

Název:	OCHRANA OSOBNÍCH ÚDAJŮ
Vnitřní směrnice č.:	A/10/2018/1
Obsah:	Postupy a opatření vztahující se ke Zpracování Osobních údajů
Přílohy:	<ol style="list-style-type: none"> 1. Interní analýza oprávněných zájmu Správce 2. Záznamy o činnostech Zpracování 3. Vzory dokumentů plnění informační povinnosti vůči jednotlivým typům subjektů údajů 4. Příklady porušení zabezpečení Osobních údajů 5. Vzor evidence žádostí Subjektu údajů
Určena:	Všem pracovníkům Společnosti
Vytvořil:	Osoba pověřená výkonem compliance
Schválil:	jednatel
Ruší směrnici č.:	
Platnost od:	25. 5. 2018
Účinnost od:	25. 5. 2018
Změna č.:	1
Přílohy	
Schválil:	
Platnost změny od:	1.2.2019
Účinnost změny od:	1.2.2019

Obsah

1. Úvodní ustanovení.....	3
1.1 Účel předpisu	3
1.2 Zásady Zpracování Osobních údajů.....	3
1.3 Definice základních pojmů.....	4
2. Vnitřní procesy související se Zpracováním Osobních údajů	4
2.1 Základní povinnosti.....	4
2.1.1 Obecné povinnosti	4
2.1.2 Zákonnost Zpracování.....	5
2.1.3 Záznamy o činnostech Zpracování	6
2.1.4 Pověřenec pro ochranu Osobních údajů	6
2.2 Informování Subjektů údajů o Zpracování Osobních údajů	6
2.3 Uplatňování práv Subjekty údajů.....	7
2.3.1 Společná pravidla a postupy.....	7
2.3.2 Zvláštní pravidla a postupy vztahující se k jednotlivým uplatňovaným právům	9
2.4 Spolupráce se Zpracovateli.....	13
2.5 Zabezpečení Zpracování Osobních údajů.....	14
2.6 Porušení zabezpečení Osobních údajů.....	15
2.7 Posouzení vlivu na ochranu Osobních údajů	15
2.8 Předávání Osobních údajů do třetích zemí nebo Mezinárodním organizacím.....	16
2.9 Likvidace Osobních údajů	16
2.10 Pravidelná školení v oblasti Osobních údajů	16
3. Dohled nad oblastí Zpracování Osobních údajů.....	17
3.1 Organizační zajištění dohledu.....	17
3.2 Postavení, pravomoci a povinnosti Osoby pověřené kontrolou zpracování osobních údajů.....	17
3.3 Úkoly Osoby pověřené kontrolou zpracování osobních údajů	18
3.3.1 Monitorování souladu činností Společnosti s Nařízením GDPR.....	18
3.3.2 Poskytování poradenství, informací a součinnosti	18
3.3.3 Prověření porušení zabezpečení Osobních údajů a související úkoly	18
3.3.4 Komunikace se Subjekty údajů.....	20
3.3.5 Školení v oblasti Osobních údajů	20
4. Závěrečná ustanovení	20

1. Úvodní ustanovení

1.1 Účel předpisu

- (1) Tento předpis stanoví vnitřní postupy a organizační opatření vztahující se ke Zpracování Osobních údajů Společností **KZ FINANCE, spol. s r.o., Elišky Krásnohorské 1140/4, Kroměříž 767 01, IČ: 25509624 (dále jen „Společnost“)** jako Správcem.
- (2) Tento předpis je určen všem zaměstnancům Společnosti (dále „pracovníci“) a osobám působícím pro Společnost jako Zpracovatelé.
- (3) Účelem tohoto předpisu je zajistit, aby Zpracování Osobních údajů ze strany Společnosti bylo v souladu s Nařízením GDPR a souvisejícími právními předpisy jak Evropské unie, tak České republiky.
- (4) Účelem tohoto předpisu je také minimalizace rizika pro práva a svobody fyzických osob související s jejich Osobními údaji.

1.2 Zásady Zpracování Osobních údajů

- (1) Při jakémkoliv Zpracování Osobních údajů je nezbytné dodržet základní zásady Zpracování uvedené v tomto článku. Vzhledem k tomu, že postupy a opatření stanovené tímto předpisem z těchto zásad vycházejí, jejich řádným dodržením dojde i k naplnění těchto základních zásad. Pokud by ale pro některou činnost související se Zpracováním Osobních údajů nebyla tímto předpisem stanovena jednoznačná pravidla, je nutné prokazatelně postupovat v souladu s níže uvedenými zásadami. Jednotlivá ustanovení tohoto předpisu je také potřeba vykládat v souladu s těmito zásadami.
- (2) Zákonost – zpracovávat Osobní údaje lze jen na základě alespoň jednoho z definovaných právních titulů a Zpracování nesmí být protiprávní (tj. nesmí probíhat za nelegálním či nelegitimním účelem).
- (3) Korektnost a transparentnost – všechny informace a všechna sdělení týkající se Zpracování Osobních údajů určené veřejnosti nebo Subjektu údajů musí být stručné, snadno přístupné, srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků.
- (4) 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.
- (5) Minimalizace údajů – shromažďovány a zpracovávány mohou být jen Osobní údaje přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.
- (6) Přesnost – Osobní údaje musí odpovídat skutečnosti, být přesné a v případě potřeby aktualizované, nepřesné údaje musí být opraveny nebo vymazány.
- (7) Omezení uložení – Osobní údaje musí být uloženy ve formě umožňující identifikaci Subjektu údajů jen po dobu nezbytnou vzhledem k účelům, pro které jsou zpracovávány.
- (8) 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.

1.3 Definice základních pojmů

- (1) Mezinárodní organizace – organizace a jí podřízené Subjekty podléhající mezinárodnímu právu veřejnému nebo jiný Subjekt zřízený dohodou mezi dvěma nebo více zeměmi nebo na jejím základě
- (2) Nařízení GDPR – Nařízení 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)
- (3) Osobní údaje – veškeré informace o Subjektu údajů
- (4) 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
- (5) Subjekt údajů – identifikovaná nebo identifikovatelná fyzická osoba, přičemž 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
- (6) Úřad – Úřad pro ochranu Osobních údajů České republiky
- (7) Zákon – zákon č. xxx/2018 Sb., o Zpracování Osobních údajů¹
- (8) 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
- (9) Zpracovatel – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný Subjekt, který zpracovává Osobní údaje pro Správce
- (10) Zvláštní kategorie Osobních údajů – Osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání, filozofickém přesvědčení nebo členství v odborech, a dále genetické údaje, biometrické údaje (pokud se zpracovávají za účelem jedinečné identifikace fyzické osoby), údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

2. Vnitřní procesy související se Zpracováním Osobních údajů

2.1 Základní povinnosti

2.1.1 Obecné povinnosti

- (1) Vzhledem k tomu, že Společnost je Správcem, je povinna dodržovat všechny povinnosti uložené Správcům Nařízením GDPR, Zákonem a dalšími s nimi souvisejícími právními předpisy. Společnost je také povinna prokázat, že při Zpracování Osobních údajů postupovala v souladu s Nařízením GDPR, resp. jeho základními zásadami. Za plnění těchto povinností je odpovědný jednatel Společnosti.

¹ Bude upřesněno po přijetí zákona.

- (2) Společnosti je povinen zajistit, aby byly dodržovány stanovené povinnosti bez ohledu na státní příslušnost nebo bydliště fyzické osoby, o jejíž Osobní údaje se jedná, a také nezávisle na tom, zda dané Zpracování Osobních údajů probíhá v Evropské unii nebo mimo ni.
- (3) Společnosti je povinen zajistit, aby byla zohledňována ochrana Osobních údajů také při návrhu a zavádění nových produktů nebo služeb, při implementaci nového nebo změně stávajícího informačního systému, při spuštění nové marketingové kampaně, při změně smluvní dokumentace se zákazníky apod.
- (4) Společnosti je povinen zajistit, aby všichni pracovníci a Zpracovatelé Společnosti byli seznámeni se svými povinnostmi i povinnostmi Společnosti souvisejícími se Zpracováním Osobních údajů, a to formou pravidelných školení v oblasti Osobních údajů.

2.1.2 Zákonost Zpracování

- (1) Obecně je možné zpracovávat Osobní údaje pouze při splnění alespoň jedné z následujících podmínek (tzv. právní tituly nebo důvody pro Zpracování):
 - a) Subjekt údajů udělil souhlas se Zpracováním svých Osobních údajů pro jeden či více konkrétních účelů;
 - b) Zpracování je nezbytné pro splnění 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 splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen Správce;
 - f) Zpracování je nezbytné pro účely oprávněných zájmů příslušného Správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody Subjektu údajů vyžadující ochranu Osobních údajů, zejména pokud je Subjektem údajů dítě.
- (2) Společnost zpracovává Osobní údaje na základě následujících právních důvodů:
 - plnění smlouvy uzavřené se Subjektem údajů – blíže viz bod (3) tohoto článku;
 - plnění právní povinnosti Společnosti – blíže viz bod (4) tohoto článku;
 - existence oprávněného zájmu Společnosti – blíže viz bod (5) tohoto článku.
- (3) Společnost je dále oprávněna zpracovávat Osobní údaje zaměstnanců, zákazníků, obchodních zástupců, dodavatelů, členů orgánů Společnosti, případně dalších Subjektů údajů, pokud s nimi byla uzavřena smlouva, kde byly tyto Osobní údaje uvedeny, nebo v souvislosti s níž byly Osobní údaje poskytnuty nebo získány, a to po dobu trvání této smlouvy.
- (4) Společnost je také oprávněna zpracovávat Osobní údaje zaměstnanců, členů orgánů Společnosti, zákazníků, obchodních zástupců, tipařů a případně dalších Subjektů údajů, aby mohla splnit povinnosti, které jí ukládají právní předpisy, např.:
 - zákon č. 262/2006 Sb., zákoník práce,
 - zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení,
 - zákon č. 48/1997 Sb., o veřejném zdravotním pojištění,
 - zákon č. 586/1992 Sb., o daních z příjmů,
 - zákon č. 89/2012 Sb., občanský zákoník,
 - zákon č. 90/2012 Sb., o obchodních společnostech a družstvech,
 - zákon č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěrenských fondů,
 - zákon č. 563/1991 Sb., o účetnictví,

- zákonem č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů
- zákonem č. 427/2011 Sb., o doplňkovém penzijním spoření, ve znění pozdějších předpisů
- zákonem č. 170/2018 Sb., o distribuci pojištění a zajištění.

- (5) Některé Osobní údaje určitých Subjektů údajů zpracovává Společnost i proto, že je to nezbytné pro účely jejích oprávněných zájmů. Bližší vysvětlení a zdůvodnění těchto oprávněných zájmů obsahují jednotlivé interní analýzy, kterou jsou v příloze č. 1 tohoto předpisu.
- (6) V ostatních případech Společnost zpracovává Osobní údaje na základě souhlasu uděleného Subjektem údajů. Tyto případy jsou stanoveny v záznamech o činnostech zpracování, jejichž aktuální verze tvoří přílohu tohoto vnitřního předpisu.
- (7) Společnost v odůvodněných případech může zpracovávat i Zvláštní kategorie Osobních údajů v případech stanovených v záznamech o činnostech zpracování, jejichž aktuální verze tvoří přílohu tohoto vnitřního předpisu. Subjekt údajů udělil Společnosti výslovný souhlas se Zpracováním těchto Osobních údajů pro jeden nebo více stanovených účelů.

2.1.3 Záznamy o činnostech Zpracování

- (1) Společnost je povinna vést záznamy o činnostech Zpracování podle čl. 30 odst. 1 Nařízení GDPR, za které odpovídá.
- (2) Tyto záznamy se vedou elektronicky ve formě tabulky a za jejich vedení a aktualizaci je odpovědný jednatel Společnosti.
- (3) Společnost je povinna tyto záznamy poskytnout na požádání Úřadu.
- (4) Aktuální záznamy o činnostech zpracování jsou vždy přílohou č. 2 tohoto předpisu.

2.1.4 Pověřenec pro ochranu Osobních údajů

- (1) Společnost není povinna jmenovat pověřence pro ochranu Osobních údajů podle čl. 37 Nařízení GDPR, protože nesplňuje ani jednu z podmínek uvedených v čl. 37 odst. 1 Nařízení GDPR, konkrétně:
 - a) Společnost není orgánem veřejné moci ani veřejným Subjektem.
 - b) Hlavní činnosti Společnosti nespočívají v operacích Zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování Subjektů údajů. Operace Zpracování Osobních údajů ve Společnosti mají podpůrnou funkci pro hlavní podnikatelskou činnost Společnosti a rozhodně nevyžadují rozsáhlé pravidelné a systematické monitorování Subjektů údajů.
 - c) Hlavní činnosti Společnosti nespočívají v rozsáhlém Zpracování Zvláštních kategorií Osobních údajů a Osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření.
- (2) Společnost pověřuje ředitelku společnosti (dále jen „**Osoba pověřená kontrolou zpracování osobních údajů**“) dohledem nad oblastí Zpracování Osobních údajů ve Společnosti. Konkrétní úkoly a pravomoci Osoby pověřené kontrolou zpracování osobních údajů související s touto činností jsou uvedeny dále v tomto předpise a zejména v kapitole 3 tohoto předpisu.

2.2 Informování Subjektů údajů o Zpracování Osobních údajů

- (1) Společnosti je povinen zajistit, aby vůči Subjektům údajů byla řádně plněna informační povinnost v souladu s čl. 13 a 14 Nařízení GDPR.
- (2) Při plnění informační povinnosti je nezbytné dbát na dodržování zásady korektnosti a transparentnosti (viz čl. 1.2 bod (3) tohoto předpisu) a postupovat v souladu s Pokynem WP 29 č. 260 (Pokyny týkající se transparentnosti).
- (3) Tato informační povinnost může být plněna prostřednictvím smlouvy, která se uzavírá se Subjektem údajů, prostřednictvím informačního dokumentu, který je Subjektu údajů předán nebo zaslán v okamžiku získání jeho Osobních údajů (případně ve lhůtách uvedených v čl. 14 odst. 3 Nařízení GDPR, pokud Společnost nezískává Osobní údaje přímo od Subjektu údajů), případně jiným vhodným způsobem.
- (4) Tam, kde je to vhodné a možné, lze informační povinnost tzv. vrstvit. To znamená, že způsobem uvedeným v předchozím bodě je Subjektu údajů poskytnuta pouze první vrstva informace a dále je odkázáno na speciální sekci internetových stránek Společnosti týkající se Osobních údajů, kde je informace kompletní. V první vrstvě musí být vždy uvedeny ty informace o Zpracování Osobních údajů, které jsou pro Subjekt údajů nejpodstatnější. Informace v obou vrstvách musí být konzistentní a nesmí být vzájemně v rozporu.
- (5) Poskytování informací dle tohoto článku nesmí být vůči Subjektům údajů zpoplatněno.
- (6) Přílohu č. 3 tohoto předpisu tvoří vzory dokumentů pro plnění informačních povinností vůči jednotlivým typům Subjektů údajů.
- (7) Jakoukoliv odchylku od zde stanových pravidel (např. týkající se rozsahu nebo způsobu plnění informační povinnosti) může schválit pouze jednatel Společnosti po předchozím vyjádření Osoby pověřené kontrolou zpracování osobních údajů.

2.3 Uplatňování práv Subjekty údajů

2.3.1 Společná pravidla a postupy

2.3.1.1 Obecná pravidla

- (1) V souladu s čl. 15 až 22 Nařízení GDPR mají Subjekty údajů vůči Správcům určitá práva vztahující se ke Zpracování Osobních údajů, které se jich týkají.
- (2) Společnost je povinna usnadňovat Subjektům údajů výkon jejich práv. V této souvislosti Společnost zřídila speciální sekci svých internetových stránek, kde jsou mimo jiné jednotlivá práva Subjektů srozumitelně popsána včetně návodu pro jejich uplatňování.
- (3) Společnosti tímto pověřuje agendou přijímání, prověřování a vyřizování žádostí Subjektů údajů Osobu pověřenou kontrolou zpracování osobních údajů. Ta je povinna postupovat v souladu s tímto předpisem, Nařízením GDPR, Pokyny WP 29 (např. Pokyny WP 29 č. 260 týkající se transparentnosti nebo Pokyny WP 29 č. 242 týkající se práva na přenositelnost údajů) a stanovisky Úřadu.
- (4) Společnost je povinna vyřizovat žádosti Subjektů údajů bezplatně, nicméně pokud jsou žádosti podané Subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, je Osoba pověřena kontrolou zpracování osobních údajů oprávněna buď

- a) uložit přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo sdělení nebo s učiněním požadovaných úkonů (o uložení tohoto poplatku je Osoba pověřena kontrolou zpracování osobních údajů povinna žadatele předem informovat); nebo
 - b) odmítnout žádosti vyhovět.
- (5) Osoba pověřena kontrolou zpracování osobních údajů je povinna se Subjekty při uplatňování jejich práv komunikovat stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků.
- (6) Osoba pověřena kontrolou zpracování osobních údajů je povinna poskytnout Subjektu údajů informace jím určeným způsobem. Pokud Subjekt údajů žádný konkrétní způsob neurčil a žádost byla podána elektronicky, je Osoba pověřena kontrolou zpracování osobních údajů povinna poskytnout informace elektronicky, v ostatních případech písemně.
- (7) Osoba pověřena kontrolou zpracování osobních údajů je povinna vést důkladnou a kompletní dokumentaci vyřizování jednotlivých žádostí, aby byla Společnost schopna doložit, kdy a o co jí Subjekty údajů žádaly, jak byla žádost prověřována a vyřízena a jaké v té souvislosti byla přijata případná opatření. Vzor evidence žádostí Subjektů údajů tvoří přílohu tohoto vnitřního předpisu.

2.3.1.2 Přijetí žádosti

- (1) Společnost je povinna zabývat se všemi žádostmi Subjektů údajů nezávisle na způsobu jejich doručení Společnosti.
- (2) Subjekt údajů se tedy může na Společnost obrátit např. osobně, telefonicky, emailem nebo poštou a svou žádost může adresovat přímo Osobě pověřené kontrolou zpracování osobních údajů, ale také vedení Společnosti nebo jakémukoliv pracovníkovi Společnosti.
- (3) Každý pracovník Společnosti, kterému je jakýmkoliv způsobem (zejména emailem nebo poštou) doručena nebo předána žádost Subjektu údajů týkající se Osobních údajů, je povinen ji neprodleně předat Osobě pověřené kontrolou zpracování osobních údajů.
- (4) Každý pracovník Společnosti, na kterého se obrátí přímo Subjekt údajů (osobně nebo telefonicky) s dotazem nebo žádostí týkající se Osobních údajů, je povinen odkázat Subjekt údajů na Osobu pověřenou kontrolou zpracování osobních údajů.
- (5) Jakmile je Osobě pověřené kontrolou zpracování osobních údajů předána nebo doručena žádost Subjektu údajů nebo je mu žádost přímo Subjektem údajů sdělena, je povinna nejprve ověřit totožnost žadatele a určit, jestli se skutečně jedná o daný Subjekt údajů. Při rozhodování o tom, jakým způsobem bude totožnost žadatele ověřena, je Osoba pověřená kontrolou zpracování osobních údajů povinna brát v potaz možné riziko újmy, která by skutečnému Subjektu údajů mohla vzniknout, kdyby se jeho práv dovolala osoba jiná.
- (6) Pokud Osoba pověřená kontrolou zpracování osobních údajů usoudí, že nemá dostatek údajů k tomu, aby mohla žadatele bezpečně identifikovat, je povinna žadatele vyzvat, aby svou totožnost doložil jinými informacemi, a v krajním případě, aby se dostavil osobně do sídla Společnosti a identifikoval se předložením průkazu totožnosti. Pokud ani po této výzvě není Osoba pověřená kontrolou zpracování osobních údajů schopna žadatele bezpečně identifikovat, je oprávněna žádost odmítnout a výkon práva neumožnit.
- (7) Pokud Osoba pověřená kontrolou zpracování osobních údajů bezpečně ověřila totožnost žadatele, je povinna přistoupit k prověření žádosti.

2.3.1.3 Prověření a vyřízení žádosti

- (1) Osoba pověřená kontrolou zpracování osobních údajů je povinna důkladně žádost prověřit. Pokud k tomu nemá sama dostatek informací, je oprávněna požádat o součinnost jakéhokoliv pracovníka Společnosti nebo vyzvat žadatele k doplnění, upřesnění nebo vysvětlení žádosti.
- (2) Při prověřování a vyřizování žádostí postupuje Osoba pověřená kontrolou zpracování osobních údajů zejména dle pravidel a postupů uvedených v čl. 2.3.2 tohoto předpisu.
- (3) Osoba pověřená kontrolou zpracování osobních údajů je povinna žádost prověřit bez zbytečného odkladu a nejpozději do jednoho měsíce od obdržení žádosti rozhodnout právě jedním z následujících způsobů:
 - a) žádosti vyhovět a provést nutná opatření či úkony,
 - b) žádost odmítnout pro její zjevnou nedůvodnost nebo nepřiměřenost,
 - c) žádost odmítnout pro nesplnění předpokladů pro její kladné vyřízení, nebo
 - d) prodloužit o nejvýše dva měsíce lhůtu pro vyhovění žádosti (pouze ale v případě potřeby a s ohledem na složitost dané žádosti a počtu obdržených žádostí od stejného žadatele).
- (4) V případě rozhodnutí uvedeného v bodě (3) písm. a) tohoto článku je Osoba pověřená kontrolou zpracování osobních údajů povinna informovat žadatele o tom, že jeho žádosti bylo vyhověno, a o provedených opatřeních či úkonech.
- (5) V případě rozhodnutí uvedeného v bodě (3) písm. b) tohoto článku je Osoba pověřená kontrolou zpracování osobních údajů povinna informovat žadatele o odmítnutí žádosti, o důvodech, proč spatřuje žádost zjevně nedůvodnou nebo nepřiměřenou.
- (6) V případě rozhodnutí uvedeného v bodě (3) písm. c) tohoto článku je Osoba pověřená kontrolou zpracování osobních údajů povinna informovat žadatele o odmítnutí žádosti, o důvodech odmítnutí.
- (7) V případě rozhodnutí uvedeného v bodě (3) písm. d) tohoto článku je Osoba pověřená kontrolou zpracování osobních údajů povinna informovat žadatele o tomto prodloužení a o jeho důvodech. V prodloužené lhůtě může Osoba pověřená kontrolou zpracování osobních údajů rozhodnout již jen způsobem uvedeným v bodě (3) písm. a) tohoto článku.

2.3.2 Zvláštní pravidla a postupy vztahující se k jednotlivým uplatňovaným právům

2.3.2.1 Právo na přístup k Osobním údajům

- (1) V rámci uplatňování tohoto práva může Subjekt údajů požadovat po Společnosti informaci, zda Společnost zpracovává Osobní údaje, které se ho týkají, či nikoliv.
- (2) Pokud Společnost skutečně Osobní údaje žadatele zpracovává, má žadatel dále právo obdržet kopie zpracovávaných Osobních údajů a také následující informace o Zpracování:
 - a) účely Zpracování;
 - b) kategorie dotčených Osobních údajů;
 - c) příjemci nebo kategorie příjemců, kterým Osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v Mezinárodních organizacích;
 - d) plánovaná doba, po kterou budou Osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
 - e) existence práva požadovat od Společnosti opravu nebo výmaz Osobních údajů týkajících se žadatele nebo omezení jejich Zpracování anebo vznést námitku proti tomuto Zpracování;

- f) právo podat stížnost u Úřadu;
 - g) veškeré dostupné informace o zdroji Osobních údajů, pokud nebyly získány přímo od žadatele;
 - h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového Zpracování pro žadatele;
 - i) pokud se Osobní údaje předávají do třetí země nebo Mezinárodní organizaci, informace o vhodných zárukách podle čl. 46 Nařízení GDPR, které se vztahují na předání.
- (3) Právo žadatele obdržet kopie zpracovávaných Osobních údajů může být omezeno nebo dokonce i odepřeno, pokud by neomezením nebo neodepřením byla nepříznivě dotčena práva a svobody jiných osob (např. obchodní tajemství Společnosti nebo Osobní údaje dalších fyzických osob).

2.3.2.2 Právo na opravu Osobních údajů

- (1) V rámci uplatňování tohoto práva může Subjekt údajů po Společnosti požadovat, aby opravila Osobní údaje, které se ho týkají (např. z důvodu jejich nepřesnosti). V případě takové žádosti je Osoba pověřená kontrolou zpracování osobních údajů povinna ověřit přesnost údajů a po dobu tohoto ověřování je povinna zajistit omezení Zpracování těchto Osobních údajů (blíže viz čl. 2.3.2.4 tohoto předpisu).
- (2) V rámci uplatňování tohoto práva může Subjekt údajů dále požadovat doplnění neúplných Osobních údajů, ale pouze v případě, že tím nebude Společnost nucena zpracovávat Osobní údaje, které nejsou potřebné pro dané účely Zpracování.
- (3) Osoba pověřená kontrolou zpracování osobních údajů je povinna zajistit, že jednotliví příjemci, jimž byly opravované Osobní údaje zpřístupněny, budou o těchto opravách informováni, ledaže by se to ukázalo jako nemožné nebo by to vyžadovalo nepřiměřené úsilí.
- (4) V případě, že to Subjekt údajů požaduje, je Osoba pověřená kontrolou zpracování osobních údajů povinna informovat žadatele o všech příjemcích uvedených v bodě (3) tohoto článku.

2.3.2.3 Právo na výmaz Osobních údajů

- (1) V rámci uplatňování tohoto práva může Subjekt údajů po Společnosti požadovat, aby vymazala Osobní údaje, které se ho týkají. Společnost je ale povinna takové žádosti vyhovět pouze v případě, že existuje alespoň jeden z důvodů uvedených v bodě (2) tohoto článku a zároveň nelze aplikovat ani jednu z výjimek uvedených v bodě (3) tohoto článku.
- (2) Důvody pro výmaz Osobních údajů jsou následující:
- a) Osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
 - b) žadatel odvolal souhlas se Zpracováním Osobních údajů, na jehož základě byly Osobní údaje zpracovány, a neexistuje žádný další právní důvod pro jejich Zpracování;
 - c) žadatel zároveň vznesl námitku proti Zpracování Osobních údajů podle čl. 21 odst. 1 Nařízení GDPR a neexistují žádné převažující oprávněné důvody pro jejich Zpracování (blíže viz čl. 2.3.2.6 tohoto předpisu);
 - d) žadatel vznesl námitku proti Zpracování Osobních údajů podle čl. 21 odst. 2 Nařízení GDPR (blíže viz čl. 2.3.2.6 tohoto předpisu);
 - e) Osobní údaje byly zpracovány protiprávně;
 - f) na Společnost se vztahuje povinnost Osobní údaje vymazat stanovená právem Evropské unie nebo právem členského státu Evropské unie;
 - g) jedná se o Osobní údaje dítěte, která byly shromážděny v souvislosti s nabídkou služeb informační Společnosti.

- (3) Výjimky z povinnosti vymazat Osobní údaje jsou následující:
- Zpracování Osobních údajů je nezbytné pro výkon práva na svobodu projevu a informace;
 - Zpracování Osobních údajů je nezbytné pro splnění právní povinnosti, jež vyžaduje Zpracování podle práva Evropské unie nebo členského státu Evropské unie, které se na Společnost vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Společnost pověřena;
 - Zpracování Osobních údajů je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3 Nařízení GDPR;
 - Zpracování Osobních údajů je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1 Nařízení GDPR, pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo splnění cílů uvedeného Zpracování;
 - Zpracování Osobních údajů je nezbytné pro určení, výkon nebo obhajobu právních nároků.
- (4) V případě, že Společnost Osobní údaje zveřejnila a následně je v rámci uplatňovaného práva na výmaz povinna tyto Osobní údaje vymazat, je Osoba pověřená kontrolou zpracování osobních údajů povinna s ohledem na dostupnou technologii a náklady na provedení, včetně technických opatření, zajistit informování Správců, kteří tyto Osobní údaje zpracovávají, že po nich žadatel požaduje, aby vymazali veškeré odkazy na tyto Osobní údaje, jejich kopie či replikace.
- (5) Osoba pověřená kontrolou zpracování osobních údajů je povinna zajistit, že jednotliví příjemci, jimž byly vymazávané Osobní údaje zpřístupněny, budou o těchto výmazech informováni, ledaže by se to ukázalo jako nemožné nebo by to vyžadovalo nepřiměřené úsilí.

2.3.2.4 Právo na omezení Zpracování

- (1) V rámci uplatňování tohoto práva může Subjekt údajů po Společnosti požadovat, aby omezila Zpracování Osobních údajů, které se ho týkají. Společnost je ale povinna takové žádosti vyhovět pouze v případě, že existuje alespoň jeden z důvodů uvedených v bodě (2) tohoto článku.
- (2) Důvody pro omezení Zpracování Osobních údajů jsou následující:
- žadatel zároveň popírá přesnost Osobních údajů (blíže viz čl. 2.3.2.2 tohoto předpisu);
 - Zpracování je protiprávní, ale žadatel odmítá výmaz Osobních údajů a místo toho žádá jen o omezení jejich použití;
 - Společnost již Osobní údaje nepotřebuje pro účely Zpracování, ale žadatel je požaduje pro určení, výkon nebo obhajobu právních nároků;
 - žadatel zároveň vznesl námitku proti Zpracování podle čl. 21 odst. 1 Nařízení GDPR (blíže viz čl. 2.3.2.6. tohoto předpisu).
- (3) Pokud Osoba pověřená kontrolou zpracování osobních údajů v rámci prověřování žádosti dospěje k závěru, že důvod pro omezení Zpracování existuje, je povinna zajistit, že Osobní údaje budou označeny a nebudou dále Společností zpracovávány (tzn. ani vymazány). Jedinou povolenou operací Zpracování je uložení.
- (4) Ze zákazu dalšího Zpracování označených Osobních údajů (tj. Osobních údajů, jejichž Zpracování bylo omezeno) uvedeného v bodě (3) tohoto článku existují následující výjimky:
- žadatel s dalším Zpracování Osobních údajů souhlasí;
 - další Zpracování Osobních údajů je nezbytné pro určení, výkon nebo obhajobu právních nároků;
 - další Zpracování Osobních údajů je nezbytné pro ochranu práv jiné fyzické osoby nebo právnické osoby;

- d) další Zpracování Osobních údajů je nezbytné z důvodu důležitého veřejného zájmu Evropské unie nebo některého členského státu Evropské unie.
- (5) Omezení Zpracování provedené z důvodu uvedeného v bodě (2) písm. a) tohoto článku trvá do okamžiku rozhodnutí o žádosti na opravu Osobních údajů (tzn. vyhovění žádosti a provedení opravy Osobních údajů nebo odmítnutí žádosti).
 - (6) Omezení Zpracování provedené z důvodu uvedeného v bodě (2) písm. b) tohoto článku trvá do okamžiku, kdy žadatel požádá o výmaz Osobních údajů nebo o zrušení omezení Zpracování.
 - (7) Omezení Zpracování provedené z důvodu uvedeného v bodě (2) písm. c) tohoto článku trvá do okamžiku, kdy žadatel požádá o zrušení omezení Zpracování.
 - (8) Omezení Zpracování provedené z důvodu uvedeného v bodě (2) písm. d) tohoto článku trvá do okamžiku rozhodnutí o vznesené námitce proti Zpracování (tzn. vyhovění žádosti nebo odmítnutí žádosti).
 - (9) Osoba pověřená kontrolou zpracování osobních údajů je povinna předem upozornit žadatele, že bude omezení Zpracování zrušeno.
 - (10) Osoba pověřená kontrolou zpracování osobních údajů je povinna zajistit, že jednotliví příjemci, jimž byly zpřístupněny Osobní údaje, jejichž Zpracování bylo omezeno, budou o tomto omezení Zpracování informováni, ledaže by se to ukázalo jako nemožné nebo by to vyžadovalo nepřiměřené úsilí.

2.3.2.5 Právo na přenositelnost údajů

- (1) V rámci uplatňování tohoto práva může Subjekt údajů po Společnosti požadovat, aby mu předala (případně umožnila stáhnout) Osobní údaje, které se ho týkají a které poskytl Společnosti, ve strukturovaném, běžně používaném a strojově čitelném formátu, a dále aby Společnost tyto Osobní údaje přímo poskytla jinému Správci.
- (2) Společnost je povinna takové žádosti vyhovět jen v případě, že Zpracování těchto Osobních údajů je založeno na souhlasu žadatele nebo na smlouvě uzavřené se žadatelem (blíže viz čl. 2.1.2 tohoto předpisu), a zároveň se Zpracování těchto Osobních údajů provádí automatizovaně (tzn., neprovádí se manuálně).
- (3) Společnost je povinna vyhovět žádosti o přímé poskytnutí Osobních údajů jinému Správci pouze v případě, že je to technicky proveditelné.
- (4) Právo žadatele na přenositelnost údajů může být omezeno nebo dokonce i odepřeno, pokud by neomezením nebo neodepřením byla nepříznivě dotčena práva a svobody jiných osob (např. obchodní tajemství Společnosti nebo Osobní údaje dalších fyzických osob).

2.3.2.6 Právo vznést námitku

- (1) V rámci uplatňování tohoto práva může Subjekt údajů po Společnosti požadovat, aby dále nezpracovávala Osobní údaje, které se ho týkají (tzn. vznést námitku proti Zpracování Osobních údajů). Existují tři druhy těchto námitek:
 - a) námitka proti Zpracování Osobních údajů na základě právního titulu oprávněného zájmu nebo plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci;

- b) námitka proti Zpracování Osobních údajů pro účely přímého marketingu na základě právního titulu oprávněného zájmu;
 - c) námitka proti Zpracování Osobních údajů pro účely vědeckého či historického výzkumu nebo pro statistické účely.
- (2) V případě podání námítky uvedené v bodě (1) písm. a) tohoto článku je Osoba pověřená kontrolou zpracování osobních údajů povinna posoudit, zda skutečně existují závažné oprávněné důvody Společnosti pro Zpracování, které převažují nad konkrétními zájmy nebo právy a svobodami žadatele. Při tomto posuzování vychází Osoba pověřená kontrolou zpracování osobních údajů především z interní analýzy uvedené v příloze č. 1 tohoto předpisu, která se vztahuje k příslušnému oprávněnému zájmu (viz také čl. 2.1.2 bod (6) tohoto předpisu).
Pokud Osoba pověřená kontrolou zpracování osobních údajů dospěje k závěru, že závažné oprávněné důvody Společnosti pro Zpracování nepřevažují nad konkrétními zájmy nebo právy a svobodami žadatele, je povinna vznesené námitce vyhovět a zajistit, že pro daný účel již Osobní údaje žadatele nebude Společnost dále zpracovávat. Pokud ale Osoba pověřená kontrolou zpracování osobních údajů dospěje k závěru, že závažné oprávněné důvody Společnosti pro Zpracování převažují nad konkrétními zájmy nebo právy a svobodami žadatele, je oprávněna vznesenou námitku s náležitým odůvodněním odmítnout, a Společnost je oprávněna Osobní údaje žadatele pro daný účel zpracovávat i nadále.
- (3) V případě podání námítky uvedené v bodě (1) písm. b) tohoto článku je Osoba pověřená kontrolou zpracování osobních údajů povinna bez zbytečného odkladu zajistit, že Osobní údaje žadatele nebudou již pro účely přímého marketingu zpracovávány.
- (4) V případě podání námítky uvedené v bodě (1) písm. c) tohoto článku je Osoba pověřená kontrolou zpracování osobních údajů povinna vznesenou námitku jako zjevně nedůvodnou odmítnout, protože Společnost nezpracovává Osobní údaje pro účely vědeckého či historického výzkumu nebo pro statistické účely.

2.4 Spolupráce se Zpracovateli

- (1) Společnost nesmí pověřit Zpracováním Osobních údajů ty Zpracovatele, kteří neposkytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané Zpracování splňovalo požadavky Nařízení GDPR a aby byla zajištěna ochrana práv Subjektů údajů.
- (2) Vedoucí pracovník Společnosti, který v rámci svých pracovních povinností má za úkol vyhledávat potenciální Zpracovatele pro určité operace Zpracování, navazovat s nimi spolupráci a následně působit jako kontaktní osoba pro tyto Subjekty (dále jen „**Kontaktní osoba**“), je povinen plnit dále uvedené povinnosti.
- (3) Kontaktní osoba je povinna vyžádat si od potenciálního Zpracovatele informace a dokumenty popisující jím zavedená technická a organizační opatření v oblasti Zpracování a ochrany Osobních údajů. Tato opatření je Kontaktní osoba povinna prověřit zejména s ohledem na jejich soulad s Nařízením GDPR a konkrétním předmětem plánované spolupráce se Zpracovatelem. Při tomto prověřování je Kontaktní osoba povinna přihlížet zejména k povaze, rozsahu, kontextu a účelům Zpracování, ke kterým by měl být daný Zpracovatel pověřen, a dále k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jejichž Osobní údaje by měl Zpracovatel zpracovávat. Kontaktní osoba je při tomto prověřování oprávněna požádat o součinnost nebo vyjádření Osoby pověřené kontrolou zpracování osobních údajů, je pak ale povinna postupovat v souladu s vyjádřením nebo doporučením Osoby pověřené kontrolou zpracování osobních údajů.
- (4) Výsledkem tohoto prověřování je buď závěr, že potenciální Zpracovatel poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření, pak je možné daného potenciálního

Zpracovatele pověřit Zpracováním, nebo že potenciální Zpracovatel neposkytuje dostatečné záruky zavedení vhodných technických a organizačních opatření, pak daného potenciálního Zpracovatele nelze pověřit Zpracováním.

- (5) V případě, že potenciálního Zpracovatele lze pověřit Zpracováním, je povinností Kontaktní osoby zajistit, že mezi daným potenciálním Zpracovatelem a Společností bude uzavřena smlouva o Zpracování Osobních údajů v souladu s čl. 28 Nařízení GDPR. Vzorovou smlouvu o Zpracování Osobních údajů poskytne Kontaktní osobě Osoba pověřená kontrolou zpracování osobních údajů, která je také povinna poskytnout Kontaktní osobě potřebnou součinnost při následné konkretizaci smlouvy a při procesu jejího uzavírání se Zpracovatelem.
- (6) Kontaktní osoba je povinna vést důkladné záznamy o výše popsaném prověřování potenciálních Zpracovatelů včetně odůvodněných závěrů takového prověřování.
- (7) Kontaktní osoba je také povinna dohlížet na to, aby Zpracovatel dodržoval všechny povinnosti stanovené mu uzavřenou smlouvou o Zpracování Osobních údajů.

2.5 Zabezpečení Zpracování Osobních údajů

- (1) Společnost je povinna provést vhodná technická a organizační opatření, aby zajistila odpovídající úroveň zabezpečení Osobních údajů, které zpracovává.
- (2) Všichni pracovníci Společnosti jsou povinni dodržovat příkazy a zákazy stanovené těmito technickými a organizačními opatřeními.
- (3) Základní technická opatření jsou stanovena ve zvláštních vnitřních předpisech Společnosti². Další specifická technická opatření jsou oprávněni v konkrétních případech nebo oblastech Zpracování stanovit vedoucí pracovníci Společnosti nebo Osoba pověřená kontrolou zpracování osobních údajů. Tato specifická technická opatření musí být stanovena s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům Zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jejichž Osobní údaje Společnost zpracovává. Při posuzování vhodné úrovně bezpečnosti je povinností výše uvedených osob zohlednit zejména rizika spojená se Zpracováním Osobních údajů (např. náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných Osobních údajů, nebo neoprávněný přístup k nim).
- (4) Základní organizační opatření jsou stanovena tímto předpisem a dalšími vnitřními předpisy Společnosti³. Další specifická organizační opatření jsou oprávněni v konkrétních případech nebo oblastech Zpracování stanovit vedoucí pracovníci Společnosti nebo Osoba pověřená kontrolou zpracování osobních údajů. Tato specifická organizační opatření musí být stanovena s přihlédnutím k nákladům na provedení, povaze, rozsahu, kontextu a účelům Zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jejichž Osobní údaje Společnost zpracovává.

² Vnitřní předpis Společnosti „Řád správy informačního systému“

³ Vnitřní předpis Společnosti „Organizační řád“; „Spisový a skartační řád“

2.6 Porušení zabezpečení Osobních údajů

Porušením zabezpečení Osobních údajů se rozumí takové porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných Osobních údajů.

- (1) Každý pracovník Společnosti, který zjistí nebo se dozví o možném porušení zabezpečení Osobních údajů, je povinen neprodleně (nejpozději do 24 hodin) informovat Osobu pověřenou kontrolou zpracování osobních údajů a poskytnout jí všechny potřebné informace a doklady s tímto podezřením související.
- (2) Kontaktní osoba, které bylo možné porušení zabezpečení Osobních údajů v souladu s čl. 33 odst. 2 Nařízení GDPR ohlášeno ze strany Zpracovatele, je povinna také neprodleně (nejpozději do 12 hodin) informovat Osobu pověřenou kontrolou zpracování osobních údajů a poskytnout jí všechny informace a doklady získané v této souvislosti od Zpracovatele.
- (3) V příloze č. 4 tohoto předpisu jsou uvedeny příklady porušení zabezpečení Osobních údajů.

2.7 Posouzení vlivu na ochranu Osobních údajů

- (1) V případě, že by Společnost hodlala zahájit určitý druh Zpracování (zejména při využití nových technologií), u kterého by bylo pravděpodobné, že s přihlédnutím k povaze, rozsahu, kontextu a účelům Zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, je jednatel Společnosti povinen zajistit, že dojde nejprve k důkladnému a zdokumentovanému posouzení vlivu zamýšlených operací Zpracování na ochranu Osobních údajů.
- (2) Provedení tohoto posouzení je nutné zejména v případech, kdy
 - a) Společnost hodlá provádět systematické a rozsáhlé vyhodnocování Osobních aspektů týkajících se fyzických osob, které by bylo založeno na automatizovaném Zpracování, včetně profilování, a na němž by se zakládala rozhodnutí, která by vyvolávala ve vztahu k fyzickým osobám právní účinky nebo by měla na fyzické osoby podobně závažný dopad;
 - b) Společnost hodlá rozsáhle zpracovávat Zvláštní kategorií údajů uvedených v čl. 9 odst. 1 Nařízení GDPR nebo Osobní údaje týkající se rozsudků v trestních věcech a trestných činů uvedených v čl. 10 Nařízení GDPR;
 - c) Společnost hodlá rozsáhle a systematicky monitorovat veřejně přístupné prostory;
 - d) Společnost hodlá provádět Zpracování, které Úřad označil za rizikové a je uvedeno ve zveřejněném seznamu druhů operací Zpracování, u nichž je provedení posouzení vlivu na ochranu Osobních údajů povinné.
- (3) Pokud jednatel Společnosti neuloží přímo Osobě pověřené kontrolou zpracování osobních údajů, aby toto posouzení provedla, tak je povinen požádat Osobu pověřenou kontrolou zpracování osobních údajů o vyjádření k zamýšlenému Zpracování a toto vyjádření musí být v posouzení zohledněno.
- (4) Dokumentace zachycující provedení tohoto posouzení musí obsahovat alespoň následující:
 - a) systematický popis zamýšlených operací Zpracování a účely Zpracování, případně včetně oprávněných zájmů Společnosti jako Správce;
 - b) posouzení nezbytnosti a přiměřenosti operací Zpracování z hlediska účelů;
 - c) posouzení rizik pro práva a svobody fyzických osob, k jejichž Osobním údajům se zamýšlené Zpracování vztahuje;

- d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany Osobních údajů a k doložení souladu s Nařízením GDPR, s přihlédnutím k právům a oprávněným zájmům Subjektů údajů a dalších dotčených osob.
- (5) Osoba pověřená kontrolou zpracování osobních údajů je povinna postupovat v této souvislosti také dle čl. 36 Nařízení GDPR (tzn. konzultovat zamýšlené Zpracování s Úřadem) a v souladu s Pokyny WP 29 č. 248 (Pokyny týkající se posouzení vlivu na ochranu údajů).

2.8 Předávání Osobních údajů do třetích zemí nebo Mezinárodním organizacím

- (1) Pro předávání Osobních údajů do třetích zemí (tzn. do zemí mimo Evropskou unii) nebo Mezinárodním organizacím platí přísná pravidla stanovená Kapitolou V Nařízení GDPR (čl. 44 až 50).
- (2) Pracovníkům Společnosti je tak přísně zakázáno umožnit předávání nebo dokonce přímo předávat Osobní údaje do třetích zemí nebo Mezinárodním organizacím.
- (3) Předání Osobních údajů do třetí země nebo Mezinárodní organizaci je povoleno jen ve výjimečných případech a po předchozím výslovném souhlasu jednatele Společnosti.
- (4) Společnosti je při rozhodování, zda tento souhlas udělí, povinen postupovat v souladu s Nařízením GDPR a Pokyny WP 29 č. 262 (Pokyny týkající se čl. 49 Nařízení GDPR), dále je povinen vyžádat si vyjádření Osoby pověřené kontrolou zpracování osobních údajů a řídit se jím, případně náležitě odůvodnit, proč se jím neřídí.

2.9 Likvidace Osobních údajů

- (1) Společnost je povinna zpracovávané Osobní údaje zlikvidovat (tzn. vymazat nebo anonymizovat), pokud pomine účel jejich Zpracování nebo pokud pro jejich Zpracování ztratí Společnost poslední právní titul.
- (2) jednatel Společnosti je povinen zajistit, že konkrétní pracovní postupy, při nichž dochází ke Zpracování Osobních údajů, budou na výše uvedenou obecnou povinnost Společnosti pamatovat a bude v jejich rámci pracovníkům Společnosti stanovena i povinnost likvidace Osobních údajů, pokud dojde k naplnění stanovených podmínek.
- (3) Společnost je také povinna Osobní údaje zlikvidovat, pokud to bude výsledkem uplatnění práva na výmaz ze strany Subjektu údajů (blíže viz čl. 2.3.2.3 tohoto předpisu).

2.10 Pravidelná školení v oblasti Osobních údajů

- (1) Každý pracovník Společnosti a spolupracující obchodní zástupce, který pro Společnost působí jako Zpracovatel, je povinen průběžně absolvovat školení v oblasti Zpracování Osobních údajů.
- (2) Každý pracovník Společnosti je oprávněn požádat Osobu pověřenou kontrolou zpracování osobních údajů o radu nebo součinnost týkající se problematiky Osobních údajů.

3. Dohled nad oblastí Zpracování Osobních údajů

3.1 Organizační zajištění dohledu

- (1) Osobu pověřenou kontrolou zpracování osobních údajů musí splňovat předpoklady pro tuto činnost:
 - a) má dostatečnou úroveň odborných znalostí, zejména detailní znalost Nařízení GDPR a veškerých souvisejících právních předpisů v oblasti ochrany Osobních údajů a detailní znalost právních předpisů dopadající na Společnost v souvislosti s její podnikatelskou činností;
 - b) má dostatečnou úroveň znalosti organizace Společnosti a jejího podnikání, zejména znalost vnitřních předpisů Společnosti, procesů ve Společnosti a informačních systémů, které Společnost používá;
 - c) má vysokou úroveň morálních, etických a profesních kvalit, zejména profesní bezúhonnost, komunikační a manažerské schopnosti, morální kredit;
 - d) není ve střetu zájmů, zejména se nepodílí na vlastní podnikatelské činnosti Společnosti.
- (2) Pro zajištění nepřetržitého a dostatečného dohledu nad oblastí Zpracování Osobních údajů je Osoba pověřená kontrolou zpracování osobních údajů povinna určit si svého zástupce, jehož úkolem je pomáhat Osobě pověřené kontrolou zpracování osobních údajů s jejími úkoly stanovenými tímto předpisem a zastupovat Osobě pověřené kontrolou zpracování osobních údajů během její nepřítomnosti. Při zastupování Osoby pověřené kontrolou zpracování osobních údajů během její nepřítomnosti má zástupce stejné povinnosti a pravomoci jako Osoba pověřená kontrolou zpracování osobních údajů.

3.2 Postavení, pravomoci a povinnosti Osoby pověřené kontrolou zpracování osobních údajů

- (1) Osoba pověřená kontrolou zpracování osobních údajů je samostatným a nezávislým pracovníkem přímo podřízeným jednatelem Společnosti, který má zejména poradní funkci a nenese za Zpracování Osobních údajů Společností odpovědnost.
- (2) Žádný pracovník Společnosti není oprávněn dávat Osobě pověřené kontrolou zpracování osobních údajů jakékoliv pokyny týkající se plnění jeho úkolů stanovených tímto předpisem. Pokud by Osoba pověřená kontrolou zpracování osobních údajů takový pokyn obdržela, je její povinností nebrat jej při plnění svých úkolů v potaz a oznámit tuto skutečnost jednatelem Společnosti.
- (3) Společnosti je povinen zajistit, aby Osoba pověřená kontrolou zpracování osobních údajů nebyla sankcionována (přímo i nepřímo) za plnění svých úkolů dle tohoto předpisu, ani ji z tohoto důvodu nesmí sám sankcionovat.
- (4) Společnosti je povinen zajistit, aby byla Osoba pověřená kontrolou zpracování osobních údajů náležitě a včas zapojena do veškerých záležitostí souvisejících s ochranou Osobních údajů, zejména,
 - a) aby byla s dostatečným předstihem zvána na jednání vedení Společnosti, pokud by se dané jednání mohlo dotýkat Osobních údajů;
 - b) aby jí byl s dostatečným předstihem předložen k vyjádření návrh jakéhokoliv rozhodnutí (např. rozhodnutí o vytvoření nového produktu, o nákupu nového nebo změně stávajícího informačního systému, o zahájení spolupráce s novým obchodním partnerem, o zavedení nového nebo změně stávajícího procesu), které by mohlo mít nějaký dopad na ochranu Osobních údajů, včetně podkladových materiálů, a aby bylo jeho vyjádření při rozhodování zohledněno nebo jeho nezohlednění náležitě odůvodněno;

- c) aby jí byl s dostatečným předstihem předložen k připomínkám návrh nového nebo návrh změn stávajícího vnitřního předpisu Společnosti, který souvisí se Zpracováním nebo ochranou Osobních údajů, a aby byly jeho připomínky zohledněny nebo jejich nezohlednění náležitě odůvodněno.
- (5) Společnosti je povinen zajistit, aby měla Osoba pověřená kontrolou zpracování osobních údajů pro plnění svých úkolů stanovených tímto předpisem dostatečné zdroje, zejména technické (např. přístup do všech potřebných informačních systémů), lidské (např. vlastní pracovní tým) a odborné (např. udržování a případně zvyšování odborné způsobilosti formou školení nebo dalšího vzdělávání).
- (6) Každý pracovník Společnosti je povinen poskytnout Osobě pověřené kontrolou zpracování osobních údajů potřebnou součinnost při plnění jejích úkolů stanovených tímto předpisem, pokud o ní požádá.
- (7) Osoba pověřená kontrolou zpracování osobních údajů je povinna při plnění svých úkolů stanovených tímto předpisem brát patřičný ohled na riziko spojené s operacemi Zpracování a současně přihlížet k povaze, rozsahu, kontextu a účelům Zpracování.
- (8) Osoba pověřená kontrolou zpracování osobních údajů je oprávněna vydávat při plnění svých úkolů stanovených tímto předpisem doporučení, kterými jsou ostatní pracovníci Společnosti povinni se řídit, ledaže by jednatel Společnosti rozhodl jinak a toto své rozhodnutí náležitě odůvodnil.
- (9) Osoba pověřená kontrolou zpracování osobních údajů je povinna zachovávat mlčenlivost ohledně všech informací, které získala v souvislosti s plněním svých úkolů.

3.3 Úkoly Osoby pověřené kontrolou zpracování osobních údajů

3.3.1 Monitorování souladu činností Společnosti s Nařízením GDPR

- (1) Osoba pověřená kontrolou zpracování osobních údajů průběžně sleduje a kontroluje, zda je dodržován tento předpis, Nařízení GDPR a další související právní předpisy. Při této činnosti je Osoba pověřená kontrolou zpracování osobních údajů oprávněna požadovat informace a dokumenty od jakéhokoliv pracovníka Společnosti.
- (2) V případě, že Osoba pověřená kontrolou zpracování osobních údajů zjistí nesoulad činností Společnosti s tímto předpisem, Nařízením GDPR či souvisejícími právními předpisy, je povinna o tom informovat jednatele Společnosti a poskytnout mu součinnost při zjednávání nápravy.

3.3.2 Poskytování poradenství, informací a součinnosti

- (1) Osoba pověřená kontrolou zpracování osobních údajů je povinna poskytovat informace, rady nebo součinnosti jakémukoliv pracovníkovi Společnosti, pokud je o to požádána a týká se to oblasti Zpracování nebo ochrany Osobních údajů.
- (2) Osoba pověřená kontrolou zpracování osobních údajů je povinna poskytnout součinnost jednatele Společnosti při vedení a aktualizaci záznamů o činnostech Zpracování (viz čl. 2.1.3 tohoto předpisu).

3.3.3 Prověření porušení zabezpečení Osobních údajů a související úkoly

- (1) V případě, že je Osoba pověřená kontrolou zpracování osobních údajů v souladu s čl. 2.6 tohoto předpisu informována o možném porušení zabezpečení Osobních údajů, je povinna toto oznámení důkladně a bezodkladně prozkoumat a učinit právě jeden z následujících závěrů:

- a) nedošlo k porušení zabezpečení Osobních údajů,
 - b) došlo k porušení zabezpečení Osobních údajů, ale je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob,
 - c) došlo k porušení zabezpečení Osobních údajů a je pravděpodobné, že by toto porušení mohlo mít za následek riziko pro práva a svobody fyzických osob,
 - d) došlo k porušení zabezpečení Osobních údajů a je pravděpodobné, že toto porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob.
- (2) O učiněném závěru a jeho odůvodnění je Osoba pověřená kontrolou zpracování osobních údajů povinna neprodleně informovat jednatele Společnosti.
- (3) Pokud je ze strany Osoby pověřené kontrolou zpracování osobních údajů učiněn závěr uvedený v bodě (1) písm. b), c) nebo d) tohoto článku, je povinností Osoby pověřené kontrolou zpracování osobních údajů navrhnout jednatele Společnosti nápravné opatření, aby ke stejnému porušení zabezpečení Osobních údajů již nemohlo v budoucnu dojít, případně i opatření ke zmírnění možných nepříznivých dopadů.
- (4) Pokud je ze strany Osoby pověřené kontrolou zpracování osobních údajů učiněn závěr uvedený v bodě (1) písm. c) nebo d) tohoto článku, je další povinností Osoby pověřené kontrolou zpracování osobních údajů ohlásit toto porušení zabezpečení Osobních údajů bez zbytečného odkladu Úřadu, a to, pokud je to možné, do 72 hodin poté, co se osoba, která Osobě pověřené kontrolou zpracování osobních údajů oznámila porušení zabezpečení Osobních údajů, o něm dozvěděla. Pokud není Osoba pověřená kontrolou zpracování osobních údajů z jakéhokoliv důvodu schopna dodržet výše uvedenou lhůtu, je povinna spolu s ohlášením uvést důvody tohoto nedodržení. Ohlášení musí obsahovat minimálně:
- a) popis povahy daného případu porušení zabezpečení Osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených Subjektů údajů a kategorií a přibližného množství dotčených záznamů Osobních údajů;
 - b) jméno a kontaktní údaje Osoby pověřené kontrolou zpracování osobních údajů;
 - c) popis pravděpodobných důsledků porušení zabezpečení Osobních údajů;
 - d) popis opatření, která Společnost přijala nebo hodlá přijmout s cílem vyřešit dané porušení zabezpečení Osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.
- (5) Pokud je ze strany Osoby pověřené kontrolou zpracování osobních údajů učiněn závěr uvedený v bodě (1) písm. d) tohoto článku, je další povinností Osoby pověřené kontrolou zpracování osobních údajů oznámit toto porušení zabezpečení Osobních údajů bez zbytečného odkladu všem Subjektům údajů, jichž se týká. V tomto oznámení je Osoba pověřená kontrolou zpracování osobních údajů povinna za použití jasných a jednoduchých jazykových prostředků popsat povahu porušení zabezpečení Osobních údajů a uvést v něm minimálně informace a opatření uvedené v bodě (4) písm. b), c) a d) tohoto článku.
- (6) Osoba pověřená kontrolou zpracování osobních údajů není povinna postupovat dle bodu (5) tohoto článku, pokud je splněna některá z následujících podmínek:
- a) v reakci na porušení zabezpečení Osobních údajů Společnost provedla okamžitá technická a organizační ochranná opatření a tato opatření byla použita u Osobních údajů dotčených porušením zabezpečení Osobních údajů (jedná se zejména o taková opatření, která učinila tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování);
 - b) v reakci na porušení zabezpečení Osobních údajů Společnost přijala okamžitá opatření, která zajistila, že hrozící vysoké riziko pro práva a svobody Subjektů údajů se pravděpodobně již neprojeví;
 - c) přímé oznámení všem Subjektům údajů by vyžadovalo nepřiměřené úsilí a zároveň bylo toto oznámení zveřejněno na internetových stránkách Společnosti.

- (7) Osoba pověřená kontrolou zpracování osobních údajů je povinna vést důkladnou dokumentaci všech oznámení o možném porušení zabezpečení Osobních údajů dle čl. 2.6 tohoto předpisu, dokumentaci prověřování těchto oznámení a učiněných závěrů včetně jejich odůvodnění, dokumentaci ohlašování Úřadu i oznamování Subjektům údajů, jakož i dokumentaci veškerých souvisejících navržených a přijatých nápravných opatřeních.
- (8) Osoba pověřená kontrolou zpracování osobních údajů je při plnění úkolů stanovených tímto článkem povinna postupovat také v souladu s Pokyny WP 29 č. 250 (Pokyny týkající se ohlašování případů porušení zabezpečení Osobních údajů).

3.3.4 Komunikace se Subjekty údajů

- (1) Osoba pověřená kontrolou zpracování osobních údajů je povinna v přiměřené lhůtě a odpovídajícím rozsahu reagovat na dotazy nebo žádosti Subjektů údajů, které jsou jí poslány nebo předány, a týkají se Zpracování nebo ochrany Osobních údajů.
- (2) Osoba pověřená kontrolou zpracování osobních údajů je také povinna plnit úkoly, které se týkají uplatňování práv Subjekty údajů a jsou mu stanoveny v čl. 2.3 tohoto předpisu.

3.3.5 Školení v oblasti Osobních údajů

- (1) Společnost je povinna zavést a udržovat aktuální školení pracovníků Společnosti v oblasti Osobních údajů.
- (2) Společnost je povinna kontrolovat, zda pracovníci toto školení absolvovali, a vyžadovat, aby jej absolvovali.

4. Závěrečná ustanovení

Tento vnitřní předpis může být aktualizován jednatelem Společnosti.

Tento vnitřní předpis je uložen v sídle Společnosti.

V Kroměříži dne 25. 5. 2018

Za KZ FINANCE, spol. s r.o.

Ing. Ivona Vojtušová
jednatel