KRAL&PARTNER
centrum pojištění

Pravidla ochrany osobních údajů

Směrnice č. A/10/2019
společnosti KRAL&PARTNER, s.r.o. se sídlem V Troskách 1238/29, 700 30, Ostrava, IČ: 26798042

je závazná pro všechny zaměstnance a vázané zástupce společnosti KRAL&PARTNER, s.r.o.

Shrnutí směrnice

Pravidla ochrany osobních údajů slouží jako návod pro zaměstnance a další osoby podílející se u Společnosti na zpracování osobních údajů fyzických osob. Tato pravidla jsou jedním z důležitých technických a organizačních opatření, jež Společnost implementovala s cílem zabezpečit náležitou ochranu osobních údajů.

Schvalování

Účinnost směrnice	25. 8. 2018	
Verze č. 3		
Garant: Ing. Michal Král	Funkce: Ředitel	1. 7. 2020
Ověřil: Hana Králová	Funkce: Jednatel	1. 7. 2020
Schválil: Hana Králová	Funkce: Jednatel	1. 7. 2020
Účinnost verze	1. 5. 2024	

Základní ustanovení

1. Pojmy

„*Informačním systémem Společnosti*“ se rozumí jakákoliv infrastruktura pro interní komunikaci a spolupráci uvnitř Společnosti;

„*Osobními údaji*“ se rozumí veškeré informace o Subjektu údajů, například jméno, identifikační číslo, lokační údaje, síťový identifikátor (IP adresa či cookies), údaje v personálním spisu, týkající se konkrétního zaměstnance, informace o pohybu dané osoby (GPS sledování), atp.;

„*Správcem*“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;

„*Subjektem údajů*“ se rozumí jakákoli identifikovaná či identifikovatelná 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;

„*Zpracovatelem*“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

„*Zpracováním*“ se rozumí 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;

2. Předmět a účel

Společnost vnímá ochranu osobních údajů jako nezbytnou součást udržitelného a odpovědného přístupu k jejím podnikatelským aktivitám. Za účelem zajištění náležité ochrany práv a svobod fyzických osob při zpracování osobních údajů těchto osob Společnost přijala tato pravidla ochrany osobních údajů (dále jen „**Pravidla**“), jež slouží jako návod pro zaměstnance a další osoby ve Společnosti podílející se na zpracování osobních údajů fyzických osob. Společnost plní své povinnosti při zpracování osobních údajů i prostřednictvím svých řádně proškolených zaměstnanců. Tato Pravidla jsou jedním z technických a organizačních opatření, jež Společnost implementovala pro zabezpečení ochrany osobních údajů, s nimiž Společnost nakládá.

Tato Pravidla dopadají na veškeré osobní údaje subjektů údajů zpracovávané Společností, bez ohledu na účel či právní titul (zákonný důvod) jejich zpracování. Tato Pravidla pojednávají o právech subjektů údajů, tedy jak o právech zaměstnanců Společnosti, tak i o jejich zákazníků, dodavatelů a obchodních partnerů dodavatelů a jiných osob, se kterými je Společnost v určitém vztahu či s nimi komunikuje.

Společnost ustanoví zaměstnance odpovědného za dodržování těchto Pravidel a ochranu osobních údajů v rámci Společnosti nebo jmenuje pověřence pro ochranu osobních údajů, vztahuje-li se na ni povinnost ustanovit pověřence. Odpovědný zaměstnanec bude mít k dispozici zdroje a pravomoci, které jsou přiměřeně potřebné pro zajištění zavedení a dodržování obecně závazných právních předpisů o ochraně osobních údajů a také jejich průběžné monitorování, podporu a školení.

3. Zásady zpracování osobních údajů

Společnost je při zpracování osobních údajů vázána obecně závaznými právními předpisy upravujícími ochranu osobních údajů, zejména 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 (obecné nařízení o ochraně osobních údajů) (dále jen „**Nařízení**“) a dalšími předpisy, které jsou nebo budou v souvislosti s ochranou osobních údajů přijaty, zejména, zákonem č. 110/2019 Sb., o zpracování osobních údajů („**Zákon**“).

Společnost zpracovává přesné a aktuální osobní údaje na základě zákonného titulu, korektně a transparentním způsobem, pouze pro určité, výslovně vyjádřené a legitimní účely, v minimálním nezbytném rozsahu, ukládá je ve formě umožňující identifikaci subjektů údajů pouze po nezbytnou dobu ve vztahu k účelu zpracování a zajišťuje jejich integritu a důvěrnost pomocí vhodných technických nebo organizačních opatření a náležitého zabezpečení před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

Společnost zajišťuje, aby nepřesné údaje s přihlédnutím k jejich účelu, pro který jsou zpracovávány, byly bezodkladně vymazány nebo opraveny.

Veškeré činnosti spojené s osobními údaji a jejich ochranou Společnost řádně dokumentuje, zejména vede záznamy o činnostech zpracování a další doklady o zpracování osobních údajů (např. evidence žádostí subjektů údajů uplatňujících svá práva vůči Společnosti, dokumentace souhlasů, dokumentace splnění informační povinnosti vůči subjektům údajů, apod.) pro naplnění zásady odpovědnosti dle Nařízení. Společnost spolupracuje s dozorovým úřadem, jímž je zejména Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7, e-mail: posta@uoou.cz, tel.: +420 234 665 111.

4. Postupy při zpracování osobních údajů

4.1. Prověrka osobních údajů a jejich zpracování

Společnost v souvislosti s přijetím Nařízení provedla kompletní prověrku a kontrolu osobních údajů, které zpracovává, a posoudila veškerá možná rizika ze zpracování vyplývající. Společnost i nadále v rámci zpracování osobních údajů a při implementaci nových procesů zpracování osobních údajů, bude zejména analyzovat, zda:

- ke zpracování dochází na základě zákonných důvodů;
- osobní údaje nejsou zpracovávány nad rámec právních předpisů;
- osobní údaje jsou zpracovávány po dobu nezbytnou k dosažení stanovených účelů, pro něž jsou zpracovávány;
- osobní údaje, které Společnost zpracovává, jsou skutečně potřebné pro její činnost (např. vedení kopií dokladů totožnosti zaměstnanců v osobním spisu; pořizování kamerových záznamů v provozovnách Společnosti;
- jsou upraveny vztahy s třetími osobami, které se účastní zpracování osobních údajů přímo či nepřímo se Společností (zejména, zda byly uzavřeny smlouvy o zpracování osobních údajů, zda byly ošetřeny závazky mezi společnými správci osobních údajů; zda jsou zaměstnanci a ostatní osoby nakládající s osobními údaji ve Společnosti vázány mlčenlivostí; zda je v případě přenosu osobních údajů do třetích zemí mimo EU zajištěna dostatečná ochrana osobních údajů i na území třetích zemí)
- byla přijata dostatečná technická a organizační opatření.

4.2. Stanovení účelu zpracování osobních údajů

Před zahájením jakéhokoli zpracování osobních údajů stanoví Společnost účel, pro který zpracovává osobní údaje. Takovým účelem je typicky uzavření smlouvy (včetně jednání směřujících k uzavření smlouvy) a plnění smlouvy se zákazníkem, vedení zaměstnanecké agendy, kontaktování potenciálních zákazníků za účelem nabídky produktů.

Za jakým účelem jsou osobní údaje subjektu údajů zpracovávány, se subjekt údajů dozví z informace, kterou mu Společnost individuálně předá (zašle) dle čl. 5 těchto Pravidel. Zpracování osobních údajů je po celou dobu prováděno výhradně v rozsahu a za účelem dosažení stanoveného účelu.

Jakmile je účel zpracování naplněn, Společnost osobní údaje v souladu se zásadou minimalizace údajů (zpracování přiměřené, relevantní, omezené na nezbytný rozsah ve vztahu k účelu zpracování) a omezení uložení vymaže, pokud je není třeba uchovávat pro jiný účel.

4.3. Vymezení rozsahu zpracovávaných osobních údajů

Společnost zpracovává osobní údaje pouze v rozsahu nezbytném pro naplnění předem stanoveného účelu. O tom, jaké konkrétní osobní údaje o daném subjektu údajů Společnost pro daný účel zpracovává, se subjekt údajů dozví z informace, kterou mu individuálně předá (zašle) Společnost dle čl. 5 těchto Pravidel.
Společnost může zpracovávat zvláštní kategorie osobních údajů (citlivé osobní údaje). Pokud by však Společnost potřebovala pro některý z účelů zpracovávat rovněž citlivé osobní údaje subjektů údajů, bude postupovat v souladu s článkem 9 Nařízení (např. bude zkoumat, zda existuje právními předpisy stanovená povinnost pro zpracování osobních údajů nebo si vyžádá výslovný souhlas subjektu údajů s takovým zpracováním).

4.4. Identifikace právního základu (důvodu) zpracování osobních údajů

Společnost zpracovává osobní údaje vždy na základě jednoho z právních základů vyjmenovaných v článku 6 Nařízení (právní základ pro zpracování). Nejčastěji uplatňovanými právními základy pro zpracování prováděná Společností jsou:

a) uzavření nebo plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
b) plnění právní povinnosti, která se na Společnost jako správce vztahuje;
c) oprávněný zájem Společnosti či třetí strany, který převažuje nad zájmy a základními právy a svobodami subjektu údajů vyžadujícími ochranu osobních údajů; nebo
d) souhlas subjektu údajů se zpracováním jeho osobních údajů.

O konkrétním právním základu zpracování osobních údajů se dotčený subjekt údajů dozví z informace, kterou mu Společnost individuálně předá (zašle) dle čl. 5 těchto Pravidel.

Oprávněný zájem Společnosti

Oprávněný zájem Společnosti určuje sama Společnost. Společnost předtím, než začne osobní údaje podle stanoveného oprávněného zájmu zpracovávat, porovná tento zájem s oprávněnými zájmy a základními právy a svobodami subjektů údajů, jejichž osobní údaje zpracovává (provede tzv. balanční test).
Pokud Společnost na základě výsledku balančního testu shledá, že může osobní údaje subjektu údajů zpracovávat na základě titulu oprávněného zájmu, informuje vždy subjekt údajů o této skutečnosti (tj. že

zpracovává údaje na základě oprávněného zájmu) v rámci informace dle čl. 5 těchto Pravidel a sdělí mu, na základě jakého konkrétního oprávněného zájmu tak činí.
Je-li základem pro zpracování osobních údajů subjektu údajů oprávněný zájem Společnosti, je subjekt údajů oprávněn vznést námitku (podrobně viz čl. 5.7 těchto Pravidel) a žádat výmaz (podrobně viz čl. 5.4 těchto Pravidel). O těchto právech je subjekt údajů informován v rámci informace dle čl. 5 těchto Pravidel, a to nejpozději v okamžiku první komunikace Společnosti se subjektem údajů.
Společnost zpracovává osobní údaje na základě oprávněných zájmů, jako je například předcházení trestným činům a přestupkům, ochrana majetku, ochrana zdraví a bezpečnost osob, vymáhání právních nároků, přímý marketing (pokud Společnost zpracovává osobní údaje pro účely splnění smlouvy, jejíž smluvní stranou je subjekt údajů, je oprávněna informovat subjekt údajů o zboží nebo službách a zasílat obchodní sdělení na e-mailovou adresu uvedenou subjektem údajů), aj.

Souhlas se zpracováním osobních údajů

Souhlas subjektu údajů se zpracováním jeho osobních údajů může být udělen pro jeden nebo více konkrétních účelů – **tento titul využívá Společnost pouze v těch případech, kdy není oprávněna zpracovávat osobní údaje na základě jiného právního základu**.
Souhlas subjektu údajů se zpracováním jeho osobních údajů využívá Společnost zejména pro pro marketingové účely Společnosti.
Souhlas se zpracováním osobních údajů může subjekt kdykoli odvolat. Pokud subjekt údajů svůj souhlas se zpracováním odvolá, neznamená to, že by zpracování osobních údajů před takovým odvoláním bylo nezákonné – odvolání souhlasu nemá zpětný účinek a zpracování osobních údajů vycházející z tohoto souhlasu před jeho odvoláním jím není dotčeno. O této skutečnost je subjekt údajů informován před tím, než vyjádří souhlas se zpracováním osobních údajů.
Příklady neplatného souhlasu:
Společnost požádá své zákazníky zároveň o souhlas se zasíláním reklamních e-mailů a se sdílením jejich osobních údajů s dalšími společnostmi v rámci skupiny. Takový souhlas není vrstevnatý, jelikož se nejedná o oddělené souhlasy pro dva různé účely, a proto je takový souhlas neplatný.
Rolování nebo procházení obchodními podmínkami, které obsahují prohlášení o souhlasu (kdy na obrazovce vyskakuje upozornění, že další procházení bude znamenat souhlas) není v souladu s požadavkem jasného a jednoznačného potvrzení. Subjekt údajů totiž při rychlém rolování rozsáhlým textem může toto upozornění přehlédnout a takové potvrzení by pak nebylo dostatečně jednoznačné.
Souhlas udělený v rámci všeobecných obchodních podmínek je neplatný.
Příklad nesprávného postupu při odvolání souhlasu:
Správce prodává své výrobky přes internet. Při prodeji každého výrobku je vyžadován souhlas s použitím kontaktních údajů pro pokročilé marketingové aktivity správce (přesahující rámec obchodních sdělení v souvislosti s prodejem výrobků). K vyjádření souhlasu pro tento účel mohou zákazníci zvolit buď NE nebo ANO. Správce zákazníky informuje, že mají možnost souhlas odvolat. K tomu mohou bezplatně kontaktovat call centrum v pracovní dny mezi 8.00 a 17.00 hod. Odvolání souhlasu zde vyžaduje telefonický hovor během pracovní doby, je to tedy pro subjekty údajů náročnější než jedno kliknutí myší, kterého bylo potřeba pro udělení souhlasu u internetového prodejce dostupného 24 hodin každý den v týdnu. ***Souhlas by měl být odvolatelný stejně jednoduše, jako byl udělen, tedy v daném případě by měla být možnost odvolat souhlas rovněž přes internet, případně e-mail****.*

4.5. Určení způsobů a prostředků zpracování osobních údajů

Společnost zpracovává osobní údaje nejčastěji v elektronické podobě neautomatizovaným způsobem (zejména osobní údaje zákazníků a dodavatelů) a rovněž v tištěné podobě neautomatizovaným způsobem (zejména pracovněprávní dokumentaci).

Společnost přijala či přijme technická a organizační opatření k ochraně osobních údajů popsaná v těchto Pravidlech a vnitřních procesních směrnicích či opatřeních nebo pokynech Společnosti a osobní údaje vždy dostatečně zabezpečuje a chrání před jejich zpřístupněním neoprávněným osobám – podrobněji k zabezpečení viz čl. **Chyba! Nenalezen zdroj odkazů.** těchto Pravidel.

4.6. Stanovení doby zpracování osobních údajů

Společnost vždy zpracovává osobní údaje po dobu přiměřenou a potřebnou k naplnění účelu zpracování osobních údajů. Doba zpracování osobních údajů je vždy určena individuálně a o její délce je subjekt osobních údajů informován také individuálně. Nad rámec takto stanovené doby je Společnost oprávněna zpracovávat osobní údaje subjektu údajů po dobu stanovenou zvláštními právními předpisy nebo po dobu potřebnou k vymáhání práv Společnosti vůči subjektu údajů. Konkrétní dobu, po kterou budou osobní údaje daného subjektu údajů zpracovávány, se subjekt údajů dozví z informace, kterou mu individuálně předá (zašle) Společnost dle čl. 5 těchto Pravidel.

Jakmile je účel zpracování osobních údajů naplněn a Společnost již nemá žádný další účel, pro který by je byla oprávněna zpracovávat, provádí Společnost výmaz osobních údajů. V případě osobních údajů zpracovávaných pouze na základě souhlasu subjektu údajů Společnost provede výmaz osobních údajů také v případě, kdy subjekt údajů svůj souhlas se zpracováním osobních údajů odvolá. Pokud jsou osobní údaje zpracovávány z titulu oprávněného zájmu a subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování, Společnost rovněž osobní údaje vymaže, poté co o tom subjekt údajů informuje.

5. Práva subjektů údajů

Každý subjekt údajů má následující práva:

a) Právo na informace
b) Právo na přístup k osobním údajům
c) Právo na opravu
d) Právo na výmaz (právo být zapomenut)
e) Právo na omezení zpracování
f) Právo na přenositelnost údajů
g) Právo vznést námitku
h) Právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování
i) Právo podat stížnost k Úřadu pro ochranu osobních údajů nebo k jinému příslušnému dozorovému úřadu v souvislosti se zpracováním osobních údajů.

Kde a jak uplatnit práva subjektu údajů?

Práva uvedená výše ad a) – h) může subjekt údajů uplatnit vůči Společnosti:

a) elektronicky na e-mailové adrese, kterou používá pro komunikaci ze Společností (kupř. emailová adresa příslušného zaměstnance Společnosti, tzv. správce klienta);
b) telefonicky na čísle, které používá pro komunikací ze Společností (kupř. telefonní číslo příslušného zaměstnance Společnosti, tzv. správce klienta);
c) u pověřence pro ochranu osobních údajů, byl-li ve Společnosti jmenován; nebo
d) písemně na adrese sídla Společností.

Společnost stanoví postupy, které usnadní výkon práv subjektů údajů a rovněž zajistí podmínky pro to, aby žádosti mohly být podávány elektronicky, zejména v případě zpracování osobních údajů elektronickými prostředky. Postup, který Společnost stanoví pro subjekty údajů k výkonu jejich práv, by měl odpovídat kontextu a povaze vztahu a komunikaci mezi Společností a subjektem údajů. Proto Společnost může dojít k závěru, že poskytne několik různých postupů pro výkon práv, které budou zohledňovat různé způsoby komunikace mezi subjekty údajů a Společností.
S cílem usnadnit výkon práv subjektů údajů Společnost zveřejňuje na svých internetových stránkách vzorové žádosti o uplatnění jednotlivých práv subjekty údajů. Pokud ale subjekt údajů nepoužije vzorovou žádost, neznamená to, že by své právo řádně neuplatnil.
Při ústním vyřizování žádosti subjektu údajů nebo poskytování informací (např. telefonicky) Společnost také zajistí, aby měla záznam a mohla doložit (pro účely prokázání souladu s požadavkem odpovědnosti): (i) žádost o informaci v mluvené podobě (ii) metodu ověření totožnosti subjektu údajů a (iii) skutečnost, že informace byla subjektu údajů poskytnuta. Pokud žádost subjektu údajů vyřizuje nebo informace poskytuje příslušný zaměstnanec Společnosti, o požadavku subjektu údajů neprodleně sepíše záznam a zároveň o tomto informuje vedoucího pracovníka společnosti (tedy, ředitele příslušného oddělení či příslušné pobočky).

Příklady k obsahu informační povinnosti:
Pokud z důvodu využití různých zdrojů nemůže být subjektu údajů sdělen původ osobních údajů, měly by být poskytnuty alespoň obecné informace.

V případě, kdy by poskytnutí informace subjektu údajů vyžadovalo nepřiměřené úsilí, je tomto ohledu třeba vzít v úvahu počet subjektů údajů, stáří dat a jakékoliv náležité záruky, jež byly přijaty.

Příklady nepřípustného postupu při informování subjektů údajů o jejich právu podat žádost:
Společnost na svém webu vyvěsí prohlášení, v němž sdělí všem subjektům údajů, aby se žádostmi o přístup k osobním údajům kontaktovaly zákaznickou službu. Takový potup by nebyl správný, protože správce měl rovněž zajistit podmínky pro to, aby žádosti mohly být podávány elektronicky, zejména v případě zpracování osobních údajů elektronickými prostředky.

Právo uvedené výše ad i) může subjekt uplatnit u Úřadu pro ochranu osobních údajů:

a) elektronicky na e-mailové adrese posta@uoou.cz;
b) prostřednictvím datové schránky ID: qkbaa2n;
c) telefonicky na čísle +420 234 665 111; nebo
d) písemně na adrese Pplk. Sochora 27, 170 00 Praha 7,

případně u jiného příslušného dozorového úřadu v souvislosti se zpracováním osobních údajů.

5.1. Právo na informace (čl. 13 a 14 Nařízení)

Každý subjekt údajů obdrží od Společnosti stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných jazykových prostředků informace související se zpracováním jeho osobních

údajů, a to v okamžiku, kdy od něj Společnost získává jeho osobní údaje. Překlad do jednoho nebo více jazyků by měl být pořízen, pokud se Společnost zaměřuje na subjekty údajů těmito jazyky mluvící.
Pokud Společnost nezíská osobní údaje přímo od subjektu údajů, poskytne subjektu údajů informace v přiměřené lhůtě po jejich získání, ale nejpozději do jednoho měsíce.

Příklad nejasné informace:
„Vaše osobní údaje můžeme použít pro vývoj nových služeb“ (není tedy jasné, o jaké služby se jedná nebo jak údaje pomohou při jejich vývoji).

Příklad prostředků poskytnutí informace subjektům údajů:
Společnosti provozující webovou stránku (website) by na této webové stránce měly uveřejnit prohlášení nebo oznámení o ochraně soukromí. Odkaz na toto prohlášení/oznámení by měl být zřetelně viditelný na každé webové stránce pod běžně užívaným názvem (třeba „Soukromí“, „Zásady ochrany soukromí“ nebo „Sdělení k ochraně soukromí“). Umístění nebo barevné řešení znesnadňující viditelnost textu nebo odkazu či ztěžující nalezení na webové stránce nebude považováno za souladné s požadavkem snadné přístupnosti. Využívají-li Společnosti aplikace jako prostředek nakládání s osobními údaji, musejí zpřístupnit informaci z internetového úložiště ještě před stažením aplikace. Po stažení aplikace by tato informace nikdy neměla být dále než na „dvě poklepání“. Obecně to znamená, že funkcionalita menu často používaná u aplikací by vždy měla obsahovat volbu „Soukromí“ nebo „Ochrana soukromí“.

Informace budou poskytovány prostřednictvím dokumentu Informace o zpracování osobních údajů zpřístupněného subjektu údajů jedním z následujících způsobů:

- zasláním v elektronické formě na emailovou adresu subjektu údajů;
- zasláním poštou na kontaktní adresu subjektu údajů; nebo
- v elektronické formě na internetových stránkách jednotlivých produktů Společnosti.

5.2. Právo na přístup k osobním údajům (čl. 15 Nařízení)

Právo na přístup k osobním údajům má tři složky. Subjekt údajů ve své žádosti adresované Společnosti určí, kterou ze složek práva na přístup k osobním údajům využívá. Vzorová žádost je dostupná v Informačním systému Společnosti a na internetových stránkách Společnosti.

Subjekt údajů má právo získat od Společnosti potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány.

Pokud Společnost osobní údaje subjektu údajů zpracovává, je povinna sdělit subjektu údajů následující informace (o které z těchto informací konkrétně subjekt žádá, rovněž stanoví ve své žádosti):

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 na Společnosti opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování nebo vznést námitku proti tomuto zpracování;
f) právo podat stížnost u Úřadu pro ochranu osobních údajů nebo u jiného příslušného dozorového úřadu v souvislosti se zpracováním osobních údajů;
g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;

h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

Pokud Společnost osobní údaje subjektu údajů zpracovává, je povinna poskytnout subjektu údajů bezplatně kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může Společnost účtovat přiměřený poplatek odpovídající administrativním nákladům na pořízení těchto kopií. Právem získat kopii zpracovávaných osobních údajů nesmějí být nepříznivě dotčena práva a svobody jiných osob.

Společnost musí subjektům údajů umožnit podání žádostí v různých formách, jež se primárně budou odvíjet od vztahu mezi Společností a subjektem údajů (písemným formulářem, elektronicky). Jestliže subjekt údajů podává žádost v elektronické formě, budou informace poskytnuty v běžně používané elektronické formě, ledaže by subjekt údajů ve své žádosti uvedl, že požaduje jiný způsob poskytnutí informací. O opatřeních přijatých na základě žádosti subjektu údajů informuje Společnost subjekt údajů do jednoho měsíce od přijetí žádosti, nejpozději však do tří měsíců od přijetí žádosti, byla-li lhůta v případě odůvodněné potřeby prodloužena.

5.3. Právo na opravu (čl. 16 Nařízení)

Subjekt údajů má právo na:

a) opravu nepřesných osobních údajů, které se ho týkají;
b) doplnění neúplných osobních údajů s přihlédnutím k účelům zpracování, a to i prostřednictvím poskytnutí dodatečného prohlášení.

Právo na opravu či doplnění subjekt údajů uplatní prostřednictvím žádosti, v níž subjekt údajů uvede své identifikační údaje, právo, jež prostřednictvím žádosti uplatňuje a způsob, jakým si přeje být informován o opatřeních přijatých Společností. Vzorová žádost je dostupná v Informačním systému Společnosti a na internetových stránkách Společnosti.
O opatřeních přijatých na základě žádosti subjektu údajů informuje Společnost subjekt údajů do jednoho měsíce od přijetí žádosti, nejpozději však do tří měsíců od přijetí žádosti, byla-li lhůta v případě odůvodněné potřeby prodloužena.
Společnost oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy osobních údajů. Pokud to subjekt údajů požaduje, informuje Společnost subjekt údajů o takto informovaných příjemcích.

5.4. Právo na výmaz / právo být zapomenut (čl. 17 Nařízení)

Na žádost subjektu údajů Společnost bez zbytečného odkladu vymaže jeho osobní údaje, pokud je dán některý z níže uvedených důvodů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
b) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování;
c) subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování osobních údajů pro účely přímého marketingu;
d) osobní údaje byly zpracovány protiprávně;
e) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené právem Evropské unie nebo členského státu, které se na Společnost vztahuje;
f) osobní údaje dítěte byly shromážděny v souvislosti s nabídkou služeb informační společnosti učiněnou přímo dítěti.

V žádosti o výmaz osobních údajů subjekt údajů uvede své identifikační údaje, právo, jež prostřednictvím žádosti uplatňuje a způsob, jakým si přeje být informován o opatřeních přijatých Společností. Vzorová žádost je dostupná na adrese v Informačním systému Společnosti a na internetových stránkách Společnosti.
Jestliže Společnost osobní údaje zveřejnila a je povinna tyto osobní údaje vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby informovala správce a zpracovatele, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.
Výše uvedené neplatí, pokud je zpracování osobních údajů nezbytné:

a) pro výkon práva na svobodu projevu a informace;
b) pro splnění právní povinnosti, jež vyžaduje zpracování osobních údajů podle práva Evropské unie nebo členského státu, které se na Společnost vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Společnost pověřena;
c) z důvodů veřejného zájmu v oblasti veřejného zdraví;
d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely, pokud je pravděpodobné, že by využití práva na výmaz znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování;
e) pro určení, výkon nebo obhajobu právních nároků.

Společnost oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré výmazy osobních údajů, pokud je to možné s vynaložením přiměřeného úsilí. Pokud to subjekt údajů požaduje, informuje Společnost subjekt údajů o tom, kteří příjemci osobních údajů byli takto informováni.
O opatřeních přijatých na základě žádosti subjektu údajů informuje Společnost subjekt údajů do jednoho měsíce od přijetí žádosti, nejpozději však do tří měsíců od přijetí žádosti, byla-li lhůta v případě odůvodněné potřeby prodloužena. Pokud na základě jedné z výše uvedených výjimek Společnost odmítne osobní údaje vymazat, informuje o tom subjekt údajů ve lhůtě jednoho měsíce od doručení žádosti, odůvodní užití výjimky a poučí subjekt údajů o právu podat stížnost u Úřadu pro ochranu osobních údajů nebo u jiného příslušného dozorového úřadu v souvislosti se zpracováním osobních údajů nebo žádat soudní ochranu.

5.5. Právo na omezení zpracování (čl. 18 a 19 Nařízení)

Subjekt údajů má právo na to, aby Společnost omezila zpracování jeho osobních údajů, v kterémkoli z těchto případů:

a) subjekt údajů popírá přesnost osobních údajů; v tomto případě bude zpracování omezeno na dobu potřebnou k tomu, aby Společnost mohla přesnost osobních údajů ověřit;
b) zpracování osobních údajů je protiprávní, subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
c) Společnost již osobní údaje nepotřebuje pro stanovený účel zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
d) subjekt údajů uplatnil právo vznést námitku proti zpracování osobních údajů; v tomto případě bude zpracování omezeno, dokud nebude ověřeno, zda oprávněné důvody Společnosti převažují nad oprávněnými důvody subjektu údajů.

V žádosti o omezení zpracování subjekt údajů uvede své identifikační údaje, právo, jež prostřednictvím žádosti uplatňuje, důvod požadovaného omezení zpracování a způsob, jakým si přeje být informován o opatřeních přijatých Společností. Vzorová žádost je dostupná v Informačním systému Společnosti a na internetových stránkách Společnosti.

O opatřeních přijatých na základě žádosti subjektu údajů informuje Společnost subjekt údajů do jednoho měsíce od přijetí žádosti, nejpozději však do tří měsíců od přijetí žádosti, byla-li lhůta v případě odůvodněné potřeby prodloužena.
V důsledku omezení zpracování osobních údajů může Společnost předmětné osobní údaje nadále ukládat, avšak zpracovány mohou být pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Evropské unie nebo některého členského státu. V těchto případech bude subjekt údajů, který dosáhl omezení zpracování osobních údajů, Společností předem upozorněn na to, že omezení zpracování bude zrušeno.
Společnost oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškerá omezení zpracování osobních údajů, pokud je to možné s vynaložením přiměřeného úsilí. Pokud to subjekt údajů požaduje, informuje Společnost subjekt údajů o tom, kterým příjemcům bylo takové oznámení podáno.

5.6. Právo na přenositelnost údajů (čl. 20 Nařízení)

Subjekt údajů má právo získat osobní údaje, které se ho týkají, které poskytl Společnosti a které jsou zpracovávány automatizovaně, pokud je současně splněna některá z níže uvedených podmínek:

a) osobní údaje jsou zpracovávány pro konkrétní účel/-y na základě souhlasu subjektu údajů;
b) jedná se o zvláštní kategorii osobních údajů zpracovávaných pro jeden nebo více stanovených účelů na základě výslovného souhlasu uděleného subjektem údajů; nebo
c) zpracování osobních údajů je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů.

Za osobní údaje poskytnuté Společnosti jsou považovány údaje, které subjekt údajů přímo, vědomě a aktivně sdělil Společnosti např. prostřednictvím formuláře, ale rovněž údaje generované na základě aktivity subjektu údajů při používání služby nebo zařízení, jako např. lokalizační údaje, data přihlášení do aplikace apod.
V žádosti o přenos osobních údajů subjekt údajů uvede své identifikační údaje, právo, jež prostřednictvím žádosti uplatňuje, komu mají být údaje předány a způsob, jakým si přeje být informován o opatřeních přijatých Společností. Vzorová žádost je dostupná v Informačním systému Společnosti a na internetových stránkách Společnosti.
O opatřeních přijatých na základě žádosti subjektu údajů informuje Společnost subjekt údajů do jednoho měsíce od přijetí žádosti, nejpozději však do tří měsíců od přijetí žádosti, byla-li lhůta v případě odůvodněné potřeby prodloužena.
Společnost osobní údaje subjektu údajů poskytne ve strukturovaném, běžně používaném a strojově čitelném formátu. Subjekt údajů je oprávněn předat získané osobní údaje jinému správci osobních údajů. Subjekt údajů si ve své žádosti zvolí, zda má Společnost osobní údaje poskytnout subjektu údajů nebo zda využije právo na to, aby jeho osobní údaje byly předány Společností přímo jinému správci/zpracovateli, je-li to technicky proveditelné.
Právem na přenositelnost údajů nesmí být nepříznivě dotčena práva a svobody jiných osob.

5.7. Právo vznést námitku (čl. 21 Nařízení)

V případě zpracování osobních údajů na základě právního titulu oprávněného zájmu Společnosti má subjekt údajů právo vznést námitku proti zpracování svých osobních údajů z důvodů týkajících se jeho konkrétní situace, které v námitce popíše. Vzorová námitka je dostupná v Informačním systému Společnosti a na internetových stránkách Společnosti.

O opatřeních přijatých na základě námitky subjektu údajů informuje Společnost subjekt údajů do jednoho měsíce od přijetí námitky, nejpozději však do tří měsíců od přijetí námitky, byla-li lhůta v případě odůvodněné potřeby prodloužena.

V případě přijetí námitky Společnost osobní údaje přestane zpracovávat (ponechá si je pouze uložené) a provede posouzení, zda má závažné oprávněné důvody pro jejich zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků. Pokud Společnost dojde k závěru, že takové důvody má, informuje o tom subjekt údajů, sdělí mu zároveň možnosti další obrany a ve zpracování osobních údajů pokračuje. Pokud Společnost naopak dojde k závěru, že dostatečné důvody pro zpracování osobních údajů nemá, subjekt údajů o tom informuje, zpracování ukončí a provede výmaz osobních údajů.
Subjekt údajů má právo vznést kdykoli námitku proti zpracování osobních údajů pro účely přímého marketingu, v důsledku čehož Společnost osobní údaje pro tento účel přestane zpracovávat.
Společnost na výše uvedené právo vznést námitku subjekt údajů výslovně, zřetelně a odděleně od jiných informací upozorní nejpozději v okamžiku první komunikace se subjektem údajů.

5.8. Právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování (čl. 22 Nařízení)

Společnost spravuje osobní údaje s respektem k právu subjektu údajů nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování osobních údajů, které se subjektu údajů významně dotýká, a to včetně profilování (tj. jakékoli formy automatizovaného zpracování osobních údajů spočívajícího v jejich použití k rozboru, odhadu nebo hodnocení určitých aspektů týkajících se subjektu údajů – např. pracovního výkonu, ekonomické situace, zájmů apod.).
Společnost může při správě osobních údajů učinit subjekt údajů předmětem automatizovaného rozhodnutí, pokud je takové rozhodnutí nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a Společností, nebo pokud je rozhodnutí povoleno právním předpisem Evropské unie nebo českého právního řádu současně vhodně zajišťujícím ochranu práv a svobod a oprávněných zájmů subjektu údajů, nebo pokud subjekt údajů k takovému rozhodnutí udělil výslovný souhlas.
Pokud subjekt údajů nechce být předmětem automatizovaného rozhodování, včetně profilování, uvede ve své žádosti adresované Společnosti své identifikační údaje, právo, jež prostřednictvím žádosti uplatňuje a způsob, jakým si přeje být informován o opatřeních přijatých Společností. Vzorová žádost je dostupná v Informačním systému Společnosti a na internetových stránkách Společnosti.

5.9. Omezení práva subjektu údajů na přístup k osobním údajům, omezení zpracování, opravu, námitku, výmaz dle § 11 Zákona

Společnost může odmítnout částečně či zcela žádost o přístup k osobním údajům nebo o výmaz osobních údajů, a to v následujících případech: (i) při vymáhání soukromoprávních nároků Společnosti (tedy v případě sporu), (ii) hrozí-li Společnosti z plnění práva požadovaného subjektem údajů újma (musí se jednat o konkrétní hrozící újmu, plynoucí například z citlivé povahy údajů, které by měly být poskytnuty v rámci práva na přístup a které není možné např. začernit, a toto riziko musí být ze strany Společnosti dostatečně podloženo), nebo (iii) je-li Společnost povinna plnit povinnosti vyplývající z AML, IDD, zákona o distribuci pojištění a zajištění a dalších zvláštních právních předpisů.

Tuto výjimku lze uplatnit pouze za splnění předpokladů stanovených § 11 Zákona a takové odmítnutí musí být řádně odůvodněno.

6. Předávání osobních údajů

Osobní údaje může Společnost jako správce zpracovávat sama (přímo svými zaměstnanci), anebo prostřednictvím třetích osob (dále jen „**Zpracovatel**“ nebo „**Zpracovatelé**“), jednotlivé kategorie Zpracovatelů Společnosti jsou uvedeny v příloze č. 1 těchto Pravidel. Společnost může rovněž vystupovat v pozici zpracovatele osobních údajů. Společnost uzavřela s každým Zpracovatelem smlouvu o zpracování osobních údajů a stejně tak uzavřela smlouvu o zpracování osobních údajů s osobami, vůči nimž Společnost vystupuje v pozici zpracovatele.
O tom, komu a v jakém rozsahu jsou informace předávány, se subjekt údajů dozví z informace, kterou mu Společnost individuálně předá (zašle).
Zpracovatelé poskytli Společnosti dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Nařízení a aby byla zajištěna ochrana práv subjektů údajů.
Společnost nepředává osobní údaje třetím osobám úplatně.
Společnost nepředává osobní údaje do třetích zemí mimo Evropskou unii a Evropský hospodářský prostor.

7. Zabezpečení ochrany osobních údajů

7.1. Technická a organizační opatření

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracovávání i k pravděpodobným a různě vážným rizikům pro práva a svobody fyzických osob Společnost zavedla vhodná technická a organizační opatření, aby zajistila úroveň zabezpečení osobních údajů odpovídající danému riziku zejména náhodnému nebo protiprávnímu zničení, ztrátě, pozměňování, neoprávněnému zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů nebo neoprávněnému přístupu k nim.
Společnost zavedla zejména následující opatření:

- šifrování osobních údajů;
- systém úrovní oprávnění pro přístup k osobním údajům, autentizace, autorizace;
- antivirová ochrana;
- monitorování přístupů konkrétních osob k osobním údajům;
- monitorování změn provedených konkrétními osobami v osobních údajích;
- rozprostření síťové služby a dat mezi větší počet serverů;
- zálohování;
- detekce úniku dat – DLP;
- správa mobilních zařízení – MDM systém;
- Firewall;
- Proxy s filtrováním nebezpečného obsahu;
- přístupový systém.

Společnost jako zaměstnavatel zavázala mlčenlivostí své zaměstnance pověřené nakládáním s osobními údaji v pracovních smlouvách a dohodách.
Vyjma výše uvedených opatření Společnost (prostřednictvím těchto Pravidel) uložila zaměstnancům a dalším osobám ve Společnosti, podílející se na zpracování osobních údajů fyzických osob, dodržování následujících organizačních opatření:

- obezřetně zacházet se svěřenými i jimi samými vytvářenými dokumenty, především tyto uchovávat na místech k tomu určených (např. uzavíratelné skříně), nenechávat je nikdy volně přístupné ani přístupné třetím osobám, včetně spolupracovníků;

- neprodleně skartovat nepotřebné dokumenty a obecně si uvědomovat svoji odpovědnost za zachování důvěrnosti jejich obsahu;
- při nakládání s Osobními údaji užívat pouze bezpečné způsoby korespondence;
- v případě používání elektronické komunikace mít na vědomí zvýšené riziko případného úniku informací a používat zabezpečenou elektronickou poštu;
- v žádném případě nesdělovat jakékoliv Osobní údaje třetím subjektům;
- všemi dostupnými prostředky chránit Osobní údaje a dokumenty je obsahující před zcizením či jakýmkoliv zneužitím;
- před odesláním dokumentu s Osobními údaji mimo prostor Společnosti aplikovat systém „čtyř očí";
- bez výslovného schválení nadřízeným zaměstnancem bezdůvodně nevynášet z prostor Společnosti žádné dokumenty obsahující Osobní údaje;
- řádně užívat všech mechanických a elektronických zabezpečovacích systémů, instalovaných v objektech Společnosti, v nichž jsou uchovávány dokumenty obsahující Osobní údaje;
- dodržovat pokyny Společnosti a jejich vedoucích zaměstnanců, týkající se ochrany Osobních údajů;
- poskytovat méně zkušeným spolupracovníkům návody a postupy bezpečného nakládání s Osobními údaji, případně je upozornit, kde lze tyto najít ve vnitřní síti Společnosti - „intranet";
- podrobně se seznámit s těmito Pravidly, stejně jako se všemi dalšími směrnicemi, instrukcemi či pokyny Společnosti, upravujícími obezřetné nakládaní s Osobními údaji.

Společnost v současné době nenabízí svoje produkty a služby prostřednictvím komunikace na dálku ve smyslu příslušných zákonů. V případě, že Společnost v budoucnu bude využít komunikace na dálku ohledně smlouvy s klientem nebo nabídky služeb Společnosti v souvislosti se smlouvou uzavřenou s klientem, IT oddělení Společnosti nastaví řešení ověření identity klienta (např. verifikačním kódem) za účelem eliminace rizika záměny identity subjektu údajů a neoprávněného zpracování osobních údajů osob mladších 15 let bez souhlasu jejich zákonného zástupce, pro zajištění dodržení požadavků § 7 Zákona.

7.2. Záznamy o činnostech zpracování osobních údajů

Společnost, ať už se nacházejí v pozici správce nebo zpracovatele osobních údajů, vede záznamy o činnostech zpracování osobních údajů. Tyto záznamy obsahují všechny informace požadované čl. 30 Nařízení. Společnost v rámci spolupráce s dozorovým úřadem a na jeho žádost tyto záznamy úřadu zpřístupní, aby na jejich základě mohly být monitorovány veškeré operace s osobními údaji ve Společnosti. Společnost vede rovněž záznamy o veškerých případech porušení zabezpečení osobních údajů včetně skutečností, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Není-li učiněno ohlášení porušení zabezpečení dozorovému úřadu dle čl. 0 těchto Pravidel, Společnost zdokumentuje v záznamech o činnostech zpracování důvody, proč jsou přesvědčena o tom, že je nepravděpodobné, že porušení bude mít za následek riziko pro práva a svobody subjektů údajů.

7.3. Analýza a posouzení rizik při zpracování osobních údajů

V případech, kdy je pravděpodobné, že operace zpracování budou představovat vysoké riziko pro práva a svobody fyzických osob, Společnost provede posouzení vlivu na ochranu osobních údajů, aby vyhodnotila zejména původ, povahu, zvláštnost a závažnost tohoto rizika. Výsledek posouzení by měl být zohledněn při rozhodování Společnosti o vhodných opatřeních, která by měla být přijata s cílem zajistit soulad zpracování s obecně závaznými právními předpisy.
Pravděpodobnost a závažnost rizika pro práva a svobody subjektu údajů by měla být určena na základě povahy, rozsahu, kontextu a účelům zpracování. Riziko by mělo být hodnoceno na základě objektivního posouzení, které stanoví, zda operace zpracování představují riziko či vysoké riziko.

Pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že operace zpracování představují vysoké riziko, které Společnost nemůže vhodnými opatřeními zmírnit, s ohledem na dostupné technologie a náklady na provedení, obrátí se Společnost s žádostí o konzultaci na dozorový úřad.

7.4. Ohlášení a oznámení porušení zabezpečení osobních údajů

Dojde-li k porušení zabezpečení osobních údajů, Společnost přijme odpovídající opatření k nápravě. Porušením zabezpečení osobních údajů je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

Jednotlivé případy porušení zabezpečení osobních údajů

- Porušení důvěrnosti – v případě neoprávněného nebo náhodného poskytnutí nebo zpřístupnění osobních údajů.
- Porušení dostupnosti – v případě náhodné nebo neoprávněné ztráty přístupu nebo zničení osobních údajů.

Příklad ztráty dostupnosti:
Smazání dat, buď náhodné nebo neoprávněnou osobou nebo, v případě bezpečně zašifrovaných dat, ztráta dešifrovacího klíče; případ, kdy Společnost není schopna obnovit přístup k datům, například ze záložního zařízení.

Zařízení obsahující kopii databáze zákazníků správce, kterou někdo ztratil nebo ukradl; existence jediné sady osobních údajů, která byla zašifrována vyděračským softwarem (ransomware) nebo správcem, jenž už nemá v držení příslušný klíč.

- Porušení integrity – v případě neoprávněného nebo náhodného pozměnění osobních údajů.

Jak posoudit riziko a vyhodnotit, zda je zapotřebí ohlašovat/oznamovat?

Společnost by při posouzení rizika měla vzít v úvahu zejména následující kritéria:

- Typ porušení
  např. porušení důvěrnosti, porušení integrity
- Povaha, citlivost a objem osobních údajů
  čím citlivější data, tím vyšší riziko pro dotčené subjekty údajů, avšak v úvahu by bylo dobré vzít také ostatní osobní údaje, které už o subjektu údajů jsou dostupné
- Snadnost identifikace jednotlivců
  je zapotřebí posoudit, jak snadné bude pro někoho s přístupem k napadeným osobním údajům identifikovat konkrétního jedince nebo propojit tyto údaje s dalšími informacemi za účelem jeho ztotožnění
- Závažnost důsledků pro jednotlivce
  v závislosti na povaze porušení dotčených osobních údajů, například u zvláštní kategorie dat, může být potenciální škoda pro jednotlivce zvlášť závažná, zejména pokud by porušení mohlo vést ke krádeži totožnosti nebo podvodu
- Zvláštní charakteristiky jednotlivce
  porušení může postihnout osobní údaje týkající se dětí
- Počet dotčených jednotlivců
  čím vyšší počet dotčených jednotlivců, tím větší dopad porušení může mít. Porušení však může mít závažný dopad i jen na jednoho člověka, podle povahy ohrožených osobních údajů a souvislostí, za kterých se tak stalo

- Zvláštní charakteristiky správce
  např. pokud správce zpracovává zvláštní kategorie údajů
- Obecné skutečnosti.

Ohlášení porušení zabezpečení osobních údajů

Dozví-li se Společnost o porušení zabezpečení osobních údajů, měla by je bez zbytečného odkladu, a je-li to možné, do 72 hodin poté, co se o něm dozvěděla, ohlásit příslušnému dozorovému úřadu. Pokud je však nepravděpodobné, že by dané porušení zabezpečení osobních údajů mělo za následek riziko pro práva a svobody fyzických osob, není zapotřebí takové porušení dozorovému úřadu ohlašovat. Vzorové ohlášení je dostupné na internetových stránkách dozorového úřadu (v době vydaní těchto Pravidel dostupné na adrese: https://www.uoou.cz/oznameni-o-poruseni-ochrany-osobnich-udaju.asp#obalhlava). Není-li možné učinit ohlášení do 72 hodin, měly by být spolu s ním uvedeny důvody zpoždění a informace mohou být poskytnuty postupně bez zbytečného odkladu.

Příklady okamžiku zjištění případu porušení:
V případě ztráty CD s nezašifrovanými daty není mnohdy možné zjistit, zda k nim získala přístup neoprávněná osoba. Takový případ však musí být ohlášen, neboť je tu dostatečná míra pravděpodobnosti, že k porušení došlo; okamžikem, kdy se o něm správce dozvěděl, je chvíle, kdy si uvědomil ztrátu CD.

Správce zjistí, že možná někdo proniknul do jeho sítě. Prověří tedy své systémy, zda osobní údaje v nich uložené nebyly ohroženy a v daném případě se jeho podezření potvrdí. Zde rovněž není pochyb o tom, že se správce o případu „dozvěděl", jelikož v daném okamžiku o něm získal jasný důkaz.

Příklad porušení, které vyžaduje ohlášení dozorovému úřadu:
E-mail v rámci přímého marketingu byl odeslán příjemcům v kolonce „komu" nebo „kopie", čímž každý z příjemců mohl zjistit elektronickou adresu ostatních příjemců.
Ohlášení dozorovému úřadu může být povinné, jestliže byl postižen velký počet jednotlivců, došlo k odhalení citlivých údajů (zdravotní data) nebo pokud existují jiné faktory představující vysoké riziko (např. zpráva obsahuje iniciační hesla). Naopak, ohlášení nemusí být nutné, pokud nedošlo k odhalení citlivých údajů a pokud došlo k odkrytí jen menšího počtu e-mailových adres.

Příklad porušení, které nevyžaduje ohlášení dozorovému úřadu:
Ztráta bezpečně zašifrovaného mobilního zařízení používaného správcem a jeho zaměstnanci. Za podmínky, že šifrovací klíč zůstal v bezpečném držení správce a nejde o jedinou kopii osobních údajů, jsou osobní údaje pro útočníka nedostupné. Znamená to, že případ porušení pravděpodobně nevyústí v riziko pro práva a svobody dotčených subjektů údajů. Vyjde-li později najevo, že šifrovací klíč byl prozrazen nebo že šifrovací software nebo algoritmus je zranitelný, pak se úroveň rizika pro práva a svobody fyzických osob změní a ohlášení může být vyžadováno.

Oznámení porušení zabezpečení osobních údajů

Společnost oznámí porušení zabezpečení osobních údajů subjektu údajů bez zbytečného odkladu, pokud je pravděpodobné, že toto porušení bude mít za následek vysoké riziko pro práva a svobody fyzické osoby, aby mohly učinit nezbytná opatření. V oznámení bude popsána povaha daného případu porušení zabezpečení osobních údajů a obsažena doporučení pro dotčený subjekt údajů, jak případné nežádoucí účinky zmírnit. Tato oznámení budou subjektům údajů doručena, jakmile je to proveditelné, v úzké spolupráci s dozorovým úřadem a v souladu s pokyny tohoto úřadu nebo jiných příslušných orgánů. Například v případě potřeby zmírnit bezprostřední riziko způsobení újmy je nutné tuto skutečnost subjektům údajů neprodleně oznámit, zatímco v situaci, kdy je zapotřebí zavést vhodná opatření s cílem zabránit tomu, aby porušení zabezpečení osobních údajů pokračovalo nebo aby docházelo k podobným případům

porušení, může být opodstatněna delší lhůta. Vzorové oznámení je dostupné v Informačním systému Společnosti a na internetových stránkách Společnosti.

Příklad porušení, které vyžaduje oznámení subjektu údajů:
E-mail v rámci přímého marketingu byl odeslán příjemcům v kolonce „komu“ nebo „kopie“, čímž každý z příjemců mohl zjistit elektronickou adresu ostatních příjemců.
Nutnost oznámení jednotlivcům bude záviset na rozsahu a druhu dotčených osobních údajů a na závažnosti možných důsledků.

8. Závěrečná ustanovení

Tento vnitřní předpis může být aktualizován jednatelem Společnosti.