

# **Interní směrnice o ochraně a zpracování osobních údajů**

# Obsah

1. Základní pojmy
2. Mapování osobních údajů
3. Zásady zpracování osobních údajů (článek 5 GDPR)
4. Podmínky poskytnutí souhlasu se zpracováním osobních údajů (článek 7 GDPR)
5. Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti (článek 8 GDPR)
6. Zpracovávání zvláštních kategorií osobních údajů (článek 9 GDPR)
7. Práva dotčené osoby (kapitola 3 GDPR)
8. Odpovědnost provozovatele (článek 24 GDPR)
9. Specificky navržena a standardní ochrana osobních údajů (článek 25 GDPR)
10. Zprostředkovatel (článek 28 GDPR)
11. Záznamy o zpracovatelských činnostech (článek 30 GDPR)
12. Bezpečnost zpracovávání (článek 32 GDPR)
13. Oznámení porušení ochrany osobních údajů kontrolnímu orgánu (článek 33 a 34 GDPR)
14. Posouzení dopadů na ochranu údajů (článek 35)
15. Určení odpovědné osoby (kapitola 4 oddíl 4 GDPR)
16. Předávání osobních údajů do třetí země nebo mezinárodní organizace
17. Mlčenlivost

Podle nařízení Evropského parlamentu a rady (EU) 2016/679, ze dne 27. dubna 2016 ochraně fyzických osob při zpracování osobních údajů a volném pohybu takovýchto údajů (dále jen GDPR)

Obsahuje technická a organizační opatření, které se naše společnost zavázala dodržovat, jelikož je podle článku 24 GDPR s ohledem na povahu, rozsah, kontext a účely zpracování, jakož i na rizika s různou pravděpodobností a závažností pro práva a svobody fyzických osob odpovědná, aby zajistila a byla schopna prokázat, že zpracování se provádí v souladu s nařízením GDPR.

název společnosti: CK SBV s.r.o.

adresa: Sokolská, 271

město: 47001 Česká Lípa

stat: Česká Republika

IČ: 25039938

DIČ: CZ25039938

Zapsána v : zapsaná v OR vedeného MěS Praha, oddíl C ,vložka 218430

**Dozorčí orgán:**

Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, PSČ 170 00, Praha 7  
se sídlem Pplk. Sochora 27, PSČ 170 00, Praha 7

[www.uoou.cz](http://www.uoou.cz)

(dále jen „dozorčí orgán“)

# 1. Základní pojmy

**dotčenou osobou** každá fyzická osoba, jejíž osobní údaje se zpracovávají,

**provozovatelem** každý, kdo sám nebo společně s jinými vymezí účel a prostředky zpracování osobních údajů a zpracovává osobní údaje vlastním jménem; provozovatel nebo konkrétní požadavky na jeho určení mohou být stanoveny ve zvláštním předpise nebo mezinárodní smlouvě, kterou je Česká republika vázána, pokud takový předpis nebo tato smlouva stanoví účel a prostředky zpracování osobních údajů,

**zprostředkovatelem** každý, kdo zpracovává osobní údaje pro správce,

**zpracováním osobních údajů** zušlechťovací operace nebo soubor zpracovatelských operací s osobními údaji nebo se soubory osobních údajů, zejména získávání, zaznamenávání, uspořádávání, strukturování, uchovávání, změna, vyhledávání, nahlížení, používání, poskytování přenosem, šířením nebo jiným způsobem, přeskupování nebo kombinování, omezení, vymazání, bez ohledu na to, zda se provádí automatizovanými prostředky nebo neautomatizovanými prostředky,

**souhlasem dotyčné osoby** jakýkoliv vážný a svobodný, konkrétní, informovaný a jednoznačný projev vůle dotčené osoby ve formě prohlášení nebo jednoznačného potvrzujícího úkonu, kterým dotyčná osoba vyjadřuje souhlas se zpracováním svých osobních údajů

**informačním systémem** jakýkoliv uspořádaný soubor osobních údajů, které jsou přístupné podle určených kritérií, bez ohledu na to, zda jde o systém centralizovaný, decentralizovaný nebo distribuován na funkčním základě nebo geografickém základě,

**biometrickými údaji** osobní údaje, které jsou výsledkem zvláštního technického zpracování osobních údajů týkajících se fyzických charakteristických znaků fyzické osoby, fyziologických charakteristických znaků fyzické osoby nebo behaviorálních charakteristických znaků fyzické osoby a které umožňují jedinečnou identifikaci nebo potvrzují jedinečnou identifikaci této fyzické osoby, jako zejména vyobrazení obličeje nebo daktyloskopické údaje,

**omezením zpracování osobních údajů** označení uložených osobních údajů za účelem omezit jejich budoucí zpracování,

**profilováním** jakákoliv forma automatizovaného zpracování osobních údajů spočívajícího v použití osobních údajů k vyhodnocení určitých osobních znaků nebo charakteristik týkajících se fyzické osoby, zejména na analýzu nebo předvídání znaků nebo vlastností dotčené osoby spojených s jejím výkoností v práci, majetkovými poměry, zdravím, osobními preferencemi, zájmy, spolehlivostí, chováním, polohou nebo pohybem,

**pseudonymizací** zpracovávání osobních údajů způsobem, že je nelze přiřadit ke konkrétní dotčené osobě bez použití dodatečných informací, pokud se takové dodatečné informace uchovávají odděleně a vztahují se na ně technická a organizační opatření k zajištění toho, aby osobní údaje nebylo možné přiřadit identifikované fyzické osobě nebo identifikovatelné fyzické osobě,

**šifrováním** transformace osobních údajů způsobem, kterým opětovné zpracování je možné pouze po zadání zvoleného parametru, jako je klíč nebo heslo,

**online identifikátorem** identifikátor poskytnutý aplikací, nástrojem nebo protokolem, zejména IP adresa, cookies, přihlašovací údaje do online služeb, radiofrekvenční identifikace, které mohou zanechávat stopy, které se zejména v kombinaci s jedinečnými identifikátory nebo jinými informacemi mohou použít pro vytvoření profilu dotčené osoby a na její identifikaci,

**porušením ochrany osobních údajů** porušení bezpečnosti, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo k neoprávněnému poskytnutí přenášených, uchovávaných osobních údajů nebo jinak zpracovávaných osobních údajů nebo k neoprávněnému přístupu k nim,

**příjemcem** každý, komu se osobní údaje poskytnou bez ohledu na to, zda je třetí stranou; za příjemce se nepovažuje orgán veřejné moci, který zpracovává osobní údaje na základě zvláštního předpisu nebo mezinárodní smlouvy, kterou je Česká republika vázána, v souladu s pravidly ochrany osobních údajů vztahujícími se na daný účel zpracování osobních údajů,

**třetí stranou** každý, kdo není dotčenou osobou, provozovatel, zprostředkovatel nebo jinou fyzickou osobou, která na základě pověření správce nebo zpracovatele zpracovává osobní údaje,

## 2. Mapování osobních údajů

Naše společnost se v tomto kroku rozhodla definovat, jaké osobní údaje zpracovává, aby byla schopna zanalyzovat zpracování osobních údajů a zajistit soulad s GDPR.

Jednotlivé kategorie osobních údajů si nadefinujeme jako jednotlivé informační systémy (IS).

### **IS Zákazníci**

jméno, příjmení, titul, ulice a číslo, PSČ, město, email, telefonní kontakt, přihlašovací jméno, heslo, údaje k reklamaci

účel zpracování: vystavení daňového dokladu, smluvní a předmluvní vztahy, reklamace.  
datum narození

### **IS Marketing**

Emailové adresy, telefonické kontakty

Účel zpracování: zasílání marketingových a reklamních emailů.

## **3. Zásady zpracování osobních údajů (článek 5 GDPR)**

Naše společnost bude dodržovat následující zásady zpracování osobních údajů:

### **3.1 Zákonnost, spravedlnost a transparentnost (článek 5 odst.1 písm. A) GDPR)**

Osobní údaje budou zpracovávány zákonným způsobem, spravedlivě a transparentně ve vztahu k dotčené osobě („zákonnost, spravedlnost a transparentnost“);

#### **3.1.1 Zákonnost zpracovávání (článek 6 GDPR)**

Naše společnost se zavázala zpracovávat údaje pouze zákonným způsobem tak, aby nedošlo k porušení základních práv dotčené osoby.

Zpracování osobních údajů naší společností bude zákonné a to zajištěním, že se provádí na základě alespoň jednoho z těchto právních základů:

- a) dotčená osoba vyjádřila souhlas se zpracováním svých osobních údajů na jeden nebo více konkrétní účely
- b) zpracování je nezbytné pro plnění smlouvy, jejíž stranou je dotčená osoba, nebo aby se na základě žádosti dotčené osoby provedly opatření před uzavřením smlouvy
- c) zpracování osobních údajů je nezbytné podle zvláštního předpisu nebo mezinárodní smlouvy, kterou je Česká republika vázána
- d) zpracování je nezbytné, aby se ochránili životně důležité zájmy subjektu údajů nebo jiné fyzické osoby
- e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci svěřené provozovateli
- f) zpracování je nezbytné pro účely oprávněných zájmů, které sleduje provozovatel nebo třetí strana, s výjimkou případů, kdy nad takovými zájmy převažují zájmy nebo základní práva a svobody subjektu údajů, které vyžadují ochranu osobních údajů, zejména pokud je dotčenou osobu dítě.

Právní základy pro jednotlivé účely zpracování osobních údajů jsou definovány v záznamech o zpracovatelských činnostech.

### **3.2 Zásada omezení účelu (článek 5 odst.1 písm. B) GDPR)**

Naše společnost bude získávat osobní údaje pouze na konkrétní určené, výslovně uvedené a legitimní účely a nesmějí být dále zpracovávány způsobem, který není slučitelný s těmito účely. Naše společnost informuje dotčenou osobu o účelu zpracování osobních údajů před jejich zpracováním.

V části mapování osobních údajů jsme si stanovili účely zpracování jednotlivých IS a osobní údaje budeme zpracovávat pouze pro účely uvedené v této části.

### **3.3 Zásada minimalizace osobních údajů (článek 5 odst.1 písm. C) GDPR)**

Naše společnost bude zpracovávat osobní údaje tak, aby toto zpracování přiměřené, relevantní a omezené na nezbytný rozsah daný účelem, na který se zpracovávají.

S cílem zajistit minimalizaci osobních údajů se naše společnost rozhodla zanalyzovat, zda jsou spracovávané údaje přiměřené, relevantní a omezené na rozsah, který je nezbytný vzhledem k účelům, pro které se zpracovávají.

Výsledky analýzy minimalizace údajů jsou uvedeny v záznamech o zpracovatelských činnostech.

### **3.4 Zásada správnosti (článek 5 odst.1 písm. D) GDPR)**

Naše společnost bude zpracovávat osobní údaje tak, aby byly správně a podle potřeby aktualizována; a přijme vhodná a účinná opatření k zajištění toho, aby osobní údaje, které jsou nesprávné z hlediska účelů, pro které se zpracovávají, bez zbytečného odkladu vymazali nebo opravili.

K zajištění zásady správnosti má naše společnost v písemném souhlasu se zpracováním osobních údajů následující formulaci:

Dotyčná osoba je povinna poskytnout pravdivé a aktuální osobní údaje. V případě změny osobních údajů je dotyčná osoba povinna změnu neprodleně oznámit provozovateli.

### **3.5 Zásada minimalizace uchování (článek 5 odst.1 písm. E) GDPR)**

Osobní údaje bude naše společnost uchovávat ve formě, která umožňuje identifikaci dotyčné osoby nejpozději, dokud je to nutné pro účel, pro který jsou osobní údaje zpracovávány.



### **3.6 Zásada integrity a důvěrnosti (článek 5 odst.1 písm. F) GDPR)**

Osobní údaje budou v naší společnosti zpracovávány způsobem, který zaručuje dostatečnou bezpečnost osobních údajů včetně ochrany před neoprávněným zpracováním osobních údajů, nezákonným zpracováním osobních údajů, náhodnou ztrátou osobních údajů, výmazem osobních údajů nebo poškozením osobních údajů a to prostřednictvím odpovídajících technických nebo organizačních opatření.

#### **3.6.1 Osobní údaje uložené v elektronické podobě**

#### **3.6.2 Osobní údaje uložené v papírové (vytištěné) podobě**

### **3.7 Zásada odpovědnosti (článek 5 odst. 2 GDPR)**

Naše společnost je odpovědná za dodržování základních zásad zpracování osobních údajů, za soulad zpracování osobních údajů se zásadami zpracování osobních údajů a je povinna tento soulad se zásadami zpracování osobních údajů na požádání úřadu prokázat.

## **4. Podmínky poskytnutí souhlasu se zpracováním osobních údajů (článek 7 GDPR)**

Společnost zajistí splnění následujících podmínek při vyjádření souhlasu dotčenou osobou

- a) souhlas odvolat se zpracováním osobních údajů musí být vyjádřen svobodně, konkrétně, informovaně a jednoznačným projevem vůle.
- b) žádost o vyjádření souhlasu musí být předložena tak, aby byla jasně odlišitelná od těchto jiných skutečností, ve srozumitelné a snadno dostupné formě a formulována jasně a jednoduše.
- c) dotyčná osoba má právo kdykoliv svůj souhlas. Odvolání souhlasu nemá vliv na zákonnost zpracovávání vycházejícího ze souhlasu před jeho odvoláním. Před poskytnutím souhlasu musí být dotčená osoba o této skutečnosti informována. Odvolání souhlasu musí být tak jednoduché jako jeho poskytnutí.

## **5. Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti (článek 8 GDPR)**

Pokud se použije čl 6 odst. 1 písm. a), v souvislosti s nabídkou služeb informační společnosti adresovanou přímo dítěti je zpracovávání osobních údajů dítěte zákonné, pouze pokud má dítě alespoň 16 let. Pokud má dítě méně než 16 let, takové zpracovávání je zákonné pouze za podmínky a v rozsahu, v jakém takový souhlas vyjádřil nebo schválil nositel rodičovské zodpovědnosti.

Naše společnost vynaloží přiměřené úsilí, aby si v takových případech ověřila, že nositel rodičovské zodpovědnosti vyjádřil souhlas nebo jej schválil, přičemž zohlední dostupnou technologii.

## 6. Zpracovávání zvláštních kategorií osobních údajů (článek 9 GDPR)

Podle GDPR se zakazuje zpracovávání osobních údajů, které odhalují rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení nebo členství v odborech, a zpracovávání genetických údajů, biometrických údajů pro individuální identifikaci fyzické osoby, údajů týkajících se zdraví nebo údajů týkajících se sexuálního života nebo sexuální orientace fyzické osoby.

Tento zákaz se však nepoužije, pokud platí některá z podmínek článku 9 odst. 2 GDPR písm. a) - j)

- a) dotyčná osoba vyjádřila výslovný souhlas se zpracováním těchto osobních údajů na jeden nebo více určených účelů s výjimkou případů, kdy se v právu Unie nebo v právu členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže dotčená osoba zrušit;
- b) zpracování je nezbytné pro účely plnění povinností a výkonu zvláštních práv provozovatele nebo dotčené osoby v oblasti pracovního práva a práva sociálního zabezpečení a sociální ochrany

## 7. Práva dotčené osoby (kapitola 3 GDPR)

Práva dotčené osoby jsou upraveny kapitolou 3 GDPR a naše společnost se zavazuje je dodržovat.

Jde například o následující práva:

### 7.1 Informace, které mají být poskytnuty při získávání osobních údajů od dotčené osoby (článek 13 GDPR)

Naše společnost poskytne dotčené osobě při zpracovávání osobních údajů následující informace:

- a) údaje o naší společnosti
- b) kontaktní údaje případné odpovědné osoby;
- c) účely zpracování
- d) právní základ zpracování
- e) jestliže se zpracování zakládá na článku 6 odst. 1 písm. f) GDPR, oprávněné zájmy, které sleduje provozovatel nebo třetí strana;
- f) příjemci nebo kategorie příjemců osobních údajů, pokud existují;
- g) v relevantním případě informace o tom, že naše společnost zamýšlí přenést osobní údaje do třetí země nebo mezinárodní organizaci
- h) doba uchovávání osobních údajů nebo, pokud to není možné, kritéria pro její určení;
- i) existence práva požadovat od provozovatele přístup k osobním údajům týkajícím se dotčené osoby a práva na jejich opravu nebo vymazání nebo omezení zpracování, nebo práva namítat proti zpracování, jakož i práva na přenositelnost údajů;
- j) pokud je zpracování založeno na článku 6 odst. 1 písm. a) nebo na článku 9 odst. 2 písm. a) GDPR, existence práva kdykoli svůj souhlas odvolat, aniž by to mělo vliv na zákonnost zpracování založeného na souhlasu uděleném před jeho odvoláním;
- k) právo podat stížnost orgánu dozoru;
- l) informace o tom, zda je poskytování osobních údajů zákonnou nebo smluvní požadavkem nebo požadavkem, která je potřebná na uzavření smlouvy, zda je dotyčná osoba povinna poskytnout osobní údaje, jakož i možné následky neposkytnutí těchto údajů;
- m) existence automatizovaného rozhodování včetně profilování uvedeného v článku 22 odst. 1 a 4 GDPR a alespoň v těchto případech smysluplné informace o použitém postupu, jakož i významu a předpokládaných důsledcích takového zpracovávání pro dotčenou osobu.

## **7.2 Informace, které mají být poskytnuty, pokud osobní údaje nebyly získány od subjektu údajů (článek 14 GDPR)**

Naše společnost poskytne dotčené osobě, pokud tyto osobní údaje nebyly získány od ní, všechny informace uvedené v bodě 7.1 této organizační směrnice a také z jakého zdroje pocházejí osobní údaje, případně informace o tom, zda údaje pocházejí z veřejně přístupných zdrojů.

Tyto informace poskytne naše společnost dotčené osobě v přiměřené lhůtě po získání osobních údajů, nejpozději však do jednoho měsíce, přičemž zohlední konkrétní okolnosti, za kterých se osobní údaje zpracovávají podle článku 14 odst. 3 GDPR

Naše společnost neposkytne subjektu údajů tyto informace v případech uvedených v článku 14 odst. 5 GDPR, zvláště pokud:

- a) dotčená osoba má již dané informace
- b) se poskytování těchto informací ukáže jako nemožné nebo by vyžadovalo nepřiměřené úsilí
- c) se získání nebo poskytnutí výslovně stanoví v právu Unie nebo v právu členského státu, kterému provozovatel podléhá, a který stanoví vhodná opatření na ochranu oprávněných zájmů subjektu údajů

## **7.3 Právo dotčené osoby na přístup k údajům (článek 15 GDPR)**

Subjekt údajů má právo získat od správce potvrzení o tom, zda se zpracovávají osobní údaje, které se jí týkají, a pokud tomu tak je, má právo získat přístup k těmto osobním údajům

## **7.4 Právo na opravu (článek 16 GDPR)**

Dotčená osoba má právo na to, aby provozovatel bez zbytečného odkladu opravil nesprávné osobní údaje, které se jí týkají. S ohledem na účely zpracování má dotčená osoba právo na doplnění neúplných osobních údajů, a to i prostřednictvím poskytnutí doplňkového vyhlášení.

## **7.5 Právo na vymazání (právo „na zapomení“, článek 17 GDPR)**

Dotyčná osoba má také právo dosáhnout u provozovatele bez zbytečného odkladu vymazání osobních údajů, které se jí týkají, a provozovatel je povinen bez zbytečného odkladu vymazat osobní údaje, pokud je splněn některý z těchto důvodů:

- a) osobní údaje již nejsou potřebné pro účely, pro které se získávaly nebo jinak zpracovány;
- b) dotyčná osoba odvolá souhlas, na jehož základě se zpracovávání provádí podle článku 6 odst. 1 písm. a) nebo článku 9 odst. 2 písm. a), a pokud neexistuje jiný právní základ pro zpracovávání;
- c) subjekt údajů odmítá zpracování podle článku 21 odst. 1 a nepřevažují žádné oprávněné důvody pro zpracování nebo subjekt údajů odmítá zpracování podle článku 21 odst. 2;
- d) osobní údaje jsou zpracovány nezákonně;
- e) osobní údaje musí být vymazány, aby se splnila zákonná povinnost podle práva Unie nebo práva členského státu, kterému provozovatel podléhá;
- f) osobní údaje se získávaly v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1.

## **7.6 Právo na omezení zpracování (článek 18 GDPR)**

Dotyčná osoba má právo na to, aby provozovatel omezil zpracování, pokud jde o jeden z těchto případů:

- a) dotyčná osoba napadne správnost osobních údajů, a to během období umožňujícího provozovateli ověřit správnost osobních údajů;
- b) zpracování je protizákonné a dotyčná osoba zpochybňuje výmaz osobních údajů a žádá místo toho omezení jejich použití;
- c) provozovatel již nepotřebuje osobní údaje pro účely zpracování, ale potřebuje je dotyčná osoba na prokázání, uplatňování nebo obhajování právních nároků;
- d) dotyčná osoba zpochybnila zpracování podle článku 21 odst. 1, a to až do ověření, zda oprávněné důvody na straně provozovatele převažují nad oprávněnými důvody dotyčné osoby.

Oznamovací povinnost v souvislosti s opravou nebo vymazáním osobních údajů nebo omezením zpracování (článek 19 GDPR)

Provozovatel oznámí každému příjemci, kterému byly osobní údaje poskytnuté, každou opravu nebo vymazání osobních údajů nebo omezení zpracování provedené podle článku 16, článku 17 odst. 1 a článku 18, pokud se to neukáže jako nemožné nebo to nevyžaduje nepřiměřené úsilí. Provozovatel o těchto příjemcích informuje dotyčnou osobu, pokud to dotyčná osoba požaduje.

## **7.7 Právo na přenositelnost údajů (článek 20 GDPR)**

Subjekt údajů má právo získat osobní údaje, které se jí týkají a které poskytla provozovateli, ve strukturovaném, běžně používaném a strojově čitelném formátu a má právo přenést tyto údaje dalšímu provozovateli, aniž její provozovatel, kterému se tyto osobní údaje poskytli, brání, pokud:

a) a zpracování zakládá na souhlasu podle článku 6 odst. 1 písm. a) nebo článku 9 odst. 2 písm. a) nebo na smlouvě podle článku 6 odst. 1 písm. b), a  
b) jestliže se zpracování provádí automatizovanými prostředky.

Dotyčná osoba má při uplatňování svého práva na přenositelnost údajů podle odstavce 1 právo na předávání osobních údajů přímo od jednoho provozovatele druhému provozovateli, pokud je to technicky možné.

## **7.8 Právo namítat (článek 21 GDPR)**

Dotyčná osoba má právo kdykoliv namítat z důvodů týkajících se její konkrétní situace proti zpracování osobních údajů, které se jí týká, které je prováděno na základě článku 6 odst. 1 písm. e) nebo f) včetně namítat proti profilování založenému na uvedených ustanoveních.

## **7.9 Automatizované individuální rozhodování včetně profilování (článek 22 GDPR)**

Dotyčná osoba má právo na to, aby se na ni nevztahovalo rozhodnutí, které je založeno výlučně na automatizovaném zpracování, včetně profilování, a které má právní účinky, které se jí týkají nebo ji podobně významně ovlivňují.



## **8. Odpovědnost provozovatele (článek 24 GDPR)**

Naše společnost se jako provozovatel zavazuje dodržovat následující obecné povinnosti:

- a) S ohledem na povahu, rozsah a účel zpracování osobních údajů a na rizika s různou pravděpodobností a závažností pro práva fyzické osoby se zavazujeme přijmout vhodná technická a organizační opatření k zajištění a prokázání toho, že zpracování osobních údajů se provádí v souladu s GDPR.
- b) Uvedená opatření budeme podle potřeby aktualizována.
- c) Budeme pravidelně prověřovat trvání účelu zpracování osobních údajů a po jeho splnění bez zbytečného odkladu zajistit výmaz osobních údajů.
- d) Naše společnost bude zachovávat mlčenlivost o osobních údajích, které zpracovává. Povinnost mlčenlivosti trvá i po ukončení zpracování osobních údajů.

## **9. Specificky navržená a standardní ochrana osobních údajů (článek 25 GDPR)**

Naše společnost se zavazuje před zpracováním osobních údajů zavést a během zpracovávání osobních údajů mít zavedenou specificky navrženou ochranu osobních údajů, která spočívá v přijetí vhodných technických a organizačních opatření, například i ve formě pseudonymizace, na účinné zavedení přiměřených záruk ochrany osobních údajů a dodržování nařízení GDPR .

Naše společnost se zavazuje při specificky navržené ochraně osobních údajů zohlednit nejnovější poznatky ochrany osobních údajů, náklady na provedení opatření, povahu, rozsah, kontext a účel zpracování osobních údajů a rizika zpracování osobních údajů s různou pravděpodobností a závažností, které zpracování osobních údajů představuje pro práva dotčené osoby.

Naše společnost se zavazuje zavést standardní ochranu osobních údajů, která spočívá v přijetí vhodných technických a organizačních opatření k zajištění zpracování osobních údajů pouze pro konkrétní účel, minimalizace množství získaných osobních údajů a rozsahu jejich zpracování, doby uchovávání a dostupnosti osobních údajů. Naše společnost zajistí, aby osobní údaje nebyly bez zásahu fyzické osoby standardně přístupné neomezenému počtu fyzických osob.

## 10. Zprostředkovatel (článek 28 GDPR)

Zprostředkovatel je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje jménem provozovatele.

Naše společnost jako provozovatel využívá zprostředkovatelů, kteří jejím jménem zpracovávají osobní údaje. Jde například o účetní a právnické společnosti. Pro naši společnost zpracovávají údaje zprostředkovatelé uvedený v příloze Zprostředkovatelé. Naše společnost bude využívat jen zprostředkovatelů poskytujících dostatečné záruky na to, že se přijmou vhodná technická a organizační opatření, aby zpracování splňovalo požadavky GDPR a aby byla zajištěna ochrana práv dotčené osoby.

Zpracovávání zprostředkovatelem pro naši společnost se řídí „smlouvou o zpracování osobních údajů“, jejíž vzor je přílohou tohoto dokumentu. Zavazuje zprostředkovatele vůči provozovateli a stanoví se jí předmět a doba zpracování, povaha a účel zpracování, typ osobních údajů a kategorie dotčených osob a povinnosti a práva provozovatele a zprostředkovatele.

Naše společnost podepíše dodatky ke smlouvám se zmíněnými zprostředkovateli, aby smlouvy splňovaly všechny náležitosti GDPR.

## 11. Záznamy o zpracovatelských činnostech (článek 30 GDPR)

### 11.1 Záznamy o zpracovatelských činnostech provozovatele

Naše společnost jako provozovatel vede záznamy o zpracovatelských činnostech a na požádání je zpřístupní dohlížitele. Tyto záznamy obsahují následující údaje:

- a) jméno / název a kontaktní údaje provozovatele a v příslušném případě společného provozovatele, zástupce provozovatele a odpovědné osoby;
- b) účely zpracování;
- c) popis kategorií dotčených osob a kategorií osobních údajů;
- d) kategorie příjemců, kterým byly nebo budou osobní údaje poskytnuté včetně příjemců v třetích zemích nebo mezinárodních organizací;
- e) případně přenosy osobních údajů do třetí země nebo mezinárodní organizaci včetně označení předmětné třetí země nebo mezinárodní organizace a v případě přenosů uvedených v článku 49 odst. 1 druhém pododstavci GDPR dokumentaci přiměřených záruk;
- f) podle možností předpokládané lhůty pro vymazání různých kategorií údajů;
- g) podle možností obecný popis technických a organizačních bezpečnostních opatření uvedených v článku 32 odst. 1. GDPR

## 11.2 Záznamy o zpracovatelských činnostech zprostředkovatele

Naše společnost jako zprostředkovatel vede záznamy o zpracovatelských činnostech a na požádání je zpřístupní dohlížitele. Tyto záznamy obsahují následující údaje:

- a) jméno / název a kontaktní údaje zprostředkovatele nebo zprostředkovatelů a každého provozovatele, jehož jménem zprostředkovatel jedná, a v příslušném případě zástupce správce nebo zpracovatele a odpovědné osoby;
- b) kategorie zpracování prováděného jménem každého provozovatele;
- c) v příslušných případech předávání osobních údajů do třetí země nebo mezinárodní organizaci včetně označení předmětné třetí země nebo mezinárodní organizace a v případě přenosů uvedených v článku 49 odst. 1 druhém pododstavci dokumentaci přiměřených záruk;
- d) podle možností obecný popis technických a organizačních bezpečnostních opatření uvedených v článku 32 odst. 1. GDPR

## 12. Bezpečnost zpracování (článek 32 GDPR)

Naše společnost přijme s ohledem na nejnovější poznatky, náklady na provedení opatření a na povahu, rozsah, kontext a účely zpracování, jakož i na rizika s různou pravděpodobností a závažností pro práva a svobody fyzických osob, vhodná technická a organizační opatření s cílem zajistit úroveň bezpečnosti přiměřenou tomuto riziku.

### **Pověření zpracovávat osobní údaje (článek 32 odst. 4 GDPR)**

Naše společnost podnikne kroky k zajištění toho, aby každá fyzická osoba jednající na základě pověření správce nebo zpracovatele, která má přístup k osobním údajům, zpracovávala tyto údaje pouze na základě našich pokynů s výjimkou případů, kdy se to od ní vyžaduje podle práva Unie nebo práva členského státu.

## **13. Oznámení porušení ochrany osobních údajů kontrolnímu orgánu (článek 33 a 34 GDPR)**

V případě porušení ochrany osobních údajů naše společnost bez zbytečného odkladu a nejlépe do 72 hodin poté, co se o této skutečnosti dozvěděla, oznámí porušení ochrany osobních údajů kontrolnímu orgánu.

Pokud oznámení nebylo kontrolnímu orgánu předloženo do 72 hodin, připojí se k němu zdůvodnění prodlení.

Oznámení o porušení ochrany osobních údajů bude obsahovat alespoň:

- a) popis povahy porušení ochrany osobních údajů, včetně, podle možnosti, kategorií a přibližného počtu dotčených osob, kterých se porušení týká a kategorií a přibližného počtu dotčených záznamů o osobních údajích;
- b) kontaktní údaje odpovědné osoby v naší společnosti, kde lze získat více informací o porušení ochrany osobních údajů;
- c) popis pravděpodobných následků porušení ochrany osobních údajů;
- d) popis opatření přijatých nebo navrhovaných provozovatelem s cílem napravit porušení ochrany osobních údajů, včetně, podle potřeby, opatření ke zmírnění možných negativních důsledků.

Naše společnost zdokumentuje každý případ porušení ochrany osobních údajů, včetně skutečností spojených s porušením ochrany osobních údajů, jeho následky a přijatá opatření k nápravě.

V případě porušení ochrany osobních údajů, které pravděpodobně povede k vysokému riziku pro práva a svobody fyzických osob, naše společnost bez zbytečného odkladu oznámí porušení ochrany osobních údajů dotčené osobě.

## **14. Posouzení vlivu na ochranu údajů (článek 35)**

Pokud typ zpracování, zejména s využitím nových technologií a s ohledem na povahu, rozsah, kontext a účely zpracování pravděpodobně povede k vysokému riziku pro práva a svobody fyzických osob, provozovatel před zpracováním provede posouzení dopadů plánovaných zpracovatelských operací na ochranu osobních údajů.

Posouzení dopadů na ochranu údajů vyžaduje zejména v případech:

- a) systematického a rozsáhlého hodnocení osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování včetně profilování a ze kterého vycházejí rozhodnutí s právními účinky týkajícími se fyzické osoby nebo s podobně závažným vlivem na ni;
  - b) zpracování ve velkém rozsahu zvláštních kategorií údajů podle článku 9 odst. 1 nebo osobních údajů o uznání viny za trestné činy a přestupky podle článku 10, nebo
  - c) systematické ho monitorování veřejně přístupných míst ve velkém rozsahu.
- Zpracovatelské činnosti naší společnosti nezahrnují případy uvedené výše, z tohoto důvodu není nutné provést posouzení dopadů na ochranu osobních údajů.

## **15. Určení odpovědné osoby (kapitola 4 oddíl 4 GDPR)**

Provozovatel je povinen určit pověřence pro ochranu osobních údajů, pokud

- a) zpracování osobních údajů provádí orgán veřejné moci nebo veřejnoprávní instituce kromě soudů při výkonu jejich pravomoci,
- b) hlavními činnostmi správce nebo zpracovatele jsou zpracovatelské operace, které si vzhledem ke své povaze, rozsahu nebo účelu vyžadují pravidelné a systematické monitorování dotčené osoby ve velkém rozsahu nebo
- c) hlavními činnostmi správce nebo zpracovatele je zpracování zvláštních kategorií osobních údajů podle článku 9 GDPR ve velkém rozsahu nebo zpracování osobních údajů týkajících se uznání viny za spáchání trestného činu nebo přestupku podle článku 10 GDPR ve velkém rozsahu.

Jelikož naše společnost nesplňuje ani jednu z uvedených podmínek, pověřence pro ochranu osobních údajů neurčuje.

## **16. Předávání osobních údajů do třetí nebo mezinárodní organizace**

Předávání osobních údajů, které se zpracovávají nebo jsou určeny pro zpracování po přenosu do třetí země nebo mezinárodní organizace, se může uskutečnit pouze tehdy, pokud provozovatel a zprostředkovatel dodržují podmínky včetně podmínek následného předávání osobních údajů z předmětné třetí země nebo od předmětné mezinárodní organizace do jiné třetí země nebo jiné mezinárodní organizace.

Úřad pro ochranu osobních údajů zveřejňuje na svých stránkách seznam třetích zemí, území a určených sektorů v dané třetí zemi a mezinárodních organizací, u nichž Evropská komise rozhodla, že v nich je zaručena odpovídající úroveň ochrany nebo již přestala být přiměřená úroveň ochrany zaručená.

Seznam je dostupný na stránce

<https://www.uoou.cz/predavani-osobnich-udaju-do-zahranici/ds-1633/p1=1633&rd=1000>

Naše společnost bude tento seznam pravidelně sledovat a v případě, že by přenášela osobní údaje do zemí mimo seznam úřadu na ochranu osobních údajů, bude postupovat podle kapitoly 4 GDPR.

## **17. Mlčenlivost**

Naše společnost je povinna zachovávat mlčenlivost o osobních údajích, které zpracovává. Povinnost mlčenlivosti trvá i po ukončení zpracování osobních údajů.

Naše společnost je také povinna zavázat mlčenlivostí o osobních údajích fyzické osoby, které přijdou do styku s osobními údaji u provozovatele nebo zprostředkovatele.

Povinnost mlčenlivosti podle věty první musí trvat i po skončení pracovního poměru, státně zaměstnaneckého poměru služebního poměru nebo obdobného pracovního vztahu této fyzické osoby.