

## SMĚRNICE O OCHRANĚ OSOBNÍCH ÚDAJŮ

Tato vnitřní směrnice pro ochranu osobních údajů upravuje nakládání s osobními údaji a opatření k zajištění ochrany osobních údajů v souladu s Nařízením 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 „**Nařízení**“ s cílem zajištění jednotného postupu při přijímání a realizaci opatření ochrany osobních údajů v podmínkách

### společnosti Cattacan, s.r.o.

IČO 27171451, se sídlem Praha 4, Kukučínova 1148/4, PSČ 142 00 (dále jen „**správce**“), (dále jen „**Směrnice**“).

Tato Směrnice se vydává jako vnitřní předpis ve smyslu ust. § 305 a násl. Zákoníku práce a je závazná pro všechny zaměstnance správce. Tato směrnice je rovněž závazná pro obchodní partnery správce, kteří se mohou při plnění svých smluvních povinností dostat do styku s osobními údaji, se kterými správce nakládá.

Směrnice je veřejně přístupná, a to v písemné podobě na vyžádání v kanceláři HR a v digitální podobě na adrese [www.cattacan.cz](http://www.cattacan.cz)

### 1. Úvod

- 1.1. Pro účely této Směrnice, a v souladu s Nařízením a ostatní platnou legislativou týkající se ochrany osobních údajů, se rozumí:
  - a. **osobními údaji** veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat za použití konkrétních identifikátorů či prvků;
  - b. **zpracováním osobních údajů** jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je např. 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;
  - c. **správce** subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
  - d. **zpracovatelem** subjekt, který zpracovává osobní údaje pro správce na základě smluvního vztahu a dle jeho pokynů;
  - e. **automatizovaným zpracováním** operace uskutečňované zcela nebo zčásti pomocí automatizovaných postupů;
  - f. **profilováním** jakákoliv forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě.

## 2. Základní zásady zpracování osobních údajů

2.1. Osobní údaje jsou zpracovávány výhradně:

- a. v souladu s Nařízením, a ostatní platnou legislativou týkající se ochrany osobních údajů a touto Směrnicí, korektně a transparentně zejména ve vztahu k subjektu osobních údajů;
- b. výhradně v souladu s účelem za jakým byly získány, v nezbytném rozsahu a po dobu nezbytnou pro daný účel;
- c. v přesné a aktuální podobě.

2.2. Osobní údaje jsou zpracovávány výhradně pokud:

- a. subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro daný účel;
- b. 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;
- c. zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
- d. zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
- e. zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, krom případů stanovených platnou legislativou.

2.3. Ke zpracování osobních údajů dochází prostřednictvím výpočetní techniky, popř. i manuálním způsobem u osobních údajů v listinné podobě, za dodržení všech bezpečnostních zásad pro správu a zpracování osobních údajů.

2.4. Veškeré osoby, kterým mohou být osobní údaje zpřístupněny, jsou poučeny o svých povinnostech ve vztahu k osobním údajům, respektují právo subjektů údajů na ochranu soukromí a jsou povinny postupovat dle Nařízení a ostatní platné legislativy týkající se ochrany osobních údajů a v souladu s touto Směrnicí, případně dalšími vnitřními předpisy, jsou-li stanoveny.

## 3. Bezpečnost nakládání s osobními údaji

3.1. Za účelem bezpečnosti nakládání s osobními údaji realizuje správce technicko - organizační opatření k zajištění ochrany osobních údajů tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

3.2. Technicko - organizačními opatřeními jsou v podmínkách správce zejména:

- a. **pseudonymizace** osobních údajů – pokud je to z hlediska obecně závazných právních předpisů možné a z hlediska provozu správce účelné a nedojde k výmazu osobních údajů, zpracuje správce osobní údaje tak, že již nemohou být přiřazeny ke konkrétnímu subjektu údajů bez použití dodatečných informací. Tyto dodatečné informace budou uchovány odděleně, aby nemohly být přiřazeny ke konkrétní fyzické osobě.
- b. **šifrování nebo jiné elektronické zabezpečení** osobních údajů – Přístupy do všech systémů jsou zabezpečeny pomocí přístupových práv a přístupová hesla jsou dostatečně nastavena a je vyžadována jejich pravidelná obnova. Přístupy z vnější sítě (internetu) jsou zabezpečeny pomocí Firewall. Pokud budou osobní údaje zasílány v elektronické podobě mimo počítačovou síť správce, budou vždy

zabezpečeny tak, aby byly náležitě chráněny proti zneužití nepovolanou osobou (šifrování datových přenosů pomocí SSL certifikátů a PKI – zabezpečení infrastruktury veřejných klíčů, zaheslování, ochrana SWQ a HW pomocí systému Sophos).

- c. **zajištění důvěrnosti, integrity, dostupnosti a odolnost** systémů a služeb zpracování – pomocí zavedení standardních nástrojů na ochranu dat (SW i HW) – odpovídá interní oddělení IT správce.
  - d. **monitorování** přístupu k osobním údajům a účinné omezení přístupu k jednotlivým osobním údajům – v podmínkách správce mají přímý přístup k osobním údajům pouze management společnosti, vedoucí osobního oddělení (HR), vedoucí finančního oddělení a vedoucí oddělení IT a účetní. Ostatní osoby mají přístup k osobním údajům pouze na vyžádání, pokud prokáží důležitý zájem na jejich zpřístupnění.
  - e. schopnosti **obnovit dostupnost** osobních údajů a přístup k nim včas v případě fyzických či technických incidentů – zajištěno formou zálohování.
  - f. **fyzické zabezpečení** prostor, kde se nachází úložiště osobních údajů v elektronické/listinné podobě. Osobní údaje v listinné podobě jsou uloženy odděleně a řádně zabezpečeny v místnosti k tomu účelu určené a má k nim přímý přístup pouze vedoucí osobního oddělení (HR) a vedoucí finančního oddělení. Servery, na kterých jsou uloženy osobní údaje, se nacházejí ve zvláštních prostorách a jsou důkladně zabezpečeny – přístup má pouze management společnosti a IT oddělení.
- 3.3. Přijatá bezpečnostní opatření procházejí pravidelným procesem **testování**, posuzování a hodnocení jejich účinnosti pro zajištění bezpečnosti nakládání s osobními údaji, a to s periodicitou nejméně jedenkrát (1x) ročně. Záznam o výsledku tohoto procesu, společně s návrhem a dodatečných opatření, se archivuje nejméně po dobu pěti (5) let.
- 3.4. Jakákoliv osoba, která jedná za **pověření** správce a má přístup k osobním údajům, zpracovává tyto osobní údaje pouze v souladu s Nařízením a ostatní legislativou týkající se ochrany osobních údajů a touto Směrnicí, pokud jí platná legislativa neukládá jinak, např. externí dodavatelé IT služeb, dodavatelé řešení Cloud a externí účetní společnost.
- 3.5. Pokud zpracovává osobní údaje pro správce **zpracovatel**, využije správce pouze zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Nařízení a ostatní legislativy týkající se ochrany osobních údajů a této Směrnice a aby byla zajištěna ochrana práv subjektu údajů.

#### 4. Doba zpracování osobních údajů

- 4.1. Osobní údaje uchovávány po dobu nezbytně nutnou k zajištění práv a povinností plynoucích ze závazkového vztahu, z příslušné legislativy, či oprávněného zájmu správce, nebo dle uděleného souhlasu.
- 4.2. Není-li v ostatních vnitřních předpisech správce uvedeno jinak, či nevyplývá-li jinak z příslušné legislativy, rozumí se dobou zpracování osobních údajů v souladu s oprávněným zájmem správce doba pěti let od okamžiku vzniku právního důvodu pro zpracování osobních údajů.

- 4.3. Není-li v ostatních vnitřních předpisech správce uvedeno jinak, či nevyplývá-li jinak z příslušné legislativy, správce omezí zpracování osobních údajů, jakmile tak v souladu s právním důvodem zpracování bude moci učinit a po uplynutí doby zpracování osobních údajů tyto řádně a bezpečně zlikviduje.

## 5. Rozsah zpracování osobních údajů

- 5.1. Osobní údaje jsou zpracovány v rozsahu, v jakém je příslušný subjekt údajů příslušnému správci poskytl, a to v souvislosti s udělením souhlasu se zpracováním osobních údajů, uzavřením smluvního či jiného právního vztahu se správcem, nebo které správce shromáždil jinak a zpracovává je v souladu s platnou legislativou či k plnění zákonných povinností správce.

## 6. Kategorie osobních údajů, které jsou předmětem zpracování

- 6.1. Není-li v ostatních vnitřních předpisech správce, uvedeno jinak, zpracovává správce tyto kategorie osobních údajů:
- a. **adresní a identifikační údaje sloužící k jednoznačné a nezaměnitelné identifikaci subjektu údajů** (jméno, příjmení, titul, rodné číslo, datum narození, adresa trvalého pobytu, IČO, DIČ) a údaje umožňující kontakt se subjektem údajů (kontaktní údaje – např. kontaktní adresa, číslo telefonu, číslo faxu, e-mailová adresa – firemní i osobní, kontakty na osoby blízké v případě naléhavé potřeby - emergency a jiné obdobné informace);
  - b. **jiné popisné údaje** (např. bankovní spojení, údaje o příjmech u správce, zápočtový list s údaji od předchozích zaměstnavatelů, údaje o rodinných příslušnících pro účely daňové a sociální);
  - c. **další údaje nezbytné pro plnění smlouvy**, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
  - d. **ostatní osobní údaje v rámci uděleného souhlasu** ze strany subjektu údajů (zpracování fotografií pro marketingové účely, použití osobních údajů za účelem výběrového řízení – CV včetně údajů získaných při pohovoru atd.);
  - e. v souladu s ostatními vnitřními předpisy správce, zejména pracovněprávními, existují-li, může správce zpracovávat údaje, mající i povahu údajů osobních údajů, vztahující se primárně ke konkrétní osobě, svěřenému pracovnímu prostředku či jinému hmotnému majetku správce; o rozsahu, účelu a ostatních podmínkách zpracování takových údajů je osoba, která je či může být jejich subjektem, vždy předem seznámena. Výpisy z Rejstříku trestů se požadují pouze u osob, které nakládají s finančními prostředky a nearchivují se.

## 7. Práva subjektů údajů

- 7.1. V souladu s čl. 12 a násl. Nařízení je subjekt osobních údajů informován o právu na přístup k osobním údajům a k následujícím informacím:
- a. **totožnost** a kontaktní údaje správce a jeho případného zástupce či případného pověřence pro ochranu osobních údajů;
  - b. **účelu** a právnímu základu zpracování osobních údajů;
  - c. **kategorii** dotčených osobních údajů;

- d. o **příjemci** nebo kategorii příjemců, kterým osobní údaje byly nebo budou zpřístupněny;
- e. předpokládané **době**, po kterou budou osobní údaje uloženy či jinak zpracovávány;
- f. veškeré dostupné informace o **zdroji** osobních údajů, pokud nejsou získány od subjektu údajů;
- g. skutečnosti, zda dochází k **automatizovanému** rozhodování, včetně profilování, za splnění příslušných požadavků Nařízení;
- h. existenci práva:
  - požadovat od správce **přístup** k osobním údajům;
  - na **opravu** nebo **výmaz**, popřípadě omezení zpracování osobních údajů;
  - vznést **námítku** proti zpracování,
  - na **přenositelnost** údajů za podmínek stanovených Nařízením;
  - na **odvolání** souhlasu se zpracováním osobních údajů, byl-li udělen;
  - **nebýt předmětem** automatizovaného rozhodnutí vč. profilování.
- i. dalších právech ve smyslu této Směrnice.

- 7.2. Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo jím pověřený zpracovatel, provádí takové zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu s Nařízením, Zákonem či ostatní platnou legislativou týkající se ochrany osobních údajů a touto Směrnicí, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může:
- a. požádat správce o **vysvětlení**;
  - b. požadovat, aby správce **odstranil** takto vzniklý stav. Zejména se může jednat o omezení zpracování, provedení opravy, doplnění nebo vymazání osobních údajů.
- 7.3. Nestanoví-li Nařízení či ostatní platná legislativa týkající se ochrany osobních údajů jinak, správce, či jím pověřená osoba, na žádost subjektu údajů podle odstavce 7.2. této Směrnice odstraní neprodleně závadný stav v souladu s Nařízením, či ostatní platnou legislativou týkající se ochrany osobních údajů.
- 7.4. Správce oznamuje jednotlivým příjemcům, jimž byly osobní údaje případně zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje.
- 7.5. Nevyhoví-li správce žádosti subjektu údajů podle odstavce 7.2. této Směrnice, má subjekt údajů právo obrátit se přímo na dozorový úřad, tedy Úřad na ochranu osobních údajů.
- 7.6. Postup podle odstavce 7.2. této Směrnice nevyklučuje, aby se subjekt údajů obrátil se svým podnětem či stížností na dozorový úřad, tedy na Úřad pro ochranu osobních údajů, adresou Pplk. Sochora 727/27, 170 00 Praha 7-Holešovice, přímo.

## 8. Kontaktní údaje na správce

**Cattacan, s.r.o.**

Email: cattacan.sro@gmail.com

Telefon: 777 860 787

odpovědná osoba: Stanislava Findejsová

Nabytí účinnosti dne: 25.5.2018

za správce: Stanislava Findejsová, jednatelka společnosti

podpis:

A handwritten signature in black ink, appearing to read 'S. Findejsová', written in a cursive style.