

## 1 Informace o zpracovateli a pověřenci pro ochranu osobních údajů

Identifikace zpracovatele	
Identifikační číslo (IČO)	
Obchodní firma nebo název, resp. jméno a příjmení	
Adresa sídla (resp. bydliště)	
Město	
PSC	

Identifikace pověřence pro ochranu osobních údajů, pokud ho zpracovatel má	
Titul	
Příjmení	
Jméno	
Kontaktní adresa	
E-mail	

## 2 Popis kategorií zpracování pro správce

<b>Identifikace správce</b>	
<b>Identifikační číslo (IČO)</b>	278 47 268
<b>Obchodní firma nebo název</b>	AGENTURA KRYŠTOF s.r.o.
<b>Adresa sídla</b>	Jesenická 3071/1D
<b>Město</b>	Šumperk
<b>PSČ</b>	787 01

### Kategorie zpracování prováděné pro správce

Zpracování osobních údajů zájemců o pojištění, pojišťovacích zprostředkovatelů případně třetích osob pro správce v oblasti:

- modelace, návrh a uzavření pojistné smlouvy,
- posouzení přijatelnosti do pojištění,
- zajišťování klientského servisu a správa pojistné smlouvy,
- nabízení výrobků a služeb správce, pokud je k tomu udělen souhlas.

přičemž podrobnosti o zajišťovaných činnostech jsou obsahem Smlouvy o obchodním zastoupení ze dne [...].

### Předání osobních údajů do třetí země nebo mezinárodní organizaci

Osobní údaje se nepředávají do třetí země.

### 3 Popis technických a organizačních bezpečnostních opatření

U zpracovatele jsou standardně zavedena zejména následující technická a organizační opatření, aby nemohlo dojít k 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:

- osobní údaje jsou uchovávány výlučně na zabezpečených serverech nebo na zabezpečených nosičích dat, jedná-li se o osobní údaje v elektronické podobě
- přístup k osobním údajům mají pouze pověřené osoby zpracovatele
- je přijata a udržována vhodná kombinace technicko-organizačních opatření a principů k zajištění požadované úrovně zabezpečení, mezi které patří zejména:
  - zajištění toho, že přístup k osobním údajům mají pouze pověřené osoby zpracovatele;
  - zabránění neoprávněnému přístupu k datovým nosičům;
  - antivirová ochrana a kontrola neoprávněných přístupů;
  - zajištění toho, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze pověřené osoby;
  - provádění šifrování a pseudonymizace osobních údajů;
  - schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování a provádění kontrol zavedených opatření a jejich korektního fungování pravidelně kontrolovat;
  - schopnost obnovit dostupnost osobních údajů a přístup k nim včas a v případě fyzických či technických incidentů.

V případech, kdy zpracovatel zpracovává osobní údaje v rámci jednoho nebo více informačních systémů, pak aplikuje ještě další opatření a principy, zejména:

- pořizování elektronických záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány;
- 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
- proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;
- ochrana perimetru informačního systému, např. víceúrovňovým firewallem;
- šifrovaný přenos dat prostřednictvím IT technologií a sítí;
- servery s osobními údaji musí vykazovat vysokou míru fyzického zabezpečení, tedy jsou např. uzamčeny v serverovně; a
- případné zálohy dat prováděné do jiné lokality jsou prováděny šifrovaným přenosem a přístup k nim mají pouze pověřené osoby zpracovatele.

Při zpracování osobních údajů v jiné než elektronické podobě jsou osobní údaje uchovány v místnostech s náležitou úrovní zabezpečení, do kterých mají přístup výlučně pověřené osoby.