad b) níže.

Ad a) Výslovný souhlas subjektu údajů

Citlivé údaje pojišťovna může zpracovávat na základě výslovného souhlasu pro účely:

- jednání o smluvním vztahu, uzavření pojistné smlouvy, přípravy modelací a návrhů, zjišťování potřeb a požadavků klienta,
- upisování a ocenění pojistného rizika a stanovení pojistného v odpovídající výši.

Souhlas je dobrovolný, avšak bez něj nelze sjednat pojištění, u něhož pojišťovna potřebuje znát údaje o zdravotním stavu ještě před vstupem do pojištění. Souhlas může subjekt údajů kdykoliv odvolat. Odvoláním souhlasu však není dotčena zákonnost zpracování údajů o zdravotním stavu a genetických údajů do okamžiku odvolání. I když na počátku byl vyžadován souhlas, tak další zpracování (v tomto případě již získaných) osobních údajů po uzavření smlouvy není vázáno na souhlas. Ve vztahu ke zpracovávaným citlivým údajům po uzavření smlouvy není nutno pro jejich další zpracování získávat souhlas v případě, kdy se využije důvod ad b) níže. Odvolání souhlasu po uzavření smlouvy tak nevede k ukončení zpracování citlivých údajů a pojišťovna není povinna příslušné osobní údaje vymazat.

PŘÍKLAD

Pojišťovna při upisování a ocenění pojistného rizika zpracovává osobní údaje budoucího pojistníka na základě právního základu nezbytnost pro splnění smlouvy (viz bod 1.4.2 Standardů výše).

V případě životního pojištění pojišťovna posuzuje před uzavřením pojistné smlouvy i citlivé údaje (standardně údaje o zdravotním stavu klienta), které si musí vyžádat od klienta, jenž jí k takovému zpracování může udělit výslovný souhlas. To platí i pro případy, kdy pojišťovna provádí automatizované individuální rozhodování.

Uvedené se netýká tzv. „obyčejných necitlivých" osobních údajů subjektu údajů, který je stranou pojistné smlouvy, jelikož pro ty je možné využít právní základ nezbytnosti pro plnění smlouvy (viz bod 1.4.2 Standardů výše). Takový právní základ však nebyl zakotven v GDPR pro citlivé údaje, a proto je jejich zpracování pro uzavření příslušných pojistných smluv závislé na souhlasu subjektů údajů.

Ad b) Určení, výkon nebo obhajoba právních nároků

Je-li to nezbytné pro určení, výkon nebo obhajobu právních nároků, zpracovává pojišťovna citlivé údaje v nezbytném rozsahu bez souhlasu zejména pro následující účely:

- plnění závazků z pojistné smlouvy, šetření pojistné události a poskytování plnění z pojistných smluv;
- správa a ukončení pojistné smlouvy, s výjimkou změny pojistné smlouvy zahrnující posouzení přijatelnosti dopojištění, kterou pojišťovna provádí na základě souhlasu subjektu údajů;
- prevence a odhalování pojistných podvodů a jiných protiprávních jednání;
- ochrana práv a právem chráněných zájmů pojišťovny.

Z uvedeného vyplývá, že pojišťovna nepotřebuje souhlas například pro zpracování zdravotních údajů poškozených osob, které uplatnily svůj nárok na náhradu újmy na zdraví z pojištění odpovědnosti.

1.5.1.1 V pojišťovnictví se uplatní též souhlasy dle vnitrostátních předpisů, konkrétně souhlas podle § 2828 nebo § 2864 zákona č. 89/2012 Sb., občanský zákoník, který je podmínkou pro vyžadování určitých informací ze strany pojišťovny. Povaha těchto souhlasů dle občanského zákoníku se přijetím GDPR nemění. Nejedná se o souhlasy dle GDPR, a tudíž se na jejich formu a podobu neaplikují podmínky souhlasu GDPR rozvedené v bodu 1.4.5.4 Standardů výše.

1.5.1.2 U pojistných smluv sjednaných před použitelností GDPR, kde byly dosud obdrženy souhlasy dle zákona o zpracování osobních údajů, není nutno získávat nové souhlasy se zpracováním údajů o zdravotním stavu. U těchto starých pojistných smluv se údaje o zdravotním stavu budou nadále zpracovávat na základě nezbytnosti pro určení, výkon nebo obhajobu právních nároků za podmínek uvedených v bodu 1.5.1 ad b) Standardů výše. Při změně pojistné smlouvy vyžadující posouzení přijatelnosti do pojištění je však udělení nového souhlasu nezbytné.

1.5.2 Osobní údaje týkající se rozsudků v trestních věcech a trestných činů

1.5.2.1 Pojišťovna zpracovává osobní údaje týkající se rozsudků v trestních věcech a trestných činů, a to v souladu s čl. 10 GDPR, tj. v souladu s ustanoveními zákona č. 141/1961 Sb., trestního řádu, ve znění pozdějších předpisů, a zákona č. 218/2003 Sb., o soudnictví ve věcech mládeže, ve znění pozdějších předpisů, a je-li to nezbytné pro:

- ochranu bezpečnosti a integrity finančního sektoru, včetně prevence, odhalování, vyšetřování trestné činnosti;
- ověřování důvěryhodnosti distributorů pojištění podle zákona o distribuci pojištění a zajištění;
- evidenci pro účely sledování podezřelých obchodů ve smyslu zákona o AML;
- plnění dalších zákonných povinností.

1.5.2.2 Výše uvedenými ustanoveními není dotčena povinnost pojišťovny sdílet údaje dle § 129b zákona č. 277/2009 Sb., o pojišťovnictví, ve znění pozdějších předpisů.

1.5.3 Rodná čísla

1.5.3.1 Pojišťovna při provozování pojišťovací činnosti zpracovává také rodná čísla; takové zpracování se považuje za zpracování nezbytné pro dodržení právní povinnosti správce. V obecné rovině je specifická potřeba zpracování osobních údajů včetně rodných čísel v pojišťovnictví zakotvena v zákoně o pojišťovnictví, dle něhož *„pojišťovna a zajišťovna při provozování pojišťovací nebo zajišťovací činnosti zpracovává osobní údaje včetně rodných čísel; takové zpracování osobních údajů se považuje za zpracování nezbytné pro dodržení právní povinnosti správce.“* [13]

1.5.3.2 V souladu se zásadou minimalizace zpracování osobních údajů zpracovává pojišťovna rodná čísla pouze v rozsahu nezbytně nutném pro výkon pojišťovací činnosti.

[13] § 6 odst. 6 zákona č. 277/2009 Sb., o pojišťovnictví, ve znění pozdějších předpisů.

1.6 Předávání osobních údajů ve skupině podniků

1.6.1 Pojišťovna si v rámci skupiny podniků, jíž je členem, může předávat s ostatními společnostmi v této skupině osobní údaje subjektů údajů pro účely:

1.6.1.1 Nabízení produktů či služeb;

Právním základem pro nabízení produktů či služeb zákazníkům pojišťovny společnostmi skupiny, jejíž je pojišťovna součástí, je souhlas s předáním osobních údajů do skupiny podniků pojišťovny pro účely marketingu.

PŘÍKLAD

Pojišťovna či skupina mají zájem na tom, aby společnosti skupiny, jejíž je pojišťovna součástí, mohly napřímo oslovit klienty pojišťovny s nabídkou svých produktů a služeb. Pojišťovna může předat osobní údaje klienta do skupiny pro tento účel jen poté, kdy klient vysloví souhlas s předáním jeho osobních údajů společnostem skupiny v rozsahu dle souhlasu. Pojišťovna publikuje na svých webových stránkách či v jiném, klientům přístupném médiu seznam podniků ve skupině, který pravidelně aktualizuje; o konkrétních změnách ve společnostech uvedených v seznamu nemusí pojišťovna klienty individuálně informovat a postačí provedení změny v publikovaném seznamu.

1.6.1.2 Pokročilé marketingové analýzy (např. věrnostní programy)

Právním základem pro pokročilé skupinové marketingové analýzy s osobními údaji zákazníků pojišťovny, pro jejichž provedení mají být osobní údaje zákazníků pojišťovny předány do skupiny podniků, jejíž je součástí, bude souhlas s předáním osobních údajů do skupiny podniků pojišťovny pro účely dané marketingové analýzy. Pojišťovna musí sama vyhodnotit vhodný právní základ dle konkrétních parametrů pokročilé marketingové analýzy.

PŘÍKLAD

Podnikatelská skupina, jejíž je pojišťovna součástí, má zájem na vytvoření věrnostního programu pro své zákazníky. V rámci fungování věrnostního programu má dojít k předání osobních údajů ve skupině. Právním základem pro zpracování osobních údajů zákazníků ve věrnostním programu bude souhlas zákazníka.

1.6.1.3 Vnitřní administrativní účely, včetně zpracování osobních údajů zákazníků

Právním základem pro předání osobních údajů zákazníků pojišťovny do skupiny podniků, jejíž je součástí, pro vnitřní administrativní účely, bude zejména oprávněný zájem. Pojišťovna by měla ideálně posoudit správnost použití oprávněného zájmu jako právního základu v balančním testu.

PŘÍKLAD

Podnikatelská skupina, jejíž je pojišťovna součástí, má vytvořen skupinový program pro zajištění a kontrolu informační bezpečnosti. Pro tento účel je nutné předávat osobní údaje dotčených subjektů údajů ve skupině podniků. Právním základem pro předání osobních údajů ve skupině podniků je oprávněný zájem pojišťovny a podnikatelské skupiny.

Právní základy, na nichž k tomuto předávání dochází, jsou blíže vymezeny v rámci jednotlivých právních základů, viz bod 1.4 Standardů výše.

1.6.2 Pro některá předávání osobních údajů ve skupině podniků musí s tímto postupem vyslovit subjekt údajů souhlas a členové skupiny musí být předem identifikováni, a to v souladu s podmínkami pro informovaný souhlas. Klient ale nemusí znovu udělovat souhlas s předáváním údajů ve skupině pokaždé, kdy dojde ke změně členů skupiny, pokud zároveň nedochází ke změně účelů nebo charakteru zpracování a klient je o možnosti takové změny

informován. Pro zajištění plné informovanosti klienta pojišťovna pravidelně aktualizuje seznam členů skupiny podniků (např. na webových stránkách). Subjekt údajů může samozřejmě kdykoli odvolat souhlas se zpracováním osobních údajů, tam, kde je vyžadován k předávání a zpracování údajů ve skupině podniků, o čemž je informován.

1.6.3 Pro předávání osobních údajů v rámci skupiny podniků mimo EHP platí pravidla GDPR pro předávání osobních údajů do třetích zemí. Pokud se společnosti skupiny podniků nachází i mimo EHP, je doporučeno přijetí závazných podnikových pravidel v rámci skupiny podniků.

PŘÍKLAD

Podnikatelská skupina, jejíž je pojišťovna součástí, má řídící podnik se sídlem v EHP. Řídící podnik vytvoří závazná podniková pravidla, která jsou přijata dozorovým úřadem příslušným dle sídla řídícího podniku (vedoucí dozorový úřad). Závazná podniková pravidla jsou poté platná pro celou podnikatelskou skupinu. Pojišťovna publikuje text závazných podnikových pravidel či jeho podstatnou část veřejně, např. na svých webových stránkách. Závazná podniková pravidla umožňují podnikatelské skupině předávat osobní údaje ve skupině podniků i svým podnikům mimo EHP.

1.7 Předávání osobních údajů do třetích zemí

1.7.1 V rámci EU je zajištěna stejná úroveň ochrany osobních údajů a zároveň volný pohyb těchto údajů. Režim předávání osobních údajů do třetích zemí je sjednocen a pojišťovna může osobní údaje do třetí země předat, pouze pokud disponuje právním základem pro takové předání (viz bod 1.7.3 Standardů).

1.7.2 Předáváním osobních údajů do třetích zemí nemusí být jen jejich fyzický přenos, ale i vzdálený přístup k osobním údajům, které jsou uloženy v zemi sídla pojišťovny a k jejichž zobrazení dochází prostřednictvím zařízení umístěného ve třetí zemi. Pojišťovna předává osobní údaje do třetích zemí zpravidla v těchto situacích:

- **sjednání zajištění nebo plnění závazků ze zajistných smluv** – pojišťovna předává zpravidla minimum osobních údajů nebo předává pseudonymizované osobní údaje. V ojedinělých případech však může docházet k předání většího množství osobních údajů, a to např. v případě potřeby sjednat nadlimitní zajištění nebo při překročení hranice pojistného plnění, které musí být zajistitelem samostatně posouzeno;
- **poskytování asistenční služby** – zejména v případě cestovního pojištění či využití mezinárodního poskytovatele asistenčních služeb dochází k předání osobních údajů v rozsahu nezbytném pro bezproblémové poskytnutí asistenčních služeb;
- **IT služby** – k předání osobních údajů dochází v případě, kdy pojišťovna využívá datového centra či jiných služeb IT ve třetí zemi nebo k uložení dat využívá cloudových služeb;
- **ostatní dodavatelé** – zejména v případě, kdy je pojišťovna součástí mezinárodní skupiny podniků, může určité služby odebírat od dodavatelů usazených ve třetích zemích; typicky se může jednat např. o kontrolu klientů[14];
- **reporting** – v případě, kdy je pojišťovna součástí mezinárodní skupiny podniků, může ad hoc docházet k předání osobních údajů do třetí země, a to zejména v rámci oznamování určitých skutečností (např. přeje-li si klient pojistit velké a nadstandardní pojistné riziko, může takové pojištění podléhat schválení mateřské společnosti, podobně mohou být oznamovány též např. soudní a jiné spory).

[14] Zákon o AML nebo zákon č. 69/2006 Sb., o provádění mezinárodních sankcí.

1.7.3 K předání osobních údajů do třetí země může dojít na vymezeném právním základě, kterým je:

a) předání založené na rozhodnutí Evropské komise o odpovídající ochraně[15], kdy není vyžadováno žádné zvláštní povolení ÚOOÚ;

b) předání založené na vhodných zárukách správce a zpracovatele za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektů údajů. Za splnění uvedených podmínek je lze předat bez povolení ÚOOÚ. Vhodnými zárukami jsou zejména:

- závazná podniková pravidla, kdy se jedná o příslušný, dozorovým úřadem schválený souhrn zásad zpracování osobních údajů v rámci skupiny, který je závazný pro všechny členy skupiny podniků. Tato pravidla platí pouze pro přenos osobních údajů v rámci jedné nadnárodní skupiny podniků;
- standardní smluvní doložky – uzavření smlouvy o zpracování osobních údajů, prostřednictvím které se zpracovatel ve třetí zemi zaváže dodržovat úroveň ochrany osobních údajů obvyklou ve státech EU;
- schválený kodex chování, který mohou dodržovat i správci a zpracovatelé ve třetí zemi, na které se GDPR nevztahuje, a tím poskytnout vhodné záruky pro předání osobních údajů do třetích zemí;
- schválený mechanismus pro vydávání osvědčení, které vydává dozorový úřad nebo vnitrostátní akreditační orgán na dobu nejvýše 3 let a může být obnovováno;
- schválený mechanismus pro vydávání osvědčení, které vydává dozorový úřad nebo vnitrostátní akreditační orgán na dobu nejvýše tří let a může být obnovováno.

c) K předání osobních údajů do třetí země ve specifických situacích, kdy není možné uplatnit žádnou ze situací ad a) a b) výše, může dojít pouze při splnění podmínek čl. 49 odst. 1 GDPR (viz bod 1.7.4 níže).

1.7.4 Ve vztahu k dozorovému úřadu je k předání osobních údajů do třetí země nutné:

a) požádat o souhlas dozorový úřad, jestliže správce hodlá předání realizovat na základě nestandardních nástrojů pro vytvoření vhodných záruk podle čl. 46 odst. 3 písm. a) a b) GDPR (tzn. nestandardní smluvní doložky; správní ujednání mezi orgány veřejné moci nebo veřejnými subjekty, která zahrnují vymahatelná a účinná práva subjektů údajů);

b) informovat dozorový úřad dle čl. 49 odst. 1 druhý pododstavec GDPR v případě jednorázového předání osobních údajů omezeného počtu subjektů údajů do třetích zemí, pokud je to nezbytné pro účely závažných oprávněných zájmů správce, jež nepřeváží nad zájmy nebo právy a svobodami subjektů údajů, a pokud nelze uplatnit žádnou z výjimek podle čl. 49 odst. 1 písm. a) až g) GDPR;

c) požádat o schválení závazných podnikových pravidel – příslušným dozorovým úřadem uvedeným v čl. 47 odst. 1 GDPR se však míní pouze vedoucí dozorový úřad pro závazná podniková pravidla, který je schválí s konečnou platností bez nutnosti zapojení ostatních dotčených dozorových orgánů.

1.7.5 Soudním nebo správním orgánům ze třetích zemí nelze osobní údaje z EU předávat, a to ani na základě čl. 48, ani na základě čl. 49 odst. 1 písm. d) GDPR. Výsada veřejného zájmu se uplatní pouze tehdy, jestliže vyplývá z práva státu Evropské unie.

[15] Další informace lze najít na webu ÚOOÚ. Stav ke dni 03. 03. 2020: https://www.uoou.cz/predavani-zalozene-na-rozhodnuti-o-odpovidajici-urovni-ochrany-osobnich-udaju/ds-5065/p1=5065

1.8 Informování o zpracování

1.8.1 Proces informování o zpracování údajů od subjektu údajů probíhá v souladu s principem transparentnosti a jasnosti. Transparentnost a jasnost by měla být dodržena po celou dobu, tj. jakékoliv změny musí být subjektu údajů oznámeny a vysvětleny.

1.8.2 Pojišťovna informuje subjekt údajů v okamžiku, kdy od něj získává osobní údaje ke zpracování, a poskytne mu zejména následující informace:

a) totožnost a kontaktní údaje pojišťovny a případného zástupce;

b) účely zpracování získaných osobních údajů a právní základy těchto zpracování;

- pokud je právním základem nezbytnost pro účely oprávněných zájmů pojišťovny či třetí strany (viz bod 1.4.4 Standardů výše), informuje pojišťovna o těchto oprávněných zájmech;
- pokud je právním základem souhlas, informuje pojišťovna subjekt údajů o možnosti jeho odvolání (viz bod 1.4.5 Standardů výše);

c) případné příjemce nebo kategorie příjemců osobních údajů, kterým pojišťovna údaje předává;

- pokud má pojišťovna v úmyslu předat údaje do třetí země, informuje o tom a též zejména o využití jednoho z právních základů (viz bod 1.7.3 Standardů výše) a ideálně identifikuje příslušné třetí země;

d) práva subjektů údajů (viz kapitola 3 Standardů níže), zvláště pak, že mají právo na přístup k osobním údajům, právo na opravu, výmaz, přenositelnost osobních údajů, právo vznést námitku;

e) pokud bude zpracování předmětem plně automatizovaného individuálního rozhodování dle čl. 22 GDPR, pojišťovna informuje o použitém postupu, jeho významu a důsledcích;

f) informace, zda je poskytnutí osobních údajů zákonným, či smluvním požadavkem, popř. požadavkem nutným pro uzavření smlouvy, informace, zda je subjekt údajů povinen údaje poskytnout a případné důsledky neposkytnutí těchto údajů.

1.8.3 Pojišťovna vždy předá subjektu údajů kontaktní údaje na pověřence pro ochranu osobních údajů, pokud ho má, stejně jako informaci o právu podat stížnost, včetně možnosti podání stížnosti u dozorového úřadu.

1.8.4 Bude-li to možné, informuje pojišťovna subjekt údajů také o době, po kterou budou jeho osobní údaje zpracovávány. Jestliže nebude možné takovou dobu určit na počátku zpracování, oznámí pojišťovna subjektu údajů alespoň kritéria pro stanovení takové doby.

1.8.5 Pokud pojišťovna získala osobní údaje nikoli přímo od subjektu údajů samotného, poskytne mu nejpozději do jednoho měsíce od získání jeho osobních údajů anebo nejpozději v okamžiku první komunikace se subjektem údajů anebo při prvním zpřístupnění osobních údajů (podle toho, který okamžik nastane nejdříve) informace uvedené v bodu 1.8.1 Standardů výše. Vedle těchto informací pojišťovna navíc informuje subjekt údajů, o jaké kategorie dotčených údajů se jedná a zdroj, ze kterého osobní údaje pocházejí.

PŘÍKLAD

O údaje získané nikoli od subjektu údajů se jedná v případech jejich získání od jiných správců, z veřejně dostupných zdrojů, datových brokerů anebo od jiných subjektů údajů. Naopak o situaci spadající pod bod 1.8.1 Standardů se nejedná v případech, kdy subjekt údajů sám poskytne pojišťovně své osobní údaje anebo je pojišťovna získá vlastním sledováním subjektu údajů (např. s využitím zařízení či softwaru k automatickému zachycování dat, jako jsou kamery, sledování přes Wi-Fi a další). V případě získání osobních údajů vlastním sledováním pojišťovna nicméně většinou informuje subjekt údajů i o zdroji a kategorii dotčených údajů.

1.8.6 Informace je možné subjektu údajů předat prostřednictvím třetí osoby, která se k tomu smluvně zaváže. Typicky se může jednat o pojišťovacího zprostředkovatele. Pojišťovny však nebudou této možnosti využívat nepřiměřeně, tedy v situacích, kdy subjekt údajů od dané třetí osoby takto komplexní informací neočekává – např. v případě lékařů. Podobně může být zavázána smluvní strana (také např. pojistník v případě skupinových smluv životního pojištění / leasingových smluv) ke splnění informační povinnosti vůči pojištěným nebo obmyšleným osobám.

1.8.7 Pojišťovna bude všechny informace určené veřejnosti nebo subjektu údajů poskytovat ve stručné formě a zároveň zajistí, aby byly snadno přístupné, srozumitelné a bezplatné. Pojišťovna může využít tzv. vrstveného přístupu pomocí stručného shrnutí základních informací s odkazy na detailnější informace.

1.8.8 Informace určené subjektům údajů mohou být poskytovány v elektronické podobě, zejména prostřednictvím webových stránek pojišťovny.

1.8.9 Pojišťovny nastaví své vnitřní postupy, zejména prostřednictvím vnitřních předpisů, tak, aby usnadnily přístup k právům subjektů údajů, zejména způsoby pro podávání žádostí a případně bezplatné obdržení přístupu k osobním údajům a možnostem nebo výmazu osobních údajů a pro uplatnění práva vznést námitku. O právu vznést námitku, pokud se uplatní, pojišťovna informuje subjekt údajů zřetelně a odděleně od dalších informací.

1.8.10 Jestliže se pojišťovna rozhodne zpracovávat osobní údaje pro jiný účel, než pro který byly údaje získány, poskytne subjektu údajů informace o tomto jiném účelu ještě před uvedeným dalším zpracováním. Pokud je právním základem tohoto dalšího zpracování souhlas subjektu údajů, vyžádá si pojišťovna před tímto dalším zpracováním jeho souhlas (viz bod 1.3.1 písm. b) a bod 1.4.5.3 písm. c) Standardů výše).

1.8.11 Pojišťovna nemusí poskytovat výše uvedené informace v případě, kdy těmito subjekt údajů již disponuje. Pokud se jedná o osobní údaje získané z jiných zdrojů než od subjektu údajů, nemusí pojišťovna navíc poskytnout výše uvedené informace v situaci, kdy poskytnutí těchto informací subjektu údajů není možné nebo by vyžadovalo neúměrné úsilí, nebo je získávání nebo zpřístupnění výslovně stanoveno právem EU nebo České republiky anebo osobní údaje musí zůstat důvěrné s ohledem na zákonnou povinnost mlčenlivosti.

PŘÍKLAD

Za situaci, kdy by poskytnutí informací subjektu údajů vyžadovalo neúměrné úsilí, je možno považovat případy zpracování osobních údajů osob účastných na likvidaci pojistné události, kdy s touto třetí osobou nemá pojišťovna žádný kontakt ani vztah (např. svědek dopravní nehody, jehož údaje získá pojišťovna v rámci šetření pojistné události).

1.8.12 Žádosti podané subjektem údajů, které jsou zjevně nedůvodné nebo nepřiměřené, např. protože se opakují, může správce (pojišťovna) odmítnout nebo za ně požadovat přiměřený poplatek za vynaložené administrativní náklady.

2

2.1 Doba zpracování

2.1.1 Pojišťovna zajistí v rámci svých vnitřních postupů a procesů, aby byl/y omezen/y na nezbytné minimum:

2.1.1.1 doby, po kterou jsou osobní údaje zpracovány;

2.1.1.2 rozsah osobních údajů, které jsou předmětem zpracování.

2.1.2 Pojišťovna zejména stanoví lhůty pro výmaz osobních údajů v rámci archivačních a skartačních pravidel, které se budou vázat k jednotlivým typům a účelům zpracování.

2.1.3 Při stanovení doby zpracování osobních údajů pojišťovna vyhodnotí:

a) povinnost uchovávat nebo jinak zpracovávat osobní údaje po dobu vyplývající z právních předpisů;

b) zda oprávněnost zpracování osobních údajů převáží nad ochranou zájmů subjektu údajů a jejich práv spojených s ochranou osobních údajů v případě právního základu oprávněného zájmu;

c) možnost anonymizace, pokud již není nutné osobní údaje zpracovávat s vazbou na jednotlivé subjekty údajů.

2.1.3.1 Po uplynutí doby zpracování pojišťovna:

a) zajistí, aby osobní údaje již nemohly být dále jinak zpracovány, ale pouze uchovány do okamžiku jejich výmazu nebo skartace; nebo

b) osobní údaje nadále zpracovává (zejména archivuje[16]) pro další účely zpracování, pokud takové jsou; nebo

c) osobní údaje anonymizuje s tím, že nebude již možné tyto údaje spojit se subjektem údajů.

Pojišťovna v rámci svého interního kontrolního systému přijme přiměřená opatření za účelem plnění povinnosti výmazu nebo archivace osobních údajů.

2.1.4 Přehled dob zpracování s ohledem na účely zpracování v pojišťovnictví

Jako obecné pravidlo pojišťovna zpracovává osobní údaje co do jejich rozsahu a časovosti jen tak, jak je nezbytné ve vztahu k danému účelu zpracování. V takovém případě, pokud osobní údaje již nejsou potřebné pro účely, pro které byly zpracovávány, doba zpracování pomíjí a pojišťovna učiní některý z kroků uvedených v bodu 2.1.3.1 Standardů výše. Nicméně v pojišťovnictví je možné nalézt i specifické lhůty zpracování s ohledem na příslušné účely.

a) Výkon pojišťovací činnosti a činností z ní vyplývajících

V případě potenciálního klienta pojišťovna zpracovává osobní údaje do konce druhého kalendářního roku od poslední komunikace s takovým klientem, pokud do té doby nedojde ke sjednání pojištění anebo subjekt údajů nepožádá o provedení opatření přijatých před uzavřením smlouvy (viz bod 1.4.2 Standardů výše).

V případě uzavření pojistné smlouvy je pojišťovna povinna zpracovávat osobní údaje a uchovávat dokumenty a záznamy související se zprostředkováním pojištění nejméně po dobu trvání smluvního vztahu a 10 let po jeho ukončení, pokud zákon o distribuci pojištění a zajištění nebo jiné právní předpisy nestanoví lhůtu delší. Mezi takové dokumenty či záznamy patří i zpracování osobních údajů týkajících se upisování rizik, profilování či scoringu.

Pojišťovna vynaloží přiměřené úsilí pro využití pseudonymizace či anonymizace osobních údajů pro účely tvorby statistik a pojistněmatematických studií pro potřebu cenotvorby.

b) Plnění požadavků dozorových a jiných státních orgánů a plnění zákonných povinností vyplývajících ze zvláštních právních předpisů

U těchto účelů pojišťovna stanoví dobu

[16] V případě, že je to stanoveno zákonem o archivnictví č. 499/2004 Sb. nebo to přikazují jiné právní předpisy.

[17] Stanovené zákonem č. 89/2012 Sb., občanský zákoník.

pro zpracování osobních údajů v souladu se zvláštními právními předpisy. Mezi tyto osobní údaje patří i osobní údaje získané při kontrole klienta za účelem plnění zákonných povinností souvisejících s opatřením proti legalizaci výnosů z trestné činnosti či daňové

PŘÍKLAD

Pro určení doby pro zpracování osobních údajů pojišťovna zohlední požadavky České kanceláře pojistitelů na délku zpracování u pojištění odpovědnosti z provozu vozidel.

legislativy.

c) Ochrana práv a právem chráněných zájmů pojišťovny (např. vymáhání pohledávek a regresů)

Pojišťovna zpracovává osobní údaje za účelem ochrany práv a právních nároků pojišťovny, a to:

- až po dobu dvou let po uplynutí doby promlčení možného nároku pojišťovny nebo třetích osob vůči pojišťovně[18] z pojistné smlouvy, z uznání dluhu nebo vyplývajícího z jiných smluvních nebo deliktních závazků nebo jiných právních skutečností (obecně se bude jednat např. o patnáctiletou promlčecí dobu);
- po dobu civilněprávního řízení, správního řízení, zvláštního právního řízení nebo jiných řízení souvisejících s finančním nebo jiným oprávněným zájmem pojišťovny a lhůt souvisejících s výkonem rozhodnutí;
- po dobu, kdy lze podle právních předpisů uplatnit jakékoliv jiné právní nároky pojišťovny, členů orgánů pojišťovny, jejich zaměstnanců, zprostředkovatelů, obchodních partnerů, klientů nebo jiných třetích osob.

d) Interní potřeby pojišťovny, tedy vnitřní administrativní potřeby pojišťovny

Pojišťovna zpracovává osobní údaje na základě svých interních potřeb po celou dobu trvání smluvního vztahu a zároveň po dobu možného uplatnění právních nároků z něho vyplývajících a po přiměřenou dobu za účelem ochrany oprávněných zájmů pojišťovny.

e) Prevence a odhalování pojistných podvodů a jiných protiprávních jednání

Pojišťovna zpracovává osobní údaje po dobu šetření pojistného podvodu nebo jiné potenciální trestněprávní činnosti, trestního řízení a lhůt souvisejících s výkonem rozhodnutí a dále až po dobu dvou let po uplynutí doby promlčení odpovědnosti za protiprávní jednání či možného nároku pojišťovny nebo třetích osob vůči pojišťovně[19] z pojistné smlouvy, z uznání dluhu nebo vyplývajícího z jiných smluvních nebo deliktních závazků nebo jiných právních skutečností (obecně se bude jednat nejčastěji o nejvýše patnáctiletou promlčecí dobu).

f) Vznik, správa a ukončení vztahů se zprostředkovateli a obchodními partnery

Pojišťovna je oprávněna zpracovávat osobní údaje o zprostředkovatelích či jiných obchodních partnerech nejméně po dobu trvání smluvního vztahu a jeho sjednávání a zároveň po dobu možného uplatnění právních nároků z něho vyplývajících a po přiměřenou dobu za účelem ochrany oprávněných zájmů pojišťovny.

g) Nabízení vlastních služeb (přímý marketing)

Pojišťovna je oprávněna zpracovávat osobní údaje potenciálních klientů na základě souhlasu až do jeho případného odvolání, nebyl-li souhlas udělen pouze na dobu určitou.

PŘÍKLAD

Pojišťovna informuje subjekty údajů, že nabízení vlastních služeb může provádět až 1 rok po ukončení veškerých smluvních vztahů, ledaže subjekt údajů podá námitku proti přímému marketingu. Pokud subjekt údajů uplatní námitku, pojišťovna nabízení vlastních služeb vůči subjektu údajů zastaví a nadále neprovádí.

h) Oslovování potenciálních klientů

Pojišťovna je oprávněna zpracovávat osobní údaje potenciálních klientů na základě souhlasu až do jeho případného odvolání, nebyl-li souhlas udělen pouze na dobu určitou.

[18] Stanovené zákonem č. 89/2012 Sb., občanský zákoník.

[19] Stanovené zákonem č. 89/2012 Sb., občanský zákoník.

i) Nabízení produktů a služeb třetích stran a předávání osobních údajů třetím stranám (zejména v rámci skupiny podniků) pro tento účel

Pojišťovna je oprávněna zpracovávat osobní údaje klientů na základě souhlasu, a to po celou dobu jeho platnosti až do jeho případného odvolání, nebyl-li souhlas udělen pouze na dobu určitou.

j) Předávání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely

Pojišťovna zpracovává osobní údaje na základě svých potřeb skupiny podniků po celou dobu trvání smluvního vztahu a zároveň po dobu možného uplatnění právních nároků z něho vyplývajících a po přiměřenou dobu za účelem ochrany oprávněných zájmů pojišťovny či skupiny.

k) Hodnocení kvality nabízených služeb

Pojišťovna zpracovává osobní údaje týkající se hodnocení kvality nabízených služeb po celou dobu trvání smluvního vztahu. Pojišťovna zkrátí dobu uchování na minimum při hodnocení kvality poskytovaných služeb a využívání statistik a vynaloží přiměřené úsilí pro využití pseudonymizace či anonymizace pro tyto účely zpracování.

3

3.1 Práva subjektu údajů

3.1.1 GDPR přiznává subjektům údajů určitá práva, jejichž účelem je vybalancovat vztah mezi správcem a subjektem údajů. Pojišťovna je povinna uplatnění těchto práv subjektů údajů umožnit bez zbytečného odkladu. Zároveň by uplatnění práva nemělo být zpoplatněno, a to až na výjimky, kdy by došlo ke zneužívání práv, např. protože se opakují, jsou zjevně nedůvodné nebo nepřiměřené. Za takových okolností může správce (pojišťovna) odmítnout uplatnění těchto práv nebo za ně požadovat přiměřený poplatek za vynaložené administrativní náklady.

3.1.2 Pojišťovna stanoví postupy, které usnadní výkon práv subjektů údajů (např. mechanismy pro podávání žádostí, obdržení bezplatného přístupu k osobním údajům, uplatnění práva vznést námitku apod.).

3.1.3 Pojišťovna informuje subjekty údajů o níže uvedených právech a způsobech, jakým pojišťovna zajišťuje uplatňování jejich práv (informační povinnost viz bod 1.8 Standardů výše).

3.1.4 Pro tyto případy si pojišťovna ověřuje identitu subjektu údajů vhodnými metodami či jejich kombinací. Metoda, respektive míra zajištění autentizace, by měla být úměrná rizikovosti uplatněného práva.

PŘÍKLAD

Vhodnými metodami k ověření identity mohou být komunikace s klientem prostřednictvím ověřeného kanálu, jako je prostředí uživatelského účtu, nebo sada otázek s předem definovanými odpověďmi, které subjekt údajů sám uvedl při prvotní identifikaci podle dokladu totožnosti.

3.2 Lhůta pro zpracování žádosti subjektu údajů

3.2.1 Žádost subjektu údajů musí být zpracována bez zbytečného odkladu, nejvýše však ve lhůtě jednoho měsíce od obdržení žádosti.

3.2.2 Tuto lhůtu lze ve výjimečných případech prodloužit. V takovém případě musí pojišťovna o této skutečnosti informovat subjekt údajů, včetně důvodů odkladu, a to ve lhůtě jednoho měsíce od podání žádosti.

3.3 Právo na přístup

3.3.1 Subjekt údajů má právo po pojišťovně požadovat, aby mu sdělila informaci o tom, zda jsou, či nejsou jeho osobní údaje zpracovávány. Pojišťovna zajistí, že uplatněné právo na opravu bude zohledněno i při případné obnově dat ze záložních zdrojů či archivů.

3.3.2 Subjekt údajů má zejména právo na přístup k informacím obsaženým v bodech 1.8.1 a 1.8.2 Standardů výše.

3.3.3 Naopak se právo na přístup nevztahuje na osobní údaje:

a) které by mohly ohrozit vyšetřování trestných činů nebo aktivity týkající se boje;

b) které by mohly ohrozit povinnost mlčenlivosti;

c) kterými mohou být nepříznivě dotčena práva a svobody jiných osob.

PŘÍKLAD

Pojišťovna nebude poskytovat údaje týkající se zdravotního stavu třetích osob. Pojišťovna též není povinna poskytnout právo na přístup jednotlivci za účelem zjištění, zda byl určen subjektem údajů jako obmyšlená osoba v pojistné smlouvě. Zároveň pojišťovna není povinna poskytovat kopie těch údajů, na které se vztahuje povinnost mlčenlivosti dle § 129a, zákona č. 277/2009 Sb., zákona o pojišťovnictví, nebo jiných právních předpisů.

3.3.4 Subjekt údajů má právo na jednu bezplatnou kopii o něm zpracovávaných osobních údajů.

Za další kopie, o které subjekt údajů požádá, může pojišťovna účtovat přiměřený poplatek na základě administrativních nákladů. Pojišťovna zpravidla poskytne kopii zpracovávaných osobních údajů ve formě, kterou je žádost podána, včetně elektronické. Kopii pojišťovna poskytne ve lhůtě jednoho měsíce, která může být prodloužena o další dva měsíce.

3.4 Právo na opravu

3.4.1 Subjekt údajů má právo požádat pojišťovnu o opravu nepřesných údajů. Pojišťovna ověří, zda osobní údaje, k nimž se žádost vztahuje, jsou přesné a aktuální. Než jsou osobní údaje ověřeny, je jejich zpracování omezeno (po jejich úspěšném ověření dochází k opětovnému zahájení zpracování, o kterém je klient před jeho započetím informován). Pojišťovna zajistí, že uplatněné právo na opravu bude zohledněno i při případné obnově dat ze záložních zdrojů či archivů.

3.4.2 Toto právo se nevztahuje zejména na osobní údaje týkající se prevence a vyšetřování pojistných podvodů nebo aktivity týkající se boje proti legalizaci výnosů z trestné činnosti a financování terorismu či jiných zákonných důvodů, pokud je to ve vztahu k takovým údajům výslovně vyloučeno.

3.5 Právo na výmaz

3.5.1 Subjekt údajů má právo, aby pojišťovna jeho osobní údaje v určitých případech dále nezpracovávala (tzv. právo na výmazu neboli právo být zapomenut).

3.5.2 Subjekt údajů může požádat pojišťovnu o výmaz např. v těchto případech:

a) pojišťovna již nepotřebuje osobní údaje pro účel, ke kterému je zpracovávala (otázka lhůt zpracování u jednotlivých účelů viz kapitola 2 Standardů výše);

b) pojišťovna zpracovávala osobní údaje na právním základě souhlasu, subjekt údajů tento souhlas odvolal a jiný základ zpracování není dán;

c) subjekt údajů podal úspěšnou námitku proti zpracování osobních údajů zpracovávaných na základě oprávněného zájmu (viz bod 3.6 Standardů níže).

Pojišťovna v případech odůvodněných žádostí vymaže nebo anonymizuje osobní údaje bez zbytečného odkladu.

3.5.3 Pojišťovna však nevymaže osobní údaje v případě, kdy je oprávněna nebo povinna je zpracovávat na základě jiného právního základu (ochrana právních nároků, plnění právní povinnosti správce) nebo pro jiný účel (např. předcházení pojistným podvodům, boj proti legalizaci výnosů z trestné činnosti a financování terorismu).

PŘÍKLAD

Klient má platnou smlouvu. Přesto však zašle pojišťovně žádost o výmaz osobních údajů. Pojišťovna zašle klientovi vysvětlující informaci, že dané žádosti nemůže vyhovět, neboť údaje zpracovává na základě platného právního titulu, plnění smlouvy.

Bývalý klient má smlouvu, jejíž platnost již uplynula, archivovanou u pojišťovny. Zašle pojišťovně žádost o výmaz osobních údajů. Pojišťovna zašle klientovi vysvětlující informaci, že dané žádosti nemůže vyhovět, neboť údaje zpracovává z právního důvodu svého oprávněného zájmu, popř. plnění právních povinností. Pojišťovna vhodným způsobem informuje klienta o archivačních lhůtách dokumentů.

3.5.4 Pokud je výmaz osobních údajů pojišťovnou odmítnut, informuje o tomto subjekt údajů, uvede důvody odmítnutí a poučí ho o možnosti podat stížnost u dozorového úřadu a o možnosti bránit se proti takovému rozhodnutí u soudu.

PŘÍKLAD

Bývalý klient má smlouvu, jejíž platnost již uplynula, archivovanou u pojišťovny. Zašle pojišťovně žádost o výmaz osobních údajů. Pojišťovna zašle klientovi vysvětlující informaci, že dané žádosti nemůže vyhovět, neboť údaje zpracovává z právního důvodu svého oprávněného zájmu, popř. plnění právních povinností. Pojišťovna vhodným způsobem informuje klienta o archivačních lhůtách dokumentů.

3.6 Právo na přenositelnost

3.6.1 Subjekt údajů má právo získat své osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu a má dále právo požádat, aby pojišťovna přímo předala tyto jeho osobní údaje jinému správci, pokud je to technicky proveditelné. Právo se vztahuje pouze na původní osobní údaje, tj. takové, které subjekt údajů předal správci. Z přenositelnosti jsou vyloučeny osobní údaje odvozené nebo vyvozené z údajů poskytnutých subjektem údajů.

3.6.2 Využití práva na přenositelnost neznamená automatický výmaz osobních údajů pojišťovnou. Pojišťovna neodpovídá za zpracování provedené subjektem údajů nebo jinou společností přijímající tyto osobní údaje.

3.6.3 Přenositelnost se uplatní, pouze pokud:

a) pojišťovna zpracovává osobní údaje automatizovaně (nejedná se např. o vedení fyzického spisu);

b) právním základem zpracování je buď souhlas subjektu údajů, nebo plnění smlouvy;

c) výkonem práva na přenositelnost nebudou nepříznivě dotčena práva třetích osob (např. anamnéza třetích osob ve zdravotní dokumentaci).

3.6.4 Právo na přenositelnost se v oblasti pojišťovnictví vztahuje zejména na tyto osobní údaje:

a) údaje subjektu údajů, které vědomě a přímo poskytl pojišťovně (např. na formuláři o oznámení pojistné události, klientem zaslaná lékařská zpráva);

b) základní osobní údaje poskytnuté klientem v pojistné smlouvě.

3.6.5 Toto právo se však nevztahuje zejména na následující osobní údaje:

a) odvozené osobní údaje (např. výsledky revizní prohlídky provedené na objednávku pojišťovny, výsledky profilování);

b) osobní údaje zpracovávané pojišťovnou pouze na základě jiných právních titulů, než je plnění smlouvy a souhlas subjektu údajů (např. plnění právních povinností v oblasti boje proti legalizaci výnosů z trestné činnosti a financování terorismu).

3.7 Právo na námitku

3.7.1 Proti zpracování osobních údajů pojišťovnou na právním základě oprávněného zájmu (viz bod 1.4.4 Standardů výše) může subjekt údajů vznést námitku. V pojišťovnictví může jít zejména o účely přímého marketingu, zahrnující profilování.

3.7.2 Pokud subjekt údajů vznese námitku proti zpracování osobních údajů pro účely přímého marketingu, přestane pojišťovna osobní údaje pro tento účel zpracovávat.

3.7.3 U ostatních účelů pojišťovna námitce vyhoví, ledaže prokáže, že její oprávněné důvody pro zpracování převažují nad základními právy a svobodami subjektu údajů, jehož osobní údaje mají být zpracovávány, anebo že je další zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků pojišťovny. Do té doby je jejich zpracování omezeno.

3.7.4 Toto právo se nevztahuje zejména na zpracování osobních údajů prováděná pojišťovnou na základě jiných právních základů než oprávněný zájem (uvedených v bodě 1.4 Standardů výše, např. plnění právní povinnosti).

3.8 Právo na omezení zpracování

3.8.1 Subjekt údajů má právo na to, aby pojišťovna omezila zpracování v případě, že:

- subjekt popírá přesnost osobních údajů, a to na dobu potřebnou k ověření stavu;
- zpracování osobních údajů je protiprávní, subjekt odmítá výmaz a požaduje pouze omezení použití jeho osobních údajů;
- pojišťovna jiné osobní údaje nepotřebuje pro účely zpracování, ale subjekt je požaduje pro určení, výkon nebo obhajobu právních nároků;
- subjekt vznesl námitku proti zpracování a do doby ověření pojišťovnou, zda její oprávněné důvody převažují nad oprávněnými důvody subjektu.

PŘÍKLAD

Omezení zpracování osobních údajů subjektu bude provedeno dle technických možností pojišťovny např. pozastavením generování následných předpisů, pozastavením procesu vymáhání pohledávek.

3.9 Automatizované rozhodování a profilování

3.9.1 Subjekt údajů má právo nebýt předmětem žádného rozhodnutí pojišťovny založeného plně na automatizovaném zpracování, včetně profilování. Toto omezení se týká pouze takových rozhodnutí, která by měla právní účinky pro subjekt údajů nebo se ho obdobným způsobem významně dotkla.

PŘÍKLAD

Pojišťovna může využívat plně automatizované zpracování včetně profilování pro marketingové účely, které nemá právní účinky pro subjekt údajů ani se ho obdobným způsobem významně nedotýká.

PŘÍKLAD

Pojišťovna provádí marketingovou kampaň, kdy oslovuje své klienty a nabízí jim typy pojištění, které sama poskytuje. Právním základem marketingové kampaně je zejména oprávněný zájem pojišťovny. Pojišťovna může dle znalostí klienta automaticky vybrat do kampaně jen ty klienty, kteří by o nabízený typ pojištění mohli mít zájem. Je-li prováděno oslovení klientů elektronicky, oslovení klienta vždy obsahuje informaci o tom, že se jedná o obchodní sdělení a možnost klienta jasným a jednoduchým způsobem odmítnout další marketing. Pokud pojišťovna dále interně vyhodnocuje či jinak zpracovává výsledky marketingové kampaně, zavede dle vhodnosti opatření typu pseudonymizace a šifrování osobních údajů.

3.9.2 Výše uvedené omezení se týká jen plně automatizovaných zpracování, tj. takových, kde není do rozhodovacího procesu zahrnut lidský zásah.

PŘÍKLAD

Pojišťovna může využívat automatizované rozhodování například při online sjednávání pojištění v rámci kalkulace.

3.9.3 I přes toto omezení v bodě 3.9.1 výše může pojišťovna plně automatizované rozhodování, včetně profilování, použít, avšak pouze pokud:

f) je nezbytné k uzavření nebo plnění pojistné smlouvy mezi subjektem údajů a pojišťovnou;

g) je povoleno právem EU nebo členského státu

nebo

h) subjekt údajů udělil výslovný souhlas s tímto plně automatizovaným individuálním rozhodováním dle čl. 22 GDPR.

3.9.4 Pojišťovna přijme před započetím provádění plně automatizovaného individuálního rozhodování opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů. V případě vydání rozhodnutí na základě plně automatizovaného zpracování, včetně profilování, umožní pojišťovna fyzické osobě, která byla předmětem takového rozhodnutí, jednoduchou cestou požádat o lidský zásah a rozhodnutí napadnout (čímž současně vyjádří svůj názor); toto právo však subjektu údajů nenáleží, pokud se jedná o automatizované individuální rozhodnutí povolené právem EU nebo členského státu.

4

4.1 Technická a organizační opatření k ochraně osobních údajů

4.1.1 Vzhledem k povaze činností vykonávaných v oblasti pojišťovnictví existují navazující specifická rizika. Pojišťovna implementuje dostatečné záruky zavedením vhodných technických a organizačních opatření, přičemž zohlední stav techniky, náklady na provedení, povahu, rozsah, kontext a účel zpracování i různě pravděpodobná a závažná rizika pro práva a svobody fyzických osob a zajistí úroveň zabezpečení odpovídající danému riziku. Pojišťovna zavedením těchto technických a organizačních opatření zajistí, aby se zpracovávaly jen osobní údaje nezbytné pro každý konkrétní účel, zejména s ohledem na jejich rozsah, doby a dostupnost.

4.1.2 Mezi přijatá opatření se může řadit zejména:

a) pseudonymizace, anonymizace a šifrování osobních údajů;

b) zajištění důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování – např. pravidelné zálohování, dodržování zásad bezpečného vývoje aplikací;

c) zajištění obnovy dostupnosti osobních údajů a přístupu k nim včas v případě fyzických či technických incidentů;

d) pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření. V tomto případě se jedná především o zavedení systémových opatření při vývoji aplikací, jejich provozu a změnách v souladu s principy informační bezpečnosti.

4.1.3 Pojišťovna zavede technická a organizační opatření k ochraně zpracovávaných údajů a k zajištění bezpečnosti zpracování, mezi něž se řadí:

a) fyzická bezpečnost – systém opatření, která mají neoprávněné osobě zabránit přístupu k informacím, popř. přístup nebo pokus o něj zaznamenat (kombinace opatření fyzické bezpečnosti a technických prostředků). Tato opatření jsou pravidelně prověřována a kontrolována, zda splňují aktuální požadavky;

b) nástroj pro ochranu integrity komunikačních sítí;

PŘÍKLAD

Nástroje typu šifrování, VPN, aplikační firewall.

c) nástroj pro ochranu před škodlivým kódem;

PŘÍKLAD

Antimalwarové řešení.

d) nástroj pro detekci kybernetických bezpečnostních událostí;

PŘÍKLAD

Systém detekce abnormálních událostí, např. systém IPS, dále systém SIEM, který umožňuje správu auditních logů a varování na události v souladu s nastavenými politikami správce.

e) aplikační bezpečnost;

f) kryptografické prostředky;

g) nástroj pro zajišťování úrovně dostupnosti;

h) zajištění toho, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby;

i) zajištění toho, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby k pořizování elektronických

záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány;

j) pořizování elektronických záznamů, které umožní určit a ověřit kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány;

k) zabránění neoprávněnému přístupu k datovým nosičům.

PŘÍKLAD

Pevné disky přenosných počítačů a pracovních stanic jsou šifrovány vhodným způsobem, aby v případě ztráty nebo krádeže nemohlo dojít k úniku chráněných údajů. Používání přenosných paměťových zařízení (USB disky, optická média apod.) je limitováno na konkrétní uživatele a zápis by měl být možný pouze na šifrovaná média ve vlastnictví společnosti.

4.1.4 Pojišťovna stanoví minimální požadavky technického zabezpečení týkající se všech zpracovatelů osobních údajů. Mezi přijaté požadavky se vedle opatření uvedených v bodu 4.1.3 písm. h)–k) oddílu B Standardů řadí:

a) používání legálního a aktualizovaného operačního systému;

b) používání antivirového řešení;

c) dodržování fyzické bezpečnosti.

4.2 Pseudonymizace a anonymizace osobních údajů

4.2.1 Pojišťovna zavede vhodná opaření k minimalizaci zpracování osobních údajů a k pseudonymizaci nebo anonymizaci osobních údajů. Zavedení těchto opatření je prováděno na základě vlastního vyhodnocení pojišťovny.

PŘÍKLAD

Pseudonymizace osobních údajů je proces skrytí identity, jehož účelem je mít možnost sbírat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost. Jako možné pseudonymizační techniky pojišťovna využívá např.:

a) zašifrování údajů (reverzibilní);

b) hashování prostřednictvím určeného klíče a současné ponechání či odstranění tohoto klíče – Informace se týkají jednotlivců, kteří jsou označeni kódem, přičemž klíč spojující kódy s běžnými identifikátory těchto jednotlivců (jméno, datum narození, adresa apod.) se uchovává odděleně;

c) tokenizace.

Pseudonymizované osobní údaje nicméně nejsou anonymizovanými údaji, proto se na ně stále vztahuje GDPR.

4.2.2 Pokud pojišťovna nemá účel a právní základ, aby mohla osobní údaje subjektu údajů dále zpracovávat (např. po uplynutí doby zpracování, viz kapitola 2 Standardů výše), příslušné osobní údaje vymaže anebo je anonymizuje.

4.2.3 Jako možné anonymizační techniky v systémech pojišťovny jsou využívány zejména tyto:

- výmaz všech informací z databází, které jsou považovány za osobní údaje, až na úroveň, kdy zbytkové údaje již neodpovídají definici osobního údaje dle terminologie GDPR;
- zobecnění, při kterém se osobní údaje v databázi pojišťovny upraví tak, aby byly natolik nekonkrétní, že určitý subjekt údajů již nebude identifikovatelným;
- seskupení, při němž administrátor či systém použije osobní údaje tak, že vytvoří nový systém dat, v němž původní data spojuje.

PŘÍKLAD

- Promíchání hodnot mezi záznamy;
- generování náhodných hodnot;
- náhrada hodnot z externího číselníku.

4.2.4 Pseudonymizovaná nebo anonymizovaná data, která jsou zejména nezbytná pro fungování klíčových systémů pojišťovny nebo pro další pojistněmatematické kalkulace, vytváření analytických modelů, výzkum a vývoj produktů a služeb, analýzy vývoje trhu anebo pro historické, statistické a vědecké účely, pojišťovna vesměs zpracovává ve svých informačních systémech.

4.3 Využití zpracovatelů

4.3.1 Pojišťovna může jako zpracovatele osobních údajů zapojit množství externích subjektů různých kategorií.

PŘÍKLAD

Zpracovatelem pro pojišťovnu jsou například poskytovatelé informačních systémů a technické infrastruktury, smluvní lékaři, externí likvidátoři, poskytovatel asistenčních služeb, externí partneři vymáhající dlužné pojistné nebo regresy nebo třeba marketingové agentury.

Pro pojišťovny, které se nachází v roli správce osobních údajů, tvoří nejvýznamnější kategorii zpracovatelů v rámci pojišťovací činnosti pojišťovací zprostředkovatelé. Níže uvedená ustanovení obsahují pravidla využití pojišťovacích zprostředkovatelů jako hlavních zpracovatelů osobních údajů v rámci distribuce pojištění a zajištění, nicméně pojišťovna postupuje obdobně i při využití jiných zpracovatelů.

4.3.2 V rámci náležité pozornosti (due diligence) při výběru zpracovatelů osobních údajů a pro dostatečné zajištění práv subjektů údajů a zároveň splnění povinností vztahujících se na správce osobních údajů pojišťovna při výběru zpracovatelů dodržuje zejména následující:

a) pojišťovna pověřuje zpracováním osobních údajů pouze zpracovatele, kteří poskytují dostatečné záruky zavedením vhodných technických a organizačních opatření (viz bod 4.1.4 Standardů), splňují požadavky právních předpisů týkajících se ochrany osobních údajů a zajistí ochranu práv subjektu údajů. Splnění těchto požadavků lze zjistit zejména prostřednictvím veřejně dostupných informací o právní subjektivitě, historii a ekonomické situaci zpracovatele (např. obchodní rejstřík, insolvenční rejstřík apod.) a dále na základě informací poskytnutých zpracovatelem o vnitřním nastavení podmínek pro zpracování, jako jsou zejména vnitřní politiky, předpisy či metodické pokyny pro zajištění správného a bezpečného zpracování dat. Při prověřování dostatečnosti zavedených technických a organizačních opatření se pojišťovna zaměřuje např. na rozsah úrovně zabezpečení zpracovatelských systémů, správu přístupových oprávnění do takových systémů a přijatá organizační opatření zaručující, že během zpracování osobních údajů nedojde k jejich úniku, změně, ztrátě nebo jinému neoprávněnému zásahu do práv subjektu údajů;

PŘÍKLAD

Vhodnou formou ke zjišťování, zdali zpracovatelé poskytují dostatečné záruky bezpečného zpracování dat, mohou být dotazníky se strukturovanou sadou otázek, které jsou zaměřeny na naplnění požadavků vyplývajících z GDPR. Je vhodné, aby pojišťovny sjednaly se zpracovateli možnost auditů nakládání s osobními údaji zpracovatelem.

b) pojišťovna zpřístupní osobní údaje zpracovateli ke zpracování až ve chvíli zavedení opatření dle písm. a);

c) zpracování osobních údajů zpracovatelem se řídí zpracovatelskou smlouvou uzavřenou v písemné formě a splňující náležitosti uvedené v čl. 28 GDPR.

4.3.3 V souladu s povinností součinnosti provádí pojišťovna kontrolu zpracovatelů osobních údajů s cílem minimalizovat rizika neoprávněného zásahu do práv subjektu údajů. Vzhledem k objemu zpracovávaných údajů je kladen důraz především na kontrolu pojišťovacích zprostředkovatelů. Zájmem pojišťovny je, aby zpracování osobních údajů pojišťovacími zprostředkovateli nebylo na újmu subjektu údajů. Při provádění kontrol postupuje pojišťovna nebo jí pověřený auditní subjekt v souladu s požadavky GDPR, Standardů, relevantní právní úpravy, zpracovatelské smlouvy a vnitřních předpisů pojišťovny. O provedených kontrolách, výsledcích a přijatých opatřeních si vede pojišťovna dokumentaci.

PŘÍKLAD

Pojišťovna vytvoří pravidelný kontrolní plán za účelem zjištění plnění požadavků vyplývajících z GDPR u vybraných zpracovatelů.

4.4 Porušení zabezpečení osobních údajů

4.4.1 Porušení zabezpečení osobních údajů je porušením zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně, neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

4.4.2 Za účelem efektivní a včasné detekce podezření na porušení zabezpečení pojišťovna používá havarijní plán pro detekci, analýzu a interní řešení bezpečnostních incidentů. Detekce incidentů probíhá například nahlášením ze strany zaměstnance nebo jiného koncového uživatele, nahlášením zpracovatelem, správcem, třetí stranou nebo prostřednictvím automatických detekčních systémů, přičemž pojišťovna průběžně vyhodnocuje funkčnost těchto postupů. Následuje evidence a klasifikace incidentu z hlediska závažnosti a jeho vyhodnocení, které vede k odpovídající reakci. Pojišťovna vede evidenci o veškerých porušeních zabezpečení osobních údajů, včetně popisu řešení, nápravných opatření a kontrolních kroků.

4.4.3 Pojišťovna musí ohlásit dozorovému úřadu pouze takové porušení zabezpečení osobních údajů, které pravděpodobně představuje riziko pro práva a svobody fyzických osob, a to do 72 hodin od okamžiku, kdy se pojišťovna o porušení zabezpečení dozví, respektive získá znalost ve smyslu důvodného stupně jistoty, že došlo k bezpečnostnímu incidentu a tím pádem k porušení zabezpečení osobních údajů. Ohlášení dozorovému úřadu může předcházet krátké prošetření s cílem zjistit, zda událost skutečně naplňuje znaky porušení zabezpečení, aniž by začala plynout lhůta 72 hodin.

4.4.4 Již při podezření na porušení zabezpečení osobních údajů podnikne pojišťovna nutná technická a organizační opatření k zamezení dalšího porušení zabezpečení, případně ke zmírnění důsledků, zejména se zřetelem na rizika hrozící subjektům údajů.

4.4.5 V případě, že interní šetření pojišťovny odhalí porušení zabezpečení, které představuje riziko pro práva a svobody fyzických osob, pojišťovna sdělí dozorovému úřadu informace dle čl. 33 GDPR. Pojišťovna může toto ohlášení učinit pomocí standardizované šablony, která tvoří přílohu těchto Standardů, pomocí formuláře „Ohlášení porušení zabezpečení osobních údajů dle GDPR" publikovaného dozorovým úřadem nebo jiným vhodným způsobem.

4.4.6 V případě, kdy porušení zabezpečení bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí pojišťovna porušení

zabezpečení osobních údajů bez zbytečného odkladu příslušnému subjektu údajů, a to transparentně a odděleně od jiných informací, například formou e-mailu nebo jiné adresné zprávy, a pokud možno v jazyce, kterému subjekt údajů porozumí. V oznámení jasně a srozumitelně uvede informace dle čl. 34 GDPR. Toto oznámení subjektu údajů lze ve výjimečných případech provést ještě před ohlášením dozorovému úřadu. Oznámení se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

a) pojišťovna zavedla náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;

b) pojišťovna přijala následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;

c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

4.4.7 Vysoké riziko pro práva a svobody fyzických osob je vyhodnocováno na základě povahy porušení zabezpečení, typu a množství osobních údajů, možnosti přímé identifikace jednotlivce, vážnosti případných dopadů na jednotlivce také vzhledem ke kategoriím dotčených subjektů údajů a případně jejich počtu. Dozorový úřad může posoudit, že porušení zabezpečení bude mít za následek vysoké riziko, a požadovat oznámení porušení subjektu údajů.

PŘÍKLAD

Ztráta nebo zcizení citlivých údajů jsou hodnoceny jako situace s vysokým rizikem pro subjekty údajů.

5

5.1 Pověřenec pro ochranu osobních údajů

5.1.1 S ohledem na skutečnost, že pojišťovna při své činnosti provádí rozsáhlé, pravidelné a systematické zpracování osobních údajů vč. osobních údajů zvláštní kategorie, je povinna jmenovat pověřence pro ochranu osobních údajů (dále jen „pověřenec), aby tento mohl být řádně a včas zapojen do všech procesů a operací zpracování osobních údajů, k nimž v pojišťovně dochází. Toto jmenování je oznámeno všem zaměstnancům.

5.1.2 Pověřencem je zaměstnanec pojišťovny nebo externí poskytovatel služeb (fyzická či právnická osoba), jejichž úkolem je dohlížet na dodržování vnitrostátních, evropských a mezinárodních předpisů, které se týkají ochrany osobních údajů, a těchto Standardů. Pověřenec musí být:

a) způsobilý k výkonu své funkce, tj. jmenován na základě profesních kvalit, zejména na základě odborných znalostí příslušných právních předpisů a praxe v oblasti ochrany osobních údajů;

b) spolehlivý, zodpovědný, důvěryhodný a bezúhonný;

c) schopen komunikovat v jednacím jazyce dle § 16 odst. 1 správního řádu, tedy jazyce českém či slovenském.

5.1.3 Mezi hlavní úkoly pověřence patří:

a) poskytování informací a poradenství pojišťovně o jejích povinnostech plynoucích z GDPR či jiných právních předpisů o ochraně osobních údajů;

b) monitoring souladu s GDPR, jinými předpisy o ochraně osobních údajů a vnitřními postupy a předpisy pojišťovny v oblasti ochrany osobních údajů;

c) poskytování poradenství a odborných vyjádření ve věcech posuzování vlivu na ochranu osobních údajů;

d) spolupráce s dozorovým úřadem;

e) působí jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování a konzultací, včetně předchozích konzultací podle čl. 36 GDPR;

f) dohled nad zajištěním vedení, správy a aktualizace záznamů o činnostech zpracování podle čl. 30 GDPR;

g) poskytování informací a poradenství v oblastech zavádění nových činností zpracování, informování subjektů údajů, předávání osobních údajů do třetích zemí, posuzování postavení pojišťovny a třetích osob při zpracování osobních údajů (včetně poradenství u uzavírání smluv o zpracování);

h) dohlíží na to, že je zaveden systém řešení případů porušení zabezpečení osobních údajů a dle vhodnosti a účelnosti je účasten při řešení těchto případů.

Aby mohl tyto úkoly řádně plnit, má pověřenec právo sledovat veškeré procesy týkající se toků osobních údajů subjektů údajů. Povinností pověřence je, aby seznámil osoby podílející se na zpracovávání osobních údajů s příslušnými právními předpisy.

5.1.4 Nalezne-li pověřenec nesoulad ve zpracovávání osobních údajů pojišťovny se zákonnými požadavky na toto zpracování, je oprávněn navrhnout vhodná opatření k nápravě. Pověřenec nenese osobní odpovědnost za nesoulad zpracování pojišťovnou se Standardy, GDPR a dalšími právními předpisy týkajícími se ochrany osobních údajů.

5.1.5 Pojišťovna včas a vhodnou formou:

a) zveřejní kontaktní údaje pověřence, na základě kterých je pro subjekty údajů snadno dosažitelný, na svých webových stránkách a na jiných vhodných místech;

b) sdělí kontaktní údaje pověřence příslušnému dozorovému úřadu.

Pojišťovna sdělí subjektu údajů kontaktní údaje pověřence, kdykoliv o to požádá, příp. jej alespoň odkáže na místo, kde tyto údaje lze nalézt.

5.1.6 Všechny subjekty údajů, jejichž osobní údaje pojišťovna zpracovává, se mohou na pověřence kdykoliv obrátit a předložit mu své návrhy, dotázat se na informace, jež souvisejí se zpracováním jejich osobních údajů, a zaslat mu stížnost týkající se zpracování osobních údajů, případně jejich řádného a dostatečného zabezpečení pojišťovnou. Komunikace mezi pověřencem a subjektem údajů se považuje za důvěrnou. Pověřenec předává pojišťovně k evidenci a ke zpracování žádosti subjektů o výkon jejich práv.

5.1.7 Pověřenec a další fyzické osoby, které se podílejí na plnění jeho úkolů v pojišťovně, jsou povinni zachovávat mlčenlivost o všech skutečnostech týkajících se ochrany osobních údajů, bezpečnostních opatření a všech dalších důležitých skutečnostech, s nimiž se seznámili při plnění úkolů pověřence nebo v souvislosti s nimi. Tato povinnost trvá i po skončení pracovního poměru či smlouvy, na jejímž základě se podílejí na plnění úkolů. Povinnosti mlčenlivosti se nelze dovolávat vůči pojišťovně, která pověřence jmenovala, orgánu činnému v trestním řízení, soudu nebo dozorovému úřadu.

5.1.8 Parametry výkonu činnosti pověřence pojišťovna zohlední ve své písemné koncepci[20], a to rovněž s ohledem na skutečnost, zda bude tato činnost vykonávaná externě, a to v souladu s pravidly pro externí zajištění činností[21].

5.1.9 Skupina podniků se může rozhodnout, že jmenuje jednoho pověřence pro celou skupinu. V případě, kdy pojišťovna jmenuje zahraničního pověřence, na svůj náklad a svou odpovědnost zajistí překlad jeho jednotlivých vyjádření do českého jazyka.

5.2 Posouzení vlivu na ochranu osobních údajů

5.2.1 Pojišťovna provádí posouzení vlivu na ochranu osobních údajů ve vztahu k nově zaváděným postupům, systémům, programům a jejich změnám, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob (s výjimkou případů, kdy dle právních předpisů není provedení posouzení vlivu pojišťovnou vyžadováno). Zejména se jedná o taková zpracování osobních údajů, při nichž dochází:

- k systematickému a rozsáhlému vyhodnocování osobních aspektů týkajících se fyzických osob, založenému na automatizovaném zpracování (včetně profilování), na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají podobný závažný dopad;
- k rozsáhlému zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se rozsudků ve věcech trestních;
- k rozsáhlému systematickému monitorování veřejně přístupných prostorů.

PŘÍKLAD

Mezi kritéria pro stanovení vysoké rizikovosti zpracování osobních údajů patří provádění ohodnocení nebo hodnocení bonity fyzických osob, včetně profilování a předpovědi, zpracování zvláštních kategorií osobních údajů, zpracování velkého rozsahu, propojování dat různých zpracování, systematické monitorování atd.

5.2.2 Hlavní cílem DPIA analýzy je jistota pojišťovny jako správce, že správně plní své povinnosti při ochraně osobních údajů. Dále DPIA analýza slouží k identifikaci organizačních a technických bezpečnostních opatření, která jsou potřeba pro pokrytí identifikovaných rizik (pozn.: hodnotí se primárně riziko subjektu údajů).

5.2.3 Každá pojišťovna si vyhodnotí nutnost provedení posouzení vlivu na ochranu osobních údajů pro své druhy zpracování a vyžádá si posudek pověřence, je-li jmenován.

C

Správa a monitorování Standardů

1 Přihlášení se ke Standardům a soulad se Standardy

1.1 Přihlášení se ke Standardům, evidence

Přihlášení ke Standardům je dobrovolné a může tak učinit kterákoli pojišťovna, která v době přihlášení dodržuje povinnosti ze Standardů vyplývající.

Přihlášení se ke Standardům probíhá tak, že dotčená pojišťovna zašle ČAP oznámení, jehož vzor tvoří přílohu těchto Standardů, o svém úmyslu připojit se k dodržování Standardů a prohlásí, že dodržuje Standardy a že zajistí dodržování Standardů i do budoucna.

Bez zbytečného odkladu po doručení oznámení a prohlášení uvedených výše ČAP vyrozumí pojišťovnu o tom, že přihlášku akceptuje, a zařadí pojišťovnu do evidence pojišťoven dodržujících Standardy.

ČAP vede veřejnou evidenci pojišťoven dodržujících Standardy. Tato evidence může být dostupná on-line na internetových stránkách ČAP.

1.2 Soulad se Standardy

Každá pojišťovna, která je v evidenci pojišťoven dodržujících Standardy, doručí ČAP do dne 30. 9. příslušného kalendářního roku podklad pro vyhodnocení jejího souladu se Standardy, a to v podobě dohodnuté/navržené ČAP, kdy zejména se může jednat o:

a) informaci o tom, zda jsou ze strany pojišťovny dodržovány Standardy, či nikoli, a to případně i ve formě auditní zprávy pojišťovny o plnění jejích povinností v oblasti ochrany osobních údajů či její části;

b) informaci, zda pojišťovna obdržela v průběhu roku stížnosti subjektů údajů na zpracování osobních údajů touto pojišťovnou, a pokud ano, případně rámcové informace o obsahu těchto stížností a způsobu jejich vypořádání.

1.3 Řešení stížností na nedodržování Standardů

ČAP nebude vyřizovat stížnosti subjektů údajů na nedodržování Standardů ze strany pojišťovny. Každou takto obdrženou stížnost předá ČAP dotčené pojišťovně.

1.4 Postih v případě porušení pravidel

Pokud bude ze strany ČAP na základě vlastní činnosti či konkrétního podnětu zjištěno, že pojišťovna opakovaně závažně porušuje tyto Standardy, je prezidium ČAP oprávněno rozhodnout o vyškrtnutí pojišťovny z evidence pojišťoven dodržujících Standardy do zhojení vytýkaných nedostatků.

V případě vyškrtnutí pojišťovny z evidence pojišťoven dodržujících Standardy může pojišťovna na základě zhojení vytýkaných nedostatků požádat o zrušení postihu (a tedy o opakované zapsání do evidence pojišťoven dodržujících Standardy). Pokud pojišťovna doloží, že vytýkané nedostatky byly zhojeny, ČAP žádosti vyhoví.

2 Správa Standardů

2.1 Pověření správou

Tyto Standardy spravuje ČAP. ČAP zajistí periodické a ad hoc vyhodnocování, zda jsou Standardy stále vyhovující z pohledu standardů trhu a legislativních požadavků; přitom se bude snažit zohledňovat též aktuální vývoj doktríny a rozhodovací praxe v oblastech ochrany osobních údajů a pojišťovnictví, zejména stanoviska Evropského sboru pro ochranu osobních údajů, konečná rozhodnutí soudních orgánů a dozorových úřadů v České republice a na evropské úrovni (Soudní dvůr EU) a informovat o tom členské pojišťovny.

V případě, že se pojišťovna, která je v evidenci pojišťoven dodržujících Standardy, dozví o nové skutečnosti nebo o novém materiálu, které jsou relevantní pro tyto Standardy a jejich aktuálnost, bude o tom ČAP v přiměřené době informovat.

2.2 Změny a aktualizace

Pokud ze strany ČAP či ze strany pracovní skupiny pojišťoven vedené ČAP bude vyhodnoceno, že je nutné Standardy aktualizovat, učiní tak ČAP postupem dle tohoto článku Standardů.

Standardy budou zpravidla aktualizovány jedenkrát ročně, pokud nebude na základě vývoje v oblastech zpracování osobních údajů a pojišťovnictví nutné aktualizovat Standardy častěji.

ČAP může i samostatně provádět dílčí změny těchto Standardů, které nebudou mít podstatný dopad na povinnosti pojišťoven dle těchto Standardů, a to rozhodnutím prezidia ČAP na základě čl. V odst. 2.2 písm. g) stanov.

Změny Standardů, které budou mít podstatný dopad na povinnosti pojišťoven dle těchto Standardů, budou schvalovány ze strany pracovní skupiny pojišťoven vedené ČAP.

Jednání této pracovní skupiny (vč. určení termínu a pořadu jednání) svolává ČAP.

Ke schválení navrhované změny je třeba nadpoloviční většiny všech pojišťoven, jejichž zástupci se účastní konkrétní pracovní skupiny, kdy každá z pojišťoven má vždy 1 hlas.

V případě provedení změny Standardů dle ustanovení výše sestaví ČAP konsolidovanou verzi Standardů a doručí ji všem pojišťovnám evidovaným jako pojišťovny dodržující Standardy; zároveň ji zveřejní na svých internetových stránkách, pokud takto byla zveřejněna předchozí verze.

Účinnost změn Standardů vůči pojišťovnám nastává uplynutím doby tří měsíců, počítané od prvního dne měsíce následujícího po měsíci, ve kterém byla pojišťovnám doručena konsolidovaná verze dle předchozího odstavce; doručování je prováděno na kontaktní e-maily pojišťoven sdělené pro tento účel. Již před účinností nové verze Standardů je pojišťovna povinna provést potřebné kroky k tomu, aby byla schopna se od počátku účinnosti změn řídit novou verzí Standardů. Doba pro nabytí účinnosti změny Standardů může být ve výjimečných případech zkrácena za účelem rychlejší reakce na potřeby trhu nebo legislativní požadavky či naopak prodloužena za účelem poskytnutí delšího času na přípravu implementace změny; tato skutečnost bude součástí rozhodnutí o provedení změny.

Příloha č. 1

k Samoregulačním standardům České asociace pojišťoven k uplatňování obecného nařízení o ochraně osobních údajů (GDPR) v pojišťovnictví

Oznámení členské pojišťovny ČAP o přistoupení

Pojišťovna: _____

(dále jen „pojišťovna“)

Pojišťovna tímto oznamuje České asociaci pojišťoven („ČAP“) svůj úmysl připojit se k dodržování Samoregulačních standardů České asociace pojišťoven k uplatňování obecného nařízení o ochraně osobních údajů (GDPR) v pojišťovnictví přijatých dne _____ (dále jen „Standardy“).

V souladu s částí C bodu 1.1 Standardů pojišťovna prohlašuje, že dodržuje Standardy a že zajistí dodržování Standardů i do budoucna.

Pojišťovna ustanovuje kontaktní a odpovědnou osobu (osoby) pro účely Standardů.

Kontaktní a odpovědná osoba:

Jméno: _____

Funkce: _____

E-mailová adresa: _____

Telefon: _____

V _____ dne _____

Za pojišťovnu: _____

Příloha č. 2

k Samoregulačním standardům České asociace pojišťoven k uplatňování obecného nařízení o ochraně osobních údajů (GDPR) v pojišťovnictví

V případě, že interní šetření pojišťovny odhalí porušení zabezpečení, které pravděpodobně představuje riziko pro práva a svobody fyzických osob, pojišťovna sdělí dozorovému úřadu informace dle čl. 33 GDPR. Pojišťovna může toto ohlášení učinit pomocí této standardizované šablony, pomocí formuláře „Ohlášení porušení zabezpečení osobních údajů dle GDPR" publikovaného dozorovým úřadem[22] nebo jiným vhodným způsobem.

Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR
Strana 1

Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

I IDENTIFIKACE SPRÁVCE

Informace jsou určeny výhradně příslušnému dozorovému úřadu. Nejsou určeny ke sdílení s třetími stranami.

I.1 Podrobné informace o společnosti

Název společnosti	
Adresa	
PSČ	
Město	
Stát	

I.2 Kontaktní osoba (k zjištění doplňujících informací)

Jméno	
Pracovní pozice	
Adresa	
PSČ	
Město	
Stát	
E-mailová adresa	
Telefonní číslo	

I.3 Typ ohlášení

☐ Kompletní ohlášení (pole obsažené v částech II a III se vyplní ve lhůtě 72 hodin od okamžiku, kdy se subjekt o porušení zabezpečení dozví)

☐ Ohlášení ve dvou krocích (pole obsažené v části II se vyplní ve lhůtě 72 hodin od okamžiku, kdy se subjekt o porušení zabezpečení dozví, a pole obsažené v části III se vyplní ve lhůtě 4 týdnů od okamžiku, kdy se subjekt o porušení zabezpečení dozví)

[22] Formulář „Ohlášení porušení zabezpečení osobních údajů dle GDPR" je k dispozici zde: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38403.

Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR Strana 2

Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

II HLAVNÍ INFORMACE K PORUŠENÍ ZABEZPEČENÍ

K vyplnění a sdílení s dozorovým úřadem ve lhůtě 72 hodin od okamžiku, kdy se subjekt o porušení zabezpečení dozví.

II.1 Odvětví dotčeného subjektu

- ☐ Zemědělství, lesnictví a rybolov
- ☐ Těžba a dobývání
- ☐ Výroba
  - ☐ Výroba potravin, nápojů a tabákových výrobků
  - ☐ Výroba textilií, oděvů, usní a souvisejících výrobků
  - ☐ Výroba dřevěných a papírových produktů, tisk a rozmnožování nahraných nosičů
  - ☐ Výroba koksu a rafinovaných ropných produktů
  - ☐ Výroba chemických látek a chemických přípravků
  - ☐ Výroba základních farmaceutických výrobků a farmaceutických přípravků
  - ☐ Výroba pryžových a plastových výrobků a ostatních nekovových minerálních výrobků
  - ☐ Výroba základních kovů a kovodělných výrobků kromě strojů a zařízení
  - ☐ Výroba počítačů, elektronických a optických přístrojů a zařízení
  - ☐ Výroba elektrických zařízení
  - ☐ Výroba strojů a zařízení
  - ☐ Výroba dopravních zařízení
  - ☐ Další výroba; opravy a instalace strojů a zařízení
- ☐ Dodávání elektřiny, plynu, páry a klimatizovaného vzduchu
- ☐ Rozvod vody; kanalizace, nakládání s odpadem a sanace
- ☐ Stavebnictví
- ☐ Velkoobchod a maloobchod; opravy motorových vozidel
- ☐ Doprava a skladování
- ☐ Ubytování
- ☐ Stravování a pohostinství
- ☐ Vydavatelské, audiovizuální a vysílací činnosti
- ☐ Telekomunikace
- ☐ IT a další informační služby
- ☐ Finanční služby a pojišťovnictví

Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR
Strana 3

- ☐ Činnosti v oblasti nemovitostí
- ☐ Právní, účetní, manažerské, architektonické, inženýrské činnosti, technické zkoušky a analytické činnosti
- ☐ Vědecký výzkum a vývoj
- ☐ Ostatní odborné, vědecké a technické činnosti
- ☐ Administrativní a podpůrné činnosti
- ☐ Veřejná správa, obrana; povinné sociální zabezpečení
- ☐ Vzdělávání
- ☐ Činnosti týkající se lidského zdraví
- ☐ Ústavní sociální péče a mimoústavní sociální péče
- ☐ Kulturní, zábavní a rekreační činnosti
- ☐ Ostatní činnosti
- ☐ Činnosti domácností jako zaměstnavatelů; činnosti domácností produkujících blíže neurčené výrobky a služby
- ☐ Činnosti domácností pro vlastní spotřebu
- ☐ Činnosti exteritoriálních organizací a orgánů

II.2 Velikost subjektu – počet zaměstnanců

- ☐ 1–9
- ☐ 10–49
- ☐ 50–249
- ☐ 250–749
- ☐ 750–1000
- ☐ > 1000

II.3 Velikost subjektu – obrat

- ☐ ≤ 2 mil. €
- ☐ ≤ 10 mil. €
- ☐ ≤ 50 mil. €
- ☐ > 50 mil. €

II.4 Stát, ve kterém se nachází hlavní provozovna

II.5 Stát, ve kterém došlo k porušení zabezpečení

II.6 Datum/čas porušení zabezpečení

II.7 Datum/čas zjištění porušení zabezpečení

Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR
Strana 4

II.8 Správa osobních údajů

☐ Na místě ☐ Cloud

II.9 Jste si vědomi příčiny vzniku porušení zabezpečení? (V případě, že ne, viz otázka 7 v části III.)

☐ Škodlivý útok
- ☐ Interní ☐ Externí

☐ Nehoda (chyba v systému)
☐ Nedbalost (lidské pochybení)
☐ Jiná

II.10 V případě škodlivého útoku je příčinou porušení zabezpečení:

☐ Neznámý nedostatek
☐ Známý nedostatek:
- ☐ Cryptolocker
- ☐ Fire reconnaissance
- ☐ Phishing
- ☐ DoS
- ☐ Malware
- ☐ Sociální inženýrství
- ☐ Vydírání

☐ Jiná

II.11 Jaký je předpokládaný dopad porušení zabezpečení?

☐ Zveřejnění údajů
☐ Krádež údajů
☐ Krádež identity nebo podvod
☐ Ztráta údajů
☐ Ztráta důvěrnosti osobních údajů
☐ Majetková škoda
☐ Přímá finanční ztráta
☐ Přerušení podnikatelské činnosti
☐ Odpovědnostní následky
☐ Poškození pověsti
☐ Jiný

Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR
Strana 5

II.12 Typ využívaných/dotčených/ukradených údajů

- ☐ Osobní
  - ☐ Citlivé (zdravotní, genetické atd.)
  - ☐ Jiné
- ☐ Jiné

II.13 V případě, že se jedná o osobní údaje, je úroveň jejich šifrování:

☐ Plná ☐ Částečná ☐ Žádná

II.14 Byly údaje, u kterých došlo k porušení zabezpečení, předmětem posouzení vlivu na ochranu osobních údajů (DPIA)?

☐ Ano ☐ Ne

II.15 Jaký typ IT podpory je využíván?

☐ Interní ☐ Externí

II.16 Jaká opatření byla přijata ke zmírnění nepříznivých účinků porušení zabezpečení?

- ☐ Obnova údajů
- ☐ Výmaz nevhodného softwaru
- ☐ Update systému
- ☐ Náhrada zničeného majetku
- ☐ Externí testování (pen testy atd.)
- ☐ Posílení bezpečnostních opatření
- ☐ Jiné

II.17 Je subjekt pojištěn pro případy tohoto typu?

☐ Ano ☐ Ne

Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR Strana 6

Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

III DOPLŇUJÍCÍ INFORMACE K PORUŠENÍ ZABEZPEČENÍ

K vyplnění a sdílení s dozorovým úřadem ve lhůtě 4 týdnů od okamžiku, kdy se subjekt o porušení zabezpečení dozví.

III.1 Datum/čas ukončení následků útoku

III.2 Kolik osobních datových souborů bylo využívaných/dotčených/ukradených?

III.3 Byly subjekty údajů obeznámeny s porušením zabezpečení?

☐ Ano ☐ Ne

III.4 Kolik subjektů údajů bylo obeznámeno?

III.5 Odhadovaná finanční ztráta

Cena obeznámení

Finanční škoda

III.6 Jaká opatření byla podniknuta nebo plánována ke zmírnění pravděpodobnosti budoucího porušení zabezpečení?

☐ Posílení bezpečnostních opatření a především:
- ☐ Audit a přepracování procesu sběru dat
- ☐ Audit a přepracování procesu zpracování dat
- ☐ Audit a přehodnocení „zpracovatele" (lze-li aplikovat)
- ☐ Šifrování data at rest

☐ Žádná opatření nebyla přijata

☐ Jiné

Šablona pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR
Strana 7

III.7 Jste si vědomi příčiny porušení zabezpečení?

- ☐ Škodlivý útok
  - ☐ Interní ☐ Externí
- ☐ Nehoda (chyba v systému)
- ☐ Nedbalost (lidské pochybení)
- ☐ Jiná

III.8 Je-li známa, jaká byla motivace k porušení zabezpečení, jednalo-li se o škodlivý útok?

III.9 Je-li znám, jaký škodlivý software byl použit v případě škodlivého útoku?

- ☐ Útok prostředníka
- ☐ Malware
- ☐ Ransomware
- ☐ SQL Injection Attack
- ☐ Cross-site scripting (XSS)
- ☐ Denial of Service (DoS)
- ☐ Session hijacking
- ☐ Credential reuse
- ☐ Jiný

Příloha č. 3

k Samoregulačním standardům České asociace pojišťoven k uplatňování obecného nařízení o ochraně osobních údajů (GDPR) v pojišťovnictví

Dle části C ustanovení 1.2 Standardů každá pojišťovna, která je v evidenci pojišťoven dodržujících Standardy, doručí ČAP do dne 30. 9. příslušného kalendářního roku podklad pro vyhodnocení jejího souladu se Standardy, a to v podobě dohodnuté/navržené ČAP, kdy zejména se může jednat o:

c) informaci o tom, zda jsou ze strany pojišťovny dodržovány Standardy, či nikoli, a to případně i ve formě auditní zprávy pojišťovny o plnění jejích povinností v oblasti ochrany osobních údajů či její části;

d) informaci, zda pojišťovna obdržela v průběhu roku stížnosti subjektů údajů na zpracování osobních údajů touto pojišťovnou, a pokud ano, případně rámcové informace o obsahu těchto stížností a způsobu jejich vypořádání.

Pojišťovna může toto ohlášení učinit pomocí této standardizované šablony.

Oznámení členské pojišťovny o vyhodnocení souladu se Samoregulačními standardy ČAP k uplatňování obecného nařízení o ochraně osobních údajů (GDPR) v pojišťovnictví ke dni 30. 9. 20____

Pojišťovna: _____

(dále jen „pojišťovna")

Pojišťovna tímto oznamuje České asociaci pojišťoven („ČAP") ve smyslu části C odst. 1.2 Samoregulačních standardů České asociace pojišťoven k uplatňování obecného nařízení o ochraně osobních údajů (GDPR) v pojišťovnictví (dále jen „Standardy"), že Standardy dodržuje/nedodržuje*.

Komentář:

(Zde uveďte informace, kterými doplníte výše konstatované. Může se jednat o informace o plnění povinnosti dodržovat Standardy, případně připojte auditní či jiné zprávy, které pojišťovna v daném roce provedla, informace o komunikaci s ÚOOÚ apod.)

_____

_____

Pojišťovna dále sděluje, že obdržela v období od 1. 10. 20___ do 30. 9. 20___ stížnosti subjektů údajů na zpracování osobních údajů:

Komentář:

(Zde uveďte rámcové informace o obsahu, způsobu vypořádání těchto stížností, příp. jejich počet.)

_____

_____

V _____ dne 30. 9. 20 ____ Za pojišťovnu: _____

*) nehodící se škrtněte

Samoregulační standardy České asociace pojišťoven k uplatňování obecného nařízení o ochraně osobních údajů (GDPR) v pojišťovnictví

Účinné od 1. srpna 2020

Vydavatel
Česká asociace pojišťoven, Main Point Pankrác, Milevská 2095/5, 140 00 Praha 4 – Nusle
Tel.: +420 222 350 150, e-mail: info@cap.cz, www.cap.cz