Příloha č. 1 – Registr rizik

ID	Odpovědná osoba	Popis	Scénář	Aktivum	Zranitelnost	Dopad	Výskyt	OHR	Významnost rizika	Dopad	Prevence
1	Právník	Riziko nepřipravenosti Zpracovatelů na GDPR	Námi vybraní zpracovatelé nejsou v souladu s GDPR (nebylo kontrolováno ani smluvně zajištěno)	Zodpovědnost Správce za vhodné zpracovatele	Nepřipravenost zpracovatelů, nehodnocení připravenosti zpracovatelů	4	2	8	Střední	Nenabytí souladu s GDPR, sankce od dozorového úřadu	Uzavření dodatků ke smlouvě o zpracování OÚ
2	Finanční manažerka	Riziko neposkytnutí součinnosti při implementaci GDPR	Zpracovatel odmítne podepsat dodatek ke smlouvě o zpracovávání OÚ	Nabytí souladu s GDPR	Neochota zpracovatelů přizpůsobení vnitřních procesů vůči GDPR	4	1	4	Malá	Nutnost výběru nového dodavatele a zvýšená časová náročnost	V případě neposkytnutí součinnosti vybrat jiného dodavatele (zpracovatele OÚ)
3	Projektový manažer	Riziko úniku informací a know how	Externí zaměstnanci vynesou know how společnosti	Renomé společnosti	Přístup k datům	5	3	15	Velmi vysoká	Poškození dobrého jména společnosti, ztráta konkurenční výhody	Smluvní zajištění vč. Smlouva o mlčenlivosti
4	Ředitel	Riziko výpadku zdrojů	Zaměstnanec podá výpověď / nebude moct pracovat z důvodu nemoci	Lidské zdroje	Přetěžování zdrojů, výpadek zdroje, fluktuace zaměstnanců	4	3	12	Vysoká	Prodloužení projektu / zvýšení finanční náročnosti	Nastavení zastupování pracovníků, prioritizace úkolů
5	Ředitel	Riziko úniku dat o SÚ	Zaměstnanci zveřejní / smažou údaje SÚ	Údaje SÚ	Lidská chyba, pokus o poškození společnosti	5	3	15	Velmi vysoká	Poškození dobrého jména společnosti	Aktivace mechanismu proti odcizení dat, omezení přístupů dle rolí
6	Projektový manažer	Riziko zvýšení finanční náročnosti projektu	Při projektu budou nalezeny další nezbytné aktivity pro nabytí souladu s GDPR.	Rozpočet projektu	Výskyt nových dosud nenaplánovaných aktivit v projektu	3	3	9	Střední	Možná neakceptace navýšení rozpočtu vedením společnosti	Precizní plánování, vytvoření rozpočtových rezerv před začátkem projektu, aktualizace business case
7	Právník	Riziko záměrného zvolení jiného právního titulu	Pracovník zvolí jiný typ právního titulu, aby mohl pokračovat ve zpracování OÚ.	Zákonnost zpracování OÚ	Neúmyslné / úmyslné ovlivňování skutečnosti	3	2	6	Střední	Nenabytí souladu s GDPR, sankce od dozorového úřadu	Review stanovených právních titulů advokátní kanceláří
8	Ředitel	Riziko neschopnosti vyhovění právu SÚ	SÚ chce uplatnit své právo, ale společnost nemá nastavenou metodiku pro výkon, tj. nedokáže např. shromáždit veškeré informace či není stanovený řešitel.	Práva subjektů údajů	Nepřipravená metodika výkonu práv SÚ	5	5	25	Kritická	Nevyhovění právu SÚ a následná sankce od dozorového úřadu	Prozatimní stanovení zodpovědné osoby za výkon práv subjektů
9	Právník	Riziko změny legislativy týkající se ochrany osobních údajů	EU nebo ÚOOÚ vydá aktualizaci podmínek zpracování OÚ.	Implementované procesy	Aktualizace legislativy	4	1	4	Malá	Nenabytí souladu s nařízením GDPR	Pravidelná aktualizace změn legislativy během projektu i po jeho dokončení advokátní kanceláří
10	Projektový manažer	Riziko špatné kontroly výstupů projektu	Vzniklá dokumentace neobsahuje nezbytné prvky.	Produkty projektu	Opomenutí části produktu	5	4	20	Kritická	Produkt (např. Směrnice pro ochranu OÚ) nebude splňovat všechny náležitosti	Vytvoření checklistů pro kvalitu a úplnost produktů
11	Projektový manažer	Riziko špatného odhadu časové náročnosti úkolů	Dochází k časovým prodlevám, projekt nabírá zpoždění.	Časová náročnost projektu	Přirozené vytváření časových rezerv na úkoly	3	4	12	Vysoká	Prodloužení projektu	Dvojité ověření časové náročnosti jednotlivých úkolů
12	Projektový manažer	Riziko nedokončení úkolů	Pro daný úkol není stanovená zodpovědná osoba.	Produkty projektu	Nejasně definové zodpovědnosti	4	2	8	Střední	Dezinformace mezi zaměstnanci o zodpovědné osobě za provedení úkolu a možnost nedokončení činnosti	Stanovení postihů a jasné definování zodpovědností

Příloha č. 2 – Registr záznamů o činnostech zpracování osobních údajů

Příloha č. 3 Informační memorandum

Informace o zpracovávání osobních údajů

Účel zpracování:
Vyřízení žádosti z webového formuláře, emailu.

Popis účelu zpracování:
Vaše osobní údaje využijeme pro následné kontaktování Vaší osoby za účelem vyřízení Vaší žádosti či poptávky po produktu. V případě složitějších žádostí z Vaší strany, můžeme využít někoho z našich partnerů pro zodpovězení Vašeho dotazu nebo žádosti.

Zpracování osobních údajů na základě právního titulu:
Plnění smlouvy, Zákonná povinnost, Oprávněný zájem, Souhlas se zpracováním OÚ

Kategorie osobních údajů, které zpracováváme:
Identifikační údaje, kontaktní údaje, údaje o produktu, komunikace.

Doba zpracování a archivace:
V případě Souhlasu se zpracováním OÚ – po dobu trvání účelu pro který byl souhlas udělen.
V případě Smlouvy – po dobu stanovenou zákonem.

Kategorie zpracovatelů nebo příjemců, kterým osobní údaje můžeme poskytnout:
Marketingové agentury, infolinka, členové partnerské sítě. Vaše osobní údaje mohou být na vyžádání poskytnuty orgánům veřejné moci, zejména soudům, Policii České republiky a dalším orgánům činným v trestním řízení v nezbytném rozsahu a v mezích zákona.

Zdroj osobních údajů:
Osobní údaje získáváme přímo od Vás.

Předávání osobních údajů do třetích zemí nebo nadnárodním společnostem:
V rámci uvedeného zpracování se Vaše osobní údaje nebudou předávat do třetích zemí ani jiným nadnárodním společnostem.

Automatizované rozhodování na základě osobních údajů:
Neprovádíme automatizované rozhodování.

Ostatní informace:
Osobní údaje mohou být předmětem archivace ve veřejném zájmu a použity pro účely historického nebo statistického výzkumu. V odůvodněných případech mohou být osobní údaje předmětem zpracovaní z důvodu řešení právních záležitostí, včetně plnění povinností vůči orgánům veřejné správy, a sledování a průběžného vyhodnocování právních rizik.

Vaše práva

1. Přístup ke zpracovávaným osobním údajům.
2. Odvolání souhlasu se zpracováním osobních údajů.
3. Opravu nepřesných či nesprávných údajů případně doplnění neúplných údajů
4. Výmaz osobních údajů v případě zániku účelu nebo neoprávněného zpracování
5. Omezení neboli blokaci zpracování osobních údajů.
6. Výpis osobních údajů ve strukturovaném a strojově čitelném formátu pro sebe, nebo pro jiného správce
7. Podání námitky proti zpracování osobních údajů, pokud se domníváte, že zpracování není oprávněné.
8. Nebýt předmětem automatizovaného rozhodování.

Uplatnění práv

[redacted] Emailem [redacted]
[redacted] Telefonicky na čísle: [redacted]
[redacted] Písemně na adrese: [redacted]

Příloha č. 4 – Směrnice o ochraně osobních údajů

Vnitřní předpis

Ochrana osobních údajů

Společnost: [redacted]

Schválil: [redacted]

Datum platnosti: [redacted]

I. PRAVIDLA PRO NÁKLÁDÁNÍ S OSOBNÍMI ÚDAJI

1. Úvod

Tato směrnice upravuje zpracování osobních údajů v [redacted] (dále jen "**Společnost**") v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („**GDPR**" nebo „**Nařízení**").

Účelem této směrnice je zajistit dodržování povinností vyplývajících z Nařízení ve Společnosti a umožnit subjektům údajů výkon jejich práv.

2. Vymezení některých pojmů

- „**osobní údaj**" veškeré informace o identifikované nebo identifikovatelné fyzické osobě, tj. osobě, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (např. 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);
- „**zvláštní kategorie osobních údajů**" osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;
- „**zpracování**" 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;
- „**omezení zpracování**" označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;
- „**správce**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
- „**zpracovatel**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;
- „**příjemce**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují;
- „**třetí strana**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jenž je oprávněna ke zpracování osobních údajů;
- „**souhlas**" subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;
- „**porušení zabezpečení osobních údajů**" jakékoliv porušení důvěrnosti, dostupnosti či integrity osobních údajů, tedy porušení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně

nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

- „**dozorový úřad**" Úřad pro ochranu osobních údajů České republiky
- „**likvidace**" osobních údajů znamená fyzické zničení jejich nosiče nebo jejich vymazání

3. ROLE A ODPOVĚDNOSTI

3.1. Pracovníci

Tento vnitřní předpis je závazný pro všechny zaměstnance, členy statutárního orgánu Společnosti, i další externí poskytovatele služeb Společnosti (dále jen „**pracovník**"), a na jeho nerespektování bude ze strany Společnosti pohlíženo jako na závažné porušení pracovních a smluvních povinností se všemi důsledky vyplývajícími z obecně závazných právních předpisů.

Každý pracovník Společnosti odpovídá za to, že zpracování osobních údajů provádí v souladu s právními předpisy a tímto interním předpisem a dalšími předpisy a dokumenty Společnosti. Každý pracovník je povinen zachovávat mlčenlivost o osobních údajích a opatřeních přijatých k jejich ochraně, o nichž se v souvislosti s výkonem své činnosti dozvěděl, a to i po skončení pracovního či jiného poměru.

4. ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Obecné zásady zpracování osobních údajů

Při zpracování osobních údajů ve Společnosti je nezbytné dodržovat následující zásady:

zákonnost, korektnost a transparentnost

- ve vztahu k subjektu údajů musí být osobní údaje zpracovávány korektně, zákonným a transparentním způsobem;

účelové omezení

- osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný;

minimalizace údajů

- zpracování musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou osobní údaje zpracovávány;

přesnost

- osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny;

omezení uložení

- osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány;

integrita a důvěrnost

- osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

5. OPATŘENÍ K ZAJIŠTĚNÍ OCHRANY OSOBNÍCH ÚDAJŮ

Systém ochrany osobních údajů je tvořen komplexem organizačních a technických opatření, která jsou ve Společnosti realizována za účelem zabezpečení ochrany a bezpečnosti osobních údajů.

5.1.Fyzická bezpečnost

5.1.1. Pracovníci

Každý pracovník je povinen zajistit ochranu pracovní stanice tak, aby nemohlo dojít k jejímu zneužití jiným pracovníkem, případně cizí neoprávněnou osobou.

Tato povinnost zahrnuje:

- Zamknutí dveří kdykoli při odchodu z kanceláře (pokud je v kanceláři sám nebo pokud odchází jako poslední)
- Neponechávat klíče v zámku kanceláře
- Dodržování pravidla čistého stolu, tzn. neponechávat v době své nepřítomnosti na pracovním stole volně položené dokumenty klasifikované jako neveřejné a aktivování funkce uzamknout stanici (WINDOWS + L), při odchodu z místnosti
- Odpovědnost za návštěvu po dobu jejího pobytu, návštěva nesmí zůstat bez dozoru
- V případě, že pracovník opouští pracovní místo a v místnosti se nenacházejí žádné další osoby, je povinen zkontrolovat uzavření oken a uzamknout místnost
- Všechny dokumenty obsahující osobní údaje musejí být při opuštění pracoviště v uzamčených skříních.

5.1.2. Kanceláře Společnosti

Společnost má sídlo a kanceláře v budově, která je dostatečně zabezpečena před vnikem nepovolaných osob.

Přímo od kanceláře Společnosti má každý z pracovníků vlastní klíč, který je vydáván na základě předávacího protokolu. V kanceláři jsou uzamykatelné skříně a stoly, v nichž jsou uloženy dokumenty citlivé a obsahující osobní údaje.

5.2. IT bezpečnost

- Přístup k osobním údajům je přidělován jen v rozsahu nezbytně nutném pro výkon funkce a revize těchto přidělených přístupů probíhá pravidelně. V případě zjištění neoprávněného přístupu se tento přístup následně odebírá. Dále je zajištěna kontrola neslučitelných oprávnění.
- V ukončení působení jakéhokoliv pracovníka ve Společnosti jsou mu jeho přístupová práva neprodleně odebrána. Informaci osobě kompetentní k odebírání přístupových práv předává personální oddělení.
- Pokud jakékoliv externě zpracovávané agendy vyžadují přístup dodavatelů, musí být tento přístup řešen smluvně, v souladu s bezpečnostní dokumentací tak, aby byla zajištěna bezpečnost osobních údajů uvnitř i vně Společnosti.
- Pracovníci mohou využívat vzdálených přístupů k IT prostředí Společnosti pouze na základě jejich pracovních a smluvně převzatých povinností a kompetencí, a to jen s využitím schválených komunikačních prostředků.
- O jednotlivých přístupech na úrovni domény jsou automaticky pořizovány logy.
- Je povoleno provozovat pouze schválený, legálně nabytý a evidovaný SW a HW ve shodě s licenčním ujednáním výrobce a způsobů využití.
- Je zajištěna správa opravných a aktualizačních balíčků programového vybavení.

- Informační aktiva jsou chráněna před počítačovými viry, spamem, spyware a jiným škodlivým kódem správným nastavením bezpečnostních mechanismů a použitím vhodného SW aplikovaného na relevantní komponenty počítačové sítě (servery, firewally i jednotlivé pracovní stanice a mobilní zařízení ve správě Společnosti).
- Zálohování dat probíhá na denní bázi, je zajištěno, že při obnově zálohy budou obnovena pouze aktuální data.
- Informační aktiva, která sloužila k uchovávání či přenosu osobních údajů a již nejsou dále potřebná nebo dosáhly konce svojí životnosti, jsou bezpečně zlikvidována a je uchován záznam o jejich likvidaci.

5.3. Postup při vzniku incidentu

Postup při vzniku incidentu viz Bezpečnostní směrnice. Vedení Společnosti, nebo jím pověřený zaměstnanec vede záznamy o incidentech.

5.4. Kontrolní činnost

Pravidelně, minimálně 1x ročně, nebo v případě výskytu závažného incidentu je prováděn interní audit se zaměřením na dodržování pravidel stanovených touto směrnicí. Audit provádí vedení Společnosti nebo jím určená osoba.

5.5. Školení zaměstnanců

Pravidelně, minimálně 1x ročně, nebo v případě výskytu závažného incidentu je prováděno školení všech pracovníků Společnosti se zaměřením na dodržování pravidel stanovených touto směrnicí. Školení je realizováno elektronickou formou nebo osobně ze strany jednatele. O školení jsou vedeny záznamy.

5.6. Pravidelná revize a aktualizace interních předpisů

Všechny interní předpisy společnosti, včetně těch, týkajících se ochrany osobních údajů jsou revidovány pravidelně 1x krát ročně. Ad hoc revize je prováděna zejména v případě výraznějších změn ve společnosti s možným dopadem na ochranu osobních údajů nebo v případě narušení zabezpečení ochrany osobních údajů. O provedení revize a aktualizace je vedena evidence. Za revizi a aktualizaci odpovídá odpovědná osoba.

5.7. Vedení a aktualizace záznamů o činnostech zpracování

Záznamy o činnostech zpracování jsou součástí pravidelné revize a aktualizace interních předpisů. Revize kompletnosti a přesnosti katalogu zpracování je prováděna pravidelně 1x krát ročně. Ad hoc revize je prováděna zejména v případě výraznějších změn ve společnosti s možným dopadem na ochranu osobních údajů. O provedení revize a aktualizace je vedena evidence. Za revizi a aktualizaci odpovídá odpovědná osoba.

5.8. Zpracovatelské vztahy

Ve všech případech, kdy Společnost využívá zpracovatele a stejně tak v případech, kdy je Společnost v pozici zpracovatele je uzavřena smlouva o zpracování osobních údajů v souladu s čl. 28 Nařízení.

6. VÝKON PRÁV SUBJEKTŮ ÚDAJŮ

Všechny požadavky subjektů údajů musí být vyřízeny bez zbytečného odkladu, nikdy ne později než do 1 měsíce ode dne jejich obdržení. Pokud není možné dodržet lhůtu, vedení Společnosti pak stanoví, jak postupovat dále.

Všichni pracovníci Společnosti jsou povinni poskytnout součinnost při vyřizování žádostí subjektů údajů. Všechny systémy Společnosti jsou nastaveny tak, aby bylo možné vyhovět žádostem subjektů údajů.

6.1. Poskytování informací

Společnost poskytuje subjektům údajů informace v souladu s článkem 13 a 14 GDPR, a to v požadovaném rozsahu, čímž zajišťuje transparentnost zpracování.

6.2. Právo subjektů údajů na přístup k osobním údajům

V případě, že o to subjekt údajů požádá, Společnost poskytne subjektu údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, umožní subjektům údajů získat přístup k těmto osobním údajům a k informacím způsobem a v rozsahu dle článku 15 GDPR.

6.3. Právo na opravu

V případě, že o to subjekt údajů požádá, případně se o nepřesných osobních údajích dozví Společnost jinak, opraví bez zbytečného odkladu nepřesné osobní údaje. V případě, kdy si to účel zpracování vyžaduje, zajistí Společnost doplnění neúplných osobních údajů dle článku 16 GDPR.

6.4. Právo na výmaz

V případě, že je dán jeden z následujících důvodů, zajistí Společnost na základě uplatnění práva subjektem údajů bez zbytečného odkladu výmaz osobních údajů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovávány;
b) subjekt údajů odvolá souhlas, na jehož základě byly osobních údaje zpracovávány, a neexistuje žádný další právní důvod pro zpracování;
c) subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;
d) osobní údaje byly zpracovány protiprávně;
e) osobní údaje musí být vymazány ke splnění právní povinnosti, která se na Společnost vztahuje;
f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační Společnosti podle čl. 8 odst. 1 GDPR.

6.5.Právo na omezení zpracování

V případě, že je dán jeden z následujících důvodů, zajistí Společnost omezení zpracování osobních údajů:

a) subjekt údajů popírá přesnost osobních údajů;
b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
c) Společnost již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
d) subjekt údajů vznesl námitku proti zpracování.

6.6.Právo na přenositelnost údajů

V případě, že o to subjekt údajů požádá a zároveň je zpracování založeno na souhlasu nebo smlouvě, a zároveň se zpracování provádí automatizovaně, umožní Společnost subjektu údajů výkon práva na přenositelnost. Osobní údaje, které subjekt údajů Společnosti poskytl a které se ho týkají, poskytne Společnost ve strukturovaném, běžně používaném a strojově čitelném formátu. Součástí tohoto práva

X

je zajištění možnosti přenesení předmětných osobních údajů k jinému správci dle požadavku subjektu údajů.

7. ARCHIVACE A LIKVIDACE OSOBNÍCH ÚDAJŮ

Společnost provádí likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovávány, případně na základě žádosti subjektu.
Konkrétní lhůty pro likvidaci osobních údajů jsou stanoveny v jednotlivých záznamech o činnostech zpracování.
Při likvidaci jsou dodržovány zákonné výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.
Veškeré listinné dokumenty likvidovány výhradně skartací a to svépomocí, nebo využitím externí společnosti. Data uchovávána v elektronické podobě jsou likvidována tak, aby nebylo možné jejich obnovení. V případě konce životnost jednotlivých elektronických zařízení jsou tato mechanicky likvidována tak, aby nebylo možné data obnovit.

8. ZÁVĚREČNÁ USTANOVENÍ

Za dodržování pravidel stanovených touto směrnicí odpovídají všichni pracovníci Společnosti.

[redacted]

.....
[redacted]

Příloha č. 5 – Metodický pokyn pro výkon práv subjektů údajů

2018

Metodický pokyn pro výkon práv subjektů

VNITŘNÍ PŘEDPIS

Společnost: [redacted]

Schválil: [redacted]

Datum platnosti: [redacted]

Obsah

1 Předmět dokumentu

Účelem tohoto dokumentu je vymezení procesu reakcí na práva subjektů údajů v souladu s následujícími předpisy:

- Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení o ochraně osobních údajů" nebo „GDPR"),
- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů v platném znění, (dále jen „zákon"),

2 Rozsah působnosti

Vnitřní předpis je závazný pro všechny zaměstnance společnosti a její nedodržování je bráno jako hrubé porušení pracovních a smluvních povinností se všemi důsledky vyplývajících z obecně závazných předpisů.

3 Vymezení základních pojmů

- „**osobní údaj**" veškeré informace o identifikované nebo identifikovatelné fyzické osobě, tj. osobě, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (např. 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);
- „**zpracování**" 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;
- „**správce**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
- „**zpracovatel**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;
- „**třetí strana**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jenž je oprávněna ke zpracování osobních údajů;
- „**souhlas**" subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

4 Výkon práv subjektů

Podle Obecného nařízení GDPR i zákonu o ochraně osobních údajů jsou subjektům údajů přiznány práva za účelem vyrovnání vztahu mezi správcem a subjektem údajů.

Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.

4.1 Právo na přístup k osobním údajům

Subjekt údajů má právo na přístup k osobním údajům ve smyslu získání informace o rozsahu zpracování jeho osobních údajů. Konkrétně má právo získat níže uvedené informace:

- účely zpracování,
- kategorie dotčených osobních údajů,
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
- plánovaná doba, po kterou budou osobní údaje uloženy,
- existence práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
- právo podat stížnost u dozorového úřadu,
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

Pokud správce o fyzické osobě žádné údaje nezpracovává, poskytuje se informace, že osobní údaje tazatele nejsou předmětem zpracování osobních údajů ze strany správce.

4.2 Právo na opravu nepřesných nebo neúplných osobních údajů

Právo na opravu nepřesných nebo neúplných osobních údajů je založena na zásadě přesnosti, kdy subjekt údajů může podat žádost, aby o něm zpracovávané osobní údaje byly upraveny dle skutečnosti. Nejedná se však o povinnost správce vyžadovat po subjektu údajů pravidelnou aktualizaci údajů (například na čtvrtletní či roční bázi).

4.3 Právo na výmaz

Subjekt údajů může využít svého práva být zapomenut, pokud je splněna alespoň jedna z níže uvedených podmínek:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,

- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovány protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti,
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 obecného nařízení.

4.4 Právo na přenositelnost osobních údajů

Subjekt údajů má právo na přenesení jeho osobních údajů k jinému správci, avšak pouze za předpokladu že:

- zpracování osobních údajů je založené na právním titulu Souhlas se zpracováním osobních údajů nebo Smlouvě,
- jedná se o automatizované zpracování.

4.5 Právo na omezení zpracování

Jedná se o formu dočasného práva subjektu údajů, které může uplatnit v případech, kdy:

- osobní údaje považuje za nepřesné, v takovém případě je zpracování omezeno do doby, kdy Správce ověří přesnost těchto údajů,
- zpracování je protiprávní a subjekt údajů požaduje omezení zpracování osobních údajů namísto jejich výmazu,
- správce osobních údajů již nepotřebuje osobní údaje subjektu údajů pro vymezený účel zpracování, ale subjekt údajů je požaduje uchovat za účelem určení, obhajoby nebo výkonu právních nároků,
- subjekt údajů vznesl námitku proti zpracování (omezení platí do doby ověření oprávněného důvodu zpracování)

Způsoby omezení zpracování:

- dočasné přenesení vybraných osobních údajů do jiného systému,
- zaměstnancům/uživatelům je znemožněn přístup k osobních údajům,
- odstranění zveřejněných osobních údajů (např. z webových stránek),
- v případě zpracování osobních údajů v systémech pro automatizované zpracování zabezpečit zastavení zpracování vybraných osobních údajů subjektu údajů.

4.6 Právo vznést námitku

Subjekt údajů má právo vznést námitku proti zpracování osobních údajů, které jsou zpracovávány na základě právních důvodů:

- zpracování je nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany.

V případě vznesení námitky Správce údajů přestane zpracovávat osobní údaje subjektu údajů, pokud neprokáže závažné oprávněné důvody pro zpracování převažující práva, svobody a zájmy subjektu údajů.

Námitku lze také vznést proti zpracování osobních údajů za účelem přímého marketingu nebo profilování. Dále v případě námitky proti přímému marketingu Správce již nemůže zpracovávat osobní údaje subjektu údajů.

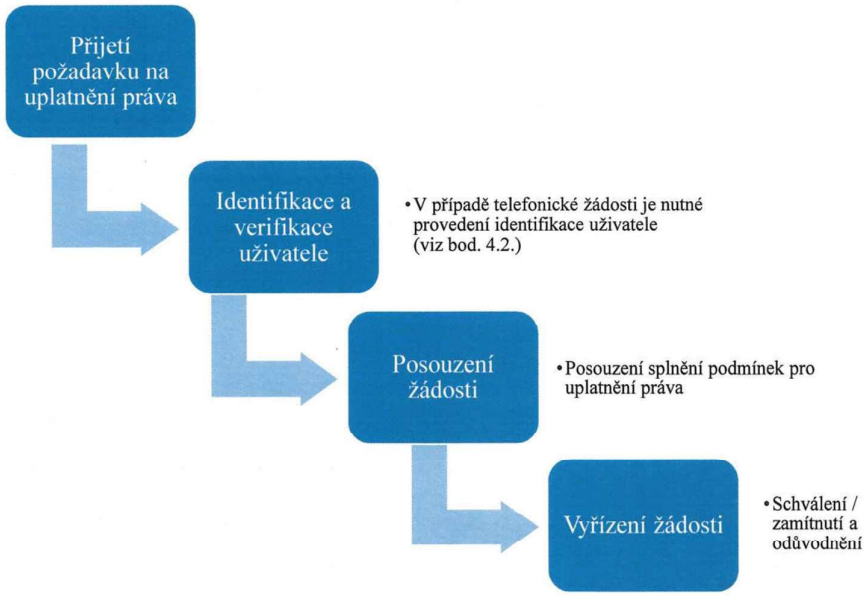
4.7 Právo nebýt předmětem automatizovaného individuálního rozhodování s právními či obdobnými účinky, zahrnujíce i profilování

Subjekt údajů má dále právo nebýt předmětem rozhodnutí, které je založeno výhradně na automatizovaném zpracování včetně profilování, jenž má na subjekt údajů právní účinky nebo se ho značným způsobem dotýká.

Při každém takovémto zpracování je nezbytné, aby konečné rozhodnutí stanovil člověk.

5 Proces vyřízení žádosti

Obrázek 1 - popis procesu vyřízení žádosti



5.1 Komunikační kanály

Subjekt údajů může podat žádost pro uplatnění svých práv vyplývajících z GDPR nařízení prostřednictvím tří komunikačních kanálů:

[redacted]Telefonicky na čísle [redacted]

2) Webového formuláře na [redacted]
3) Doporučeným dopisem na sídlo společnosti

[redacted]

5.2 Identifikace a verifikace žadatele

Pro vyřízení výkonu práv subjektu údajů je nezbytné provést identifikaci a verifikaci daného subjektu údajů za účelem potvrzení jeho totožnosti a redukce podvodného pokusu o manipulaci s osobními údaji.

Zaměstnanec, který žádost obdrží, provede verifikaci uživatele na základě informací, které může znát pouze subjekt údajů v závislosti na charakteru zpracovávaných informací.

Příklad

Pokud zaměstnanec vyřizuje žádost subjektu údajů po telefonu, dotáže se subjektu údajů na takové informace, které jsou námi zpracovávány a měly by být známé pouze jeho osobě např. poslední 4 čísla z rodného čísla nebo při držení údajů z webového formuláře se dotázat na jméno klienta, email případně telefonní číslo.

5.3 Lhůta pro vyřízení žádosti

Dle Obecného nařízení GDPR musí být obdržená žádost vyřízena bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. GDPR umožňuje lhůtu ve zvláštních případech prodloužit a to s ohledem na složitost a počet žádostí o další dva měsíce. V takových případech však subjekt údajů musí být o takové skutečnosti informován spolu s důvodu pro odklad vyřízení.

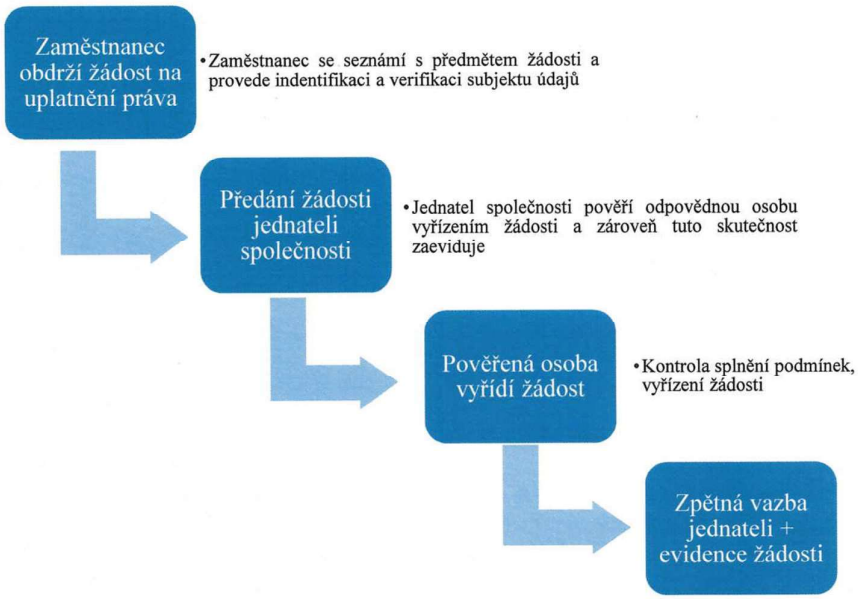
5.4 Odmítnutí žádosti

Správce může odmítnout žádost subjektu údajů pouze v případě, kdy doloží, že nemůže zjistit totožnost subjektu údajů nebo se žádosti opakují, aniž by byly důvodné a přiměřené.

5.5 Účtování nákladů

Veškeré úkony spojené s výkonem práv subjektu údajů se poskytují **bezplatně.** Pouze v případech, kdy se zjevně dochází k opakovaným nedůvodným nebo nepřiměřeným žádostem od subjektu údajů může Správce osobních údajů (společnost) uložit přiměřený poplatek, který zohledňuje administrativní náklady spojené s vyřízením žádosti.

5.6 Interní proces vyřízení žádosti



6 Závěrečná ustanovení

Za dodržování pravidel stanovených touto směrnicí odpovídají všichni pracovníci Společnosti.

[redacted]

.....

[redacted]

VZOR: ŽÁDOST SUBJEKTU ÚDAJŮ

Identifikace Subjektu údajů

Jméno a příjmení: _____

Datum narození: _____

Adresa: _____

Další identifikace (e-mail, telefonní číslo,...):_____

Předmět žádosti – Jaké právo chci využít

Právo na přístup

Stačí mi znát typy osobních údajů, které o mě zpracováváte (např. údaje nutné k plnění smlouvy nebo smluv, které jsme společně uzavřeli, nebo monitorování toho, jak využívám zakoupené služby atd.); nebo

Chci znát podrobně všechny osobní údaje, které se mě týkají, a které zpracováváte, ale nepotřebuji obdržet kopie těchto osobních údajů; nebo

Chci znát podrobně všechny osobní údaje, které se mě týkají, a které zpracováváte, a dále žádám o zaslání kopie těchto osobních údajů, a to tímto způsobem:

na následující emailovou adresu: _____; nebo

na následující adresu: _____.

Právo na opravu

Přeji si opravit/doplnit následující osobní údaje: _____

Aktuální hodnota osobních údajů je: _____

Právo na výmaz

Přeji si, abyste o mně dále nezpracovávali následující osobní údaje _____ a vymazali je z vašich systémů.

Právo na omezení zpracování (popište, jaké zpracování si přejete omezit, případně uveďte, kterých osobních údajů se má omezení týkat)

Přeji si, abyste omezili následující zpracování _____ (popis zpracování, které si přejete omezit) mých osobních údajů _____ (kterých osobních údajů se má omezení týkat).

Právo na přenositelnost

Žádám o přenos těchto/všech osobních údajů, které o mě zpracováváte, _____, v následujícím formátu _____.

Osobní údaje přeneste mně na následující emailovou adresu: _____

NEBO

Přeneste osobní údaje přímo následujícímu novému správci:

Jméno správce: _____

Adresa správce: _____

Email správce:_____

Telefon správce: _____

Právo vznést námitku proti zpracování

Vznáším námitku proti následujícímu zpracování mých osobních údajů: _____

Pokud žádáte o výmaz/omezení zpracování a uznáme oprávněnost Vaší žádosti, budeme o výmazu/změně/omezení zpracování osobních údajů informovat všechny příjemce, kterým byly Vaše osobní údaje zpřístupněny, s výjimkou případů, kdy by to bylo nemožné nebo by to vyžadovalo nepřiměřené úsilí. Máte zájem o informaci o takových příjemcích osobních údajů? (**ANO/NE**)

Důvod žádosti

Pokud žádáte o výkon práva na výmaz, práva na omezení zpracování nebo práva vznést námitku, uveďte, prosím, zdůvodnění Vaší žádosti. Pokud tak neučiníte, nemůže být žádosti vyhověno.

_____

_____

VZOR: ODPOVĚĎ NA ŽÁDOST SUBJEKTU ÚDAJŮ

Identifikace Subjektu údajů

Jméno a příjmení: _____

Datum narození: _____

Adresa: _____

Další identifikace (e-mail, telefonní číslo, ...): _____

Odpověď na žádost, č.j.: _____

Vaši žádost o (právo, které subjekt údajů uplatnil) ze dne _____ jsme pečlivě posoudili s následujícím závěrem:

Právo na přístup

Ve Vaší žádosti jste upřednostnil/a (vybrat jednu z níže uvedených variant)

Znát kategorie osobních údajů, které o Vás zpracováváme (např. plnění smlouvy nebo smluv, které jsme společně uzavřeli, nebo monitorování toho, jak využívám zakoupené služby). Níže tedy uvádíme, že o Vás zpracováváme následující typy osobních údajů:

_____

Znát podrobně všechny osobní údaje a další předepsané informace, které se Vás týkají a které zpracováváme, ale nepotřebujete obdržet kopie těchto osobních údajů. V příloze tedy uvádíme podrobný přehled o Vašich osobních údajích, které zpracováváme, spolu s následujícími informacemi:

účely zpracování,

kategorie dotčených osobních údajů,

příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,

plánovaná doba, po kterou budou osobní údaje uloženy; a

to, zda dochází k automatizovanému rozhodování či nikoliv.

Znát podrobně všechny osobní údaje, které se Vás týkají, a které zpracováváme, a dále žádáte o zaslání kopie těchto osobních údajů, a to tímto způsobem:

na následující emailovou adresu: _____; nebo

na následující adresu: _____.

V příloze tedy uvádíme podrobný přehled o Vašich osobních údajích, které zpracováváme, spolu s následujícími informacemi:

účely zpracování,

kategorie dotčených osobních údajů,

příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,

plánovaná doba, po kterou budou osobní údaje uloženy; a

to, zda dochází k automatizovanému rozhodování či nikoliv.

Současně Vám zasíláme kopie Vašich osobních údajů na Váš email, uvedený ve Vaší žádosti/na Vaši adresu, uvedenou ve Vaší žádosti.

NEBO:

Vaši žádost bohužel musíme zamítnout z následujících důvodů: _____

NEBO:

Zjistili jsme, že o Vás nezpracováváme žádné osobní údaje.

Právo na opravu

Na základě Vaší žádosti jsme opravili/doplnili následující osobní údaje: _____

Současně budeme o opravě nebo doplnění osobních údajů informovat příjemce, kterým byly Vaše osobní údaje zpřístupněny.

PŘÍPADNĚ

Bohužel nemůžeme o opravě nebo doplnění informovat následující příjemce, vzhledem k tomu, že to není možné, resp. by to vyžadovalo nepřiměřené úsilí: _____

Právo na výmaz

Osobní údaje, které můžeme vymazat: _____

Výše uvedené osobní údaje vymažeme z našich systémů do _____. O likvidaci Vašich osobních údajů Vás budeme informovat emailem.

Současně budeme o výmazu osobních údajů informovat příjemce, kterým byly Vaše osobní údaje zpřístupněny.

PŘÍPADNĚ

Bohužel nemůžeme o likvidaci informovat následující příjemce, vzhledem k tomu, že to není možné, resp. by to vyžadovalo nepřiměřené úsilí: _____

Osobní údaje, které bohužel nemůžeme zlikvidovat, protože nám v tom brání závažné právní důvody:

_____

_____

Právo na přenositelnost

Osobní údaje, které můžeme přenést: _____

Výše uvedené osobní údaje přeneseme Vám na Vaši emailovou adresu _____/novému správci, _____ na jeho emailovou adresu_____ v následujícím formátu _____ do _____. Přenos bude zabezpečen způsobem dohodnutým s Vámi/s novým správcem. O provedení přenosu Vašich osobních údajů Vás budeme informovat emailem.

Osobní údaje, které bohužel nemůžeme přenést, protože nám v tom brání závažné právní důvody:

_____

_____

Pozor! Neručíme za to, že nový správce bude Vaše osobní údaje zpracovávat s odpovídající péčí a bezpečně. Proto Vám doporučujeme, abyste se ujistil, že nový správce bude Vaše osobní údaje zpracovávat s řádnou péčí a při zajištění odpovídajících bezpečnostních opatření (uvést v případě, že odpovídáte na žádost o přenos osobních údajů).

Poučení

Lhůta: Informace musí být poskytnuta bez zbytečného odkladu, nejdéle do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení.

Poplatek: Zásadně platí, že informace se poskytují bezplatně. Pouze v případě, kdy se žádosti opakují, může správce účtovat přiměřený poplatek na základě administrativních nákladů. Dále, pokud jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost dokládá správce. **Zneužitím** nelze a priori rozumět výkon práv subjektu údajů.

Právo podat stížnost kvůli způsobu vyřízení žádosti: Pokud nebudete spokojeni s vyřízením Vaší žádosti, máte právo si stěžovat u správce-adresáta Vaší žádosti na této adrese: _____.

Můžete rovněž podat stížnost u Úřadu pro ochranu osobních údajů (ÚOOÚ).

DATUM:

PODPIS: