Bezpečnostní směrnice společnosti Finance Bulldog

1. Základní ustanovení a výklad pojmů
Tato směrnice upravuje technická a organizační opatření vedoucí k ochraně osobních údajů v souladu s právními předpisy, zejm. obecným nařízením o ochraně osobních údajů (nařízení EU 2016/679 - dále jen nařízení) a závaznými národními předpisy.

Účelem zabezpečení je zamezení neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Tato směrnice se vztahuje na zprostředkovatele finančních služeb a jejich spolupracovníky v souladu se právními předpisy týkajícími se distribuce finančních služeb (dále jen „zákon o distribuci"). Dále se tato směrnice vztahuje na příslušné osoby Finance Bulldog, které přicházejí do styku s osobními údaji.

Porušení povinností této směrnice je podstatným porušením zprostředkovatelské smlouvy uzavřené s Finance Bulldog se všemi důsledky z takového porušení vyplývajícími.
Spolupracovníkem se rozumí osoba oprávněná k výkonu zprostředkovatelské činnosti podle příslušného zákona, která vykonává zprostředkovatelskou činnost na základě smlouvy se zprostředkovatelem. Spolupracovníkem je např. podřízený pojišťovací zprostředkovatel nebo jiné kategorie zprostředkovatelů v souladu s platnými předpisy. Spolupracovníkem mohou být i další osoby spolupracující se zprostředkovatelem na základě smluvního vztahu (pracovní poměr, příkazní smlouva, smlouva o obchodním zastoupení, smlouva o spolupráci atd.).

Osobním údajem (dále jen „OÚ") se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Osobním údajem tedy může být např. i telefonní číslo, emailová adresa (zejm. pokud obsahuje jméno a/či příjmení), rodné číslo, kód zaměstnance, číslo bankovního účtu, číslo pojistné smlouvy, za určitých okolností např. i IP adresa = informace, dle které lze přímo či nepřímo (ve spojení s dalšími informacemi či údaji) určit konkrétní fyzickou osobu.

Citlivým údajem osobní údaj zvláštní kategorie vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů. Citlivým údajem je dále informace týkajících se rozsudků v trestních věcech a trestných činů.

V oblasti pojištění půjde především o informace o konkrétní prodělané či aktuální nemoci či úrazu, podstoupené léčbě, hospitalizaci, podstoupených vyšetřeních, medikaci apod. (nejčastěji ve formě zdravotního dotazníku, lékařských zpráv, zdravotní dokumentace, dokumentace poskytnuté v rámci likvidace pojistných událostí apod.).

Subjektem údajů se rozumí fyzická osoba, k níž se osobní údaje vztahují, neuplatní se ve vztahu k právnickým osobám, uplatní se však pro fyzické osoby podnikající.

Správcem osobních údajů se rozumí každý subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele.

Zpracovatelem se rozumí každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje.

Zpracováním osobních údajů se rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo

pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Likvidací osobních údajů se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalšího zpracování.

Prostor je zabezpečené místo vyhrazené pro zpracování OÚ, např. obchodní místo, provozovna zprostředkovatele apod.

Systémem se rozumí jakýkoli počítačový program, který je provozován společností Finance Bulldog, jako je například Informační systém (dále jen „systém")

2. Technické a organizační opatření
Zprostředkovatel se zavazuje plnit níže uvedená technická a organizační opatření vedoucí k ochraně osobních údajů:

2.1. Všichni Spolupracovníci Zprostředkovatele pracující s OÚ musí být seznámeni s níže uvedenými pravidly pro zpracování osobních údajů a jejich odpovědnostmi a povinnostmi v procesu zpracování OÚ formou poučení před vlastní prací s OÚ. Zprostředkovatel zajistí pravidelné školení Spolupracovníků.

2.2. V případě porušení stanovených pravidel pro práci s OÚ Spolupracovníkem musí Zprostředkovatel neprodleně informovat Finance Bulldog o tomto porušení a o provedených opatřeních a vyvodit odpovědnost za toto porušení vůči Spolupracovníkovi.

2.3. Zprostředkovatel ani Spolupracovníci Zprostředkovatele nesmí sdílet OÚ s osobami, které nejsou oprávněny s danými OÚ pracovat.

2.4. Zprostředkovatel i každý jeho Spolupracovník pracující s OÚ musí mít vlastní přístupová oprávnění do systémů uchovávajících OÚ. K jakým datům a jaké operace s daty mohou spolupracovníci provádět, definuje Zprostředkovatel, přičemž rozsah podléhá schválení Finance Bulldog. Zprostředkovatel bude dbát na to, aby měli Spolupracovníci přístup jenom k OÚ, které potřebují pro výkon své činnosti. Finance Bulldog následně zajistí dle interních procesů požadovaná přístupová oprávnění v systému.

2.5. V případě, že jakýkoliv Spolupracovník již dále nemá mít přístup k OÚ nebo mají být přístupová oprávnění upravena, je Zprostředkovatel povinen neprodleně, nejpozději však do 24 hodin informovat Finance Bulldog o této skutečnosti. Finance Bulldog následně provede odebrání či úpravu přístupových oprávnění.

2.6. Zprostředkovatel musí poskytnout veškerou součinnost v případě požadavku na revizi účtů ze strany Finance Bulldog, jakož i při kontrole dodržování všech technicko-organizačních opatření sloužících k ochraně OÚ ze strany Finance Bulldog.

2.7. Zprostředkovatel i jeho Spolupracovníci pracující s OÚ musí používat hesla s dostatečnou bezpečnostní sílou, aby je nebylo možné jednoduše uhodnout nebo získat.

2.8. Zprostředkovatel i jeho spolupracovníci nesmí mít své přihlašovací údaje k systémům zpracujícím OÚ nebo k pracovní stanici volně dostupné a musí dbát na bezpečnost a důvěrnost těchto přihlašovacích údajů (např. poznačení přístupových údajů na poznámkový blok na pracovním stole je zakázáno). Zprostředkovatel ani jeho Spolupracovníci nesmí sdělit své přihlašovací údaje do systému sobě navzájem či třetí osobě.

2.9. Zprostředkovatel i jeho spolupracovníci jsou povinni zabezpečit svou pracovní stanici pomocí programu pro odhalení škodlivého programového vybavení (tj. antivirus) a dbát na používání aktuální verze operačního systému.

2.10. Zprostředkovatel i jeho spolupracovníci jsou povinni před jakoukoli operací zvážit, zda jde o citlivý osobní údaj. Takovýto údaj nesmí být vložen do systému. V případě, že je zprostředkovatel, nebo spolupracovník na pochybách, vždy k údaji přistupuje jako k citlivému.

3. Opatření fyzické bezpečnosti osobních údajů
3.1. Prostory, kde dochází k manuálnímu nebo automatizovanému zpracování OÚ, musí za účelem zabránění neoprávněnému přístupu k OÚ splňovat následující:

a) přístup do prostor, kde dochází k zpracování OÚ, musí být chráněn vhodnými zámky;
b) v případě, že tyto prostory mají okna, která jsou přístupná z vnější strany budovy a představují potenciální místo průniku do budovy, musí být tato okna chráněna mřížemi, bezpečnostními fóliemi, nebo elektronickým zabezpečovacím systémem, nebo musí být dokumenty s OÚ uzamčeny v zabezpečeném úložném prostoru (např. trezor, plechová skříň, pevná uzamykatelná skříň).
c) Případně je možné zabezpečit prostory jinými opatřeními, které poskytují stejnou nebo vyšší míru ochrany (např. elektronické zabezpečovací systémy, ochranka atp.).

3.2. Skříně, pořadače a jiné objekty sloužící pro uchovávání dokumentů a jiných médií (CD, DVD apod.) s OÚ musí být, za účelem zabránění neoprávněnému přístupu k OÚ, uzamykatelné.

3.3. Zprostředkovatel i všichni Spolupracovníci Zprostředkovatele musí dbát na zamykání prostorů a objektů s OÚ (tj. uzavření oken a uzamknutí dveří) v případě krátkodobé i dlouhodobé nepřítomnosti na pracovišti.

3.4. Zprostředkovatel i všichni Spolupracovníci Zprostředkovatele musí dodržovat pravidla čistého stolu. Tj. v případě krátkodobé i dlouhodobé nepřítomnosti na pracovišti zajistit uložení dokumentů s OÚ do objektů určených pro uchovávání dokumentů, tak, aby nebyly tyto dokumenty volně přístupné pro neoprávněné osoby.

3.5. Likvidace dokumentů a médií s OÚ musí probíhat tak, aby nebylo možné tyto OÚ získat prostým nalezením vyhozených dokumentů a médií. Pro likvidaci papírových dokumentů se musí využívat skartace, pro likvidaci jiných médií příslušné metody (např. normovaným přepisem, fyzickou likvidací, odevzdáním na určenou pobočku) pro zamezení čitelnosti a rekonstrukci dat.

3.6. Zprostředkovatel i všichni jeho Spolupracovníci jsou povinni nakládat s dokumenty obsahujícími OÚ v listinné či elektronické podobě mimo zabezpečené prostory určené ke zpracování OÚ tak, aby nemohlo dojít k jejich neoprávněnému zpracování či zneužití, např. změně, ztrátě, zničení, přenosům, odcizení, zničení či odposlechnutí (zejména neponechávat dokumenty obsahující OÚ v listinné i elektronické podobě v autě či veřejném prostoru bez dohledu), či k neoprávněnému nebo nahodilému přístup k nim. Pro přenos OÚ musí použít vhodné ochranné obaly (např. uzamykatelný kufřík, neprůhledné desky, zaheslované PC/paměťové kary atp.).

3.7. Zobrazovací zařízení (monitor a další) musí být umístěno tak, aby zobrazované osobní údaje (dále jen OÚ) nemohly být zachyceny neoprávněnými osobami.

3.8. Zprostředkovatel nesmí pro přenos informací obsahujících OÚ v elektronické podobě používat veřejná úložiště dat (např. Uloz.to, letecká pošta, cloud). Zveřejněním, resp. uložením dat klientů či dat Finance Bulldog samotné na veřejném úložišti dat, může dojít k potenciálním závažným důsledkům vyplývajícím jak z porušování mlčenlivosti o pojištění osob dle zákona č. 89/2012, občanský zákoník, a zákona č. 277/2009 Sb., o pojišťovnictví, tak z porušování právních předpisů a smluvních ujednání na ochranu osobních údajů, potažmo i porušování odborné péče, obchodních tajemství a know-how a obecně poškozování zájmů Finance Bulldog.

4. Lhůty
4.1. Zprostředkovatel je povinen zajistit skartaci listin, nebo nosičů, obsahující OÚ dle skartačního řádu. Lhůta ve skartačním řádu zprostředkovatele však nesmí být delší než lhůta uvedená ve skartačním řádu společnosti Finance Bulldog.

4.2. V případě, že zprostředkovatel nemá vlastní skartační řád, má se za to, že v plném rozsahu přejímá skartační řád společnosti Finance Bulldog.

5. Hlášení incidentů
5.1. V případě, že zprostředkovatel, nebo jeho spolupracovníci zjistí, že mohlo dojít k narušení bezpečnosti OÚ (neoprávněné zveřejnění, nakládání, atd.) Řídí se následujícím postupem:

a) Provede všechny kroky vedoucímu k minimalizaci případných škod. Především pak provede nezbytné kroky vedoucí k zastavení pokračování incidentu
b) Písemnou formou na e- mail **zou@financebulldog.cz** či telefonicky kontaktuje jednatele Finance Bulldog.
c) V písemné komunikaci popíše druh incidentu a jak k němu došlo.
d) Dále se řídí pokyny jednatele.

V Pelhřimově 20.5.2018
Václav Pech
Jednatel Finance Bulldog, s.r.o.

Platná od 20.5.2018
Účinná od 25.5.2018