



Skupina PPF

Zásady ochrany osobních údajů

OBSAH

1. ÚVOD.....	6
1.1 Jaké zákony o ochraně osobních údajů platí a kdy se použijí?.....	6
1.2 Co jsou osobní údaje?.....	6
1.3 Co je zpracování?	7
1.4 Co je „automatizované zpracování“ a „evidence“?	7
1.5 Kdo osobní údaje spravuje?.....	8
1.6 Proč je důležité „správce“ a „zpracovatele“ rozlišovat?.....	9
2. KLÍČOVÉ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ	9
2.1 Podmínky zpracování	10
2.2 Zpracování omezené účelem (zásada účelového omezení)	10
2.3 Transparentní zpracování (zásada transparentnosti).....	11
2.4 Přiměřené, relevantní a omezené na to, co je nezbytné pro účely zpracování (zásada minimalizace údajů)	12
2.5 přesné a v případě potřeby aktualizované (zásada správnosti).....	13
2.5.1 Kdy jsou osobní údaje „přesné“ nebo „nepřesné“?	13
2.5.2 Musí být osobní údaje vždy aktuální?	13
2.5.3 Co jsou „přiměřené kroky“?	13
2.6 uchovávány jen po dobu nezbytnou pro účely, pro které jsou zpracovávány, a poté zničeny nebo anonymizovány (zásada omezení uchovávání).....	14
2.7 Zpracovávání v souladu s právy subjektů údajů	14
2.7.1 Právo být informován	14
2.7.2 Právo na přístup k osobním údajům.....	14
2.7.3 Právo na opravu	15
2.7.4 Právo na výmaz.....	15
2.7.5 Právo na omezení zpracování	16
2.7.6 Právo na přenositelnost údajů	16
2.7.7 Právo vznést námitku.....	17

2.7.8	Práva související s automatizovaným rozhodováním včetně profilování	17
2.7.9	Způsoby řešení žádostí subjektů údajů	19
2.7.10	Oznámení příjemcům osobních údajů	19
2.8	Zpracovávají bezpečně a důvěrně (zásada integrity a důvěrnosti).....	19
2.8.1	Povinnost zavést bezpečnostní opatření.....	19
2.8.2	povinnost hlásit případy porušení zabezpečení osobních údajů.	20
2.9	Předávány příjemcům mimo EU pouze, pokud jsou splněny určité podmínky	21
2.9.1	Co je to předávání osobních údajů?	21
2.9.2	Předávání osobních údajů v rámci EHP.....	22
2.9.3	Předávání údajů z EU příjemcům mimo EHP	22
3.	ODPOVĚDNÝ PŘÍSTUP K OCHRANĚ SOUKROMÍ	23
3.1	Zásada odpovědného přístupu k ochraně soukromí.....	23
3.2	Vedení záznamů o činnostech zpracování	23
3.3	Záměrná a standardní ochrana osobních údajů.....	24
3.4	Posouzení vlivu na ochranu osobních údajů.....	24
4.	CO SE STANE, KDYŽ PŘEDPISY NEDODRŽÍTE?	25
	PŘÍLOHA Č. 1 – SCHÉMA – CO JSOU OSOBNÍ ÚDAJE (OÚ)?	27
	PŘÍLOHA Č. 2 – DALŠÍ POKYNY OHLEDNĚ PODMÍNEK ZPRACOVÁNÍ.....	28
	PŘÍLOHA Č. 3 – KDY SE MŮŽETE DOVOLÁVAT OPRÁVNĚNÉHO ZÁJMU?	31

Úvod

Evropská unie přijala nový regulační rámec, který stanoví určité změny pravidel ochrany osobních údajů. Obecné nařízení o ochraně osobních údajů (**GDPR**) přehodnocuje některé požadavky na ochranu osobních údajů, posiluje práva subjektů údajů, zavádí nové povinnosti týkající se odpovědnosti pro společnosti a upravuje stávající omezení předávání osobních údajů do zahraničí.

Skupina PPF se v rámci své společenské odpovědnosti zavázala dodržovat mezinárodní právní předpisy o ochraně osobních údajů. Tyto zásady ochrany osobních údajů (dále jen „**Zásady ochrany osobních údajů**“) vychází z celosvětově uznávaných základních principů ochrany osobních údajů. Ochrana osobních údajů představuje základní kámen, na kterém lze vystavět vzájemnou důvěru mezi obchodními partnery, a řádné nakládání s osobními údaji v souladu s legislativními požadavky je proto nesmírně důležité pro úspěch skupiny PPF.

Skupina PPF musí v rámci své činnosti shromažďovat osobní údaje osob, s nimiž jedná. Mezi tyto osoby patří zaměstnanci (současní, bývalí a potenciální), zákazníci, dodavatelé a další obchodní partneři. Shromažďované informace v zásadě zahrnují jméno, adresu, e-mailovou adresu a u zaměstnanců datum narození, počet dětí, rodinný stav, číslo sociálního zabezpečení a daňové číslo, rodné jméno matky a další údaje stanovené zákonem. Základní právní principy vyžadují, aby s těmito údaji bylo nakládáno řádně bez ohledu na způsob, jakým jsou shromažďovány, zaznamenány a používány (např. na počítači nebo jiných digitálních médiích, v tištěné nebo obrazové podobě).

Tyto Zásady ochrany osobních údajů se vztahují na všechny společnosti skupiny PPF (každá z nich dále jen „**PPF**“) a jejich zaměstnance. Zásady ochrany osobních údajů se vztahují na veškeré zpracování osobních údajů. Těmto Zásadám ochrany osobních údajů nepodléhají anonymizované údaje, např. určené pro statistická hodnocení či studie.

Zásady ochrany osobních údajů se skládají z následujících tří částí:

- **Klíčové zásady:** Kapitola 2 popisuje základní principy, které PPF musí při zpracování osobních údajů dodržovat (např. účelové omezení, minimalizace údajů, přesnost atd.).
- **Odpovědnost:** PPF musí přijmout opatření, která jí umožní průběžně prokazovat dodržování předpisů. Jedná se o nový požadavek podle nařízení GDPR. V kapitole 3 popisujeme opatření, která bude muset PPF zavést, aby se stala organizací s odpovědným přístupem k ochraně soukromí (např. školení, vedení záznamů o činnostech zpracování, zavedení zásad ochrany osobních údajů atd.).
- **Sankce:** jednou z klíčových změn, které nařízení GDPR přinese, jsou sankce, jež mohou být uloženy v případech porušení pravidel ochrany osobních údajů. V kapitole 4 je uveden základní popis nových sankcí.

Tyto Zásady ochrany osobních údajů zahrnují mezinárodně uznávané principy ochrany osobních údajů. Nenahrazují však stávající vnitrostátní právní předpisy o ochraně osobních údajů a vnitrostátní zásady ochrany osobních údajů, ale spíše je doplňují. Dojde-li k rozporu mezi příslušnými vnitrostátními předpisy a zásadami ochrany soukromí a těmito Zásadami ochrany osobních údajů, nebo stanoví-li příslušné vnitrostátní předpisy a zásady ochrany soukromí přísnější požadavky než tyto Zásady ochrany osobních údajů, budou mít vnitrostátní předpisy a zásady přednost. PPF odpovídá za dodržování těchto Zásad ochrany osobních údajů a právních povinností s přihlédnutím k výše uvedeným kolizním normám.

Dodržování Zásad ochrany osobních údajů a platných právních předpisů o ochraně osobních údajů je pravidelně prověřováno prostřednictvím auditů ochrany osobních údajů a dalších kontrol.

Vedení společností skupiny PPF odpovídá za zpracování údajů ve své oblasti působnosti. Má proto povinnost zajistit splnění právních požadavků a pravidel obsažených v Zásadách ochrany osobních údajů. Vedení společnosti odpovídá za zavedení organizačních, personálních a technických opatření,

aby bylo veškeré zpracování údajů prováděno v souladu s právními předpisy o ochraně osobních údajů. Abychom vyhověli tomuto požadavku, PPF bude každý rok přezkoumávat a pokud to bude nutné, pozměňovat oznámení o ochraně dat a souhlasy subjektů údajů. Přezkoumání je místně koordinováno osobou zodpovědnou za ochranu údajů a manažery lidských zdrojů a zahrnuje všechny příslušné odbory a zaměstnance.

Všechny vaše případné dotazy ohledně nařízení GDPR a toho, jak bude PPF dodržovat tyto Zásady ochrany osobních údajů, zodpoví pověřenec pro ochranu osobních údajů. S jakýmkoli dotazy či připomínkami se na nás můžete obrátit na adrese dataprivacy@ppfeurope.com.

1. ÚVOD

1.1 Jaké zákony o ochraně osobních údajů platí a kdy se použijí?

V oblastech, kde skupina PPF působí, jsou hlavními platnými právními předpisy týkajícími se ochrany osobních údajů a soukromí:

- Místní právní předpisy na ochranu dat
- Obecné nařízení EU o ochraně osobních údajů č. 679/2016 (GDPR) (platné od 25. května 2018)

Právní předpisy o ochraně osobních údajů se použijí, jsou-li:

- osobní údaje zpracovávány zcela nebo částečně automatizovaně nebo
- zpracovávány osobní údaje, které jsou obsaženy v evidenci (nebo do ní mají být zařazeny).

Klíčovými pojmy jsou „osobní údaje“, „zpracování“, „automatizované zpracování“ a „evidence“.

1.2 Co jsou osobní údaje?

Pojem „osobní údaje“ má velmi široký rozsah (viz rámeček).

Mohou se jimi rozumět i takové údaje, které samy o sobě neumožňují identifikaci osoby, k níž se vztahují.

Tak je tomu například, pokud:

Osobními údaji jsou jakékoli informace týkající se identifikované nebo identifikovatelné fyzické osoby, které samostatně nebo v kombinaci s jinými informacemi identifikují konkrétní fyzickou osobu. 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.

- jsou údaje použity k hodnocení osoby, k určitému zacházení s ní či k ovlivnění jejího stavu nebo chování,
- údaje budou mít pravděpodobně vliv na práva a zájmy osoby.

Osobní údaje, které jsou kódované, pseudonymizované nebo šifrované, se ve většině případů stále považují za osobní údaje. Osobní údaje se za osobní údaje nadále nepovažují, pokud byly anonymizovány tak, že technicky není možné spojit je s příslušnou fyzickou osobou.

Osobními údaji se nerozumí jen údaje, které se vztahují k soukromému životu fyzické osoby (např. adresa soukromého bydliště). Mohou za ně být považovány i údaje týkající se profesního života fyzické osoby (např. telefonní číslo do kanceláře).

Mezi informace, které dle okolností zřejmě budou považovány za osobní údaje, patří například:

- podrobnosti o mzdě a bankovním účtu pracovníka ve vašem informačním systému.
- e-mail o incidentu týkajícím se určitého jmenovitě identifikovaného pracovníka,

- poznámkový blok vedoucího pracovníka obsahující informace o určitém pracovníkovi.

Mezi informace, které dle okolností zřejmě nebudou považovány za osobní údaje, patří například:

- zpráva o srovnání úspěšnosti různých kampaní, která neobsahuje žádné údaje týkající se fyzických osob
- zpráva o výsledcích pohovorů s odcházejícími pracovníky, kde jsou všechny odpovědi anonymizovány, a výsledky není možné spojit s konkrétními osobami.

Zpracováním se rozumí jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šířením nebo jakýmkoli jiným způsobem, seřazení či zkombinování, omezení, výmaz nebo zničení.

Některé kategorie citlivých osobních údajů podléhají zvláštní ochraně. Jedná se o takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a o zpracování genetických či biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Citlivým osobním údajem může být například informace, že zaměstnanec pracuje na poloviční úvazek z důvodu poranění nohy.

Zpracování citlivých osobních údajů je v zásadě zakázáno, s výjimkou případů podléhajících přísným podmínkám, např. je-li to nezbytné z hlediska životně důležitých zájmů fyzické osoby, fyzická osoba k tomu udělila souhlas nebo je to nutné pro obhajobu právních nároků.

V příloze č. 1 těchto Zásad ochrany osobních údajů naleznete jednoduchý diagram, který vám pomůže určit, zda určité údaje představují osobní údaje.

1.3 Co je zpracování?

Pojem „zpracování“ má velmi široký rozsah (viz rámeček).

Pod „zpracování“ se řadí většina činností, při nichž společnost nakládá s osobními údaji, například:

- vedení personálních složek
- monitorování kamerovým systémem (pokud monitorování neprobíhá v místě, které není přístupné fyzickým osobám)
- vedení databáze CRM s podrobnostmi o kontaktních osobách zákazníků PPF
- zasílání newsletterů na e-mailové adresy, které se týkají fyzické osoby (např. janos.kovacs@company.com)
- ukládání osobních údajů na serveru

Evidencí se rozumí jakýkoli strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného

1.4 Co je „automatizované zpracování“ a „evidence“?

Automatizovaným zpracováním se v zásadě rozumí zpracování prostřednictvím informačních systémů (servery, síť, PC, notebooky, tablety, chytré telefony, kamerové systémy apod.).

Pokud tedy používáte ke zpracování osobních údajů nějaký informační systém, jedná se o zpracování a použijí se právní předpisy o ochraně osobních údajů. Právní předpisy o ochraně osobních údajů se však použijí i v případě, že používáte osobní údaje výhradně v papírové evidenci.

Například složka s názvem „Zaměstnanci – dovolená“ s abecedním řazením je pravděpodobně evidencí a vztahují se na ni právní předpisy o ochraně osobních údajů.

1.5 Kdo osobní údaje spravuje?

Zákony o ochraně osobních údajů rozlišují „správce“ a „zpracovatele“.

Správce určuje *účely* a *způsob* zpracování osobních údajů. Může tak činit buď samostatně, nebo společně s jinými organizacemi. Správce tedy celkově dohlíží na to, „proč“ a „jak“ jsou údaje zpracovány.

Chcete-li zjistit, zda jste správcem, musíte zjistit, která organizace rozhoduje:

- že budou osobní údaje shromažďovány a na jakém právním základě,
- jaké osobní údaje se budou shromažďovat, tj. obsah údajů,
- za jakým účelem nebo účely mají být údaje použity,
- o kterých fyzických osobách se mají údaje shromažďovat,
- zda údaje sdělit, a pokud ano, komu,
- zda se uplatní právo subjektů na přístup k osobním údajům a jiná práva fyzických osob, tj. uplatnění výjimek, a
- jak dlouho údaje uchovávat nebo zda na nich provádět nerutinní změny.

Všechna tato rozhodnutí může činit pouze správce v rámci svého celkového dohledu nad procesem zpracování údajů.

V souladu s podmínkami smlouvy se správcem a jeho smlouvou může zpracovatel rozhodovat:

- o tom, jaké informační systémy nebo jiné metody pro shromažďování osobních údajů použít,
- o tom, jak osobní údaje uchovávat,
- o podrobnostech zabezpečení osobních údajů,
- o způsobu předávání osobních údajů z jedné organizace do jiné,
- o způsobu získání osobních údajů o některých fyzických osobách,
- o tom, jak zajistit soulad s harmonogramem uchovávání údajů, a
- o způsobu výmazu nebo likvidace údajů.

Tyto seznamy nejsou vyčerpávající, ale ilustrují rozdíly mezi rolí správce a zpracovatele. Poukazují na to, že zpracovatel má volnost využívat své technické znalosti, aby rozhodl, jak jménem správce provádět určité činnosti. Nemůže však činit žádná rozhodnutí na vyšší úrovni, například k čemu budou osobní údaje používány a jaký je jejich obsah. Taková rozhodnutí smí činit pouze správce.

1.6 Proč je důležité „správce“ a „zpracovatele“ rozlišovat?

Povinnosti, které v souvislosti s ochranou údajů náleží správci a zpracovatelům, nejsou totožné.

Správci často ze zákonů o ochraně osobních údajů plyne více povinností než zpracovatelům. Například pokud zpracovatel zpříčiní porušení zabezpečení osobních údajů, je zpracovatel povinen o takovém porušení informovat správce a správce je případně povinen informovat o něm úřady pro ochranu údajů (a někdy i dotčené osoby).

Správci a zpracovatelé rovněž musí uzavřít písemnou smlouvu, která musí zajistit, aby zpracovatel:

- zpracovával údaje pouze na základě pokynů správce,
- aby zaměstnanci zpracovatele a dílčí zpracovatelé byli vázáni povinností mlčenlivosti,
- nesdílel údaje se třetími osobami s výjimkou dílčích zpracovatelů pověřených správcem,
- přijal veškerá vhodná technická a organizační opatření k zajištění úrovně zabezpečení odpovídající danému riziku,
- najal dílčího zpracovatele pouze s předchozím písemným (konkrétním nebo obecným) souhlasem správce, přičemž na dílčího zpracovatele se musí vztahovat v souvislosti s ochranou údajů stejné povinnosti jako na zpracovatele,
- byl správcem nápomocen při zajišťování dodržování povinností správce ohledně zachování důvěrnosti údajů, oznamování incidentů týkajících se bezpečnosti údajů, vyřizování žádostí subjektu údajů a posuzování dopadů na soukromí,
- dle volby správce po uplynutí doby trvání nebo ukončení poskytování služeb vymazal nebo vrátil správcem veškeré údaje + vymazal existující kopie (ledaže je zpracovatel ze zákona povinen údaje uchovávat; v takovém případě není zpracovatel oprávněn tyto údaje uchovávat déle, než vyžaduje zákon), a
- akceptoval jakékoli audity ze strany správce za účelem ověření dodržování smlouvy a právních povinností zpracovatele ohledně ochrany údajů.

PPF je, co se týče zpracování osobních údajů, většinou považována za správce. Při sdílení osobních údajů s externí osobou (např. externími poskytovateli služeb), měli byste ověřit, zda tato třetí osoba bude jednat jako správce, nebo jako zpracovatel. V druhém jmenovaném případě by externí strana měla údaje zpracovávat pouze vaším jménem a měla by s PPF uzavřít písemnou smlouvu, která obsahuje ustanovení o ochraně osobních údajů.

Pokud PPF určí způsob zpracování společně s jiným správcem, musí být jasně vymezeny příslušné povinnosti obou správců ohledně zpracování, včetně povinností vůči subjektům údajů, zejména pokud jde o informační povinnosti (viz bod 2.3).

2. KLÍČOVÉ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ

Každé zpracování osobních údajů musí splňovat následující klíčové zásady ochrany osobních údajů. Osobní údaje musí být:

1. zpracovávány na základě právního důvodu (podmínky zpracování)
2. zpracovávány pro omezený okruh účelů (zásada účelového omezení)
3. zpracovávány způsobem, který je pro subjekt údajů transparentní (zásada transparentnosti)

4. přiměřené, relevantní a omezené na rozsah, který je nezbytný k dosažení účelu, pro který jsou zpracovávány (zásada minimalizace údajů)
5. přesné a v případě potřeby aktualizované (zásada správnosti)
6. uchovávány jen po dobu nezbytnou pro účely, pro které jsou zpracovávány, a poté zničeny nebo anonymizovány (zásada omezení uchovávání)
7. zpracovávány v souladu s právy subjektů údajů
8. zpracovávány bezpečně a důvěrně (zásada integrity a důvěrnosti)
9. předávány příjemcům mimo EU pouze, pokud jsou splněny určité podmínky

Tyto zásady jsou podrobněji vysvětleny níže.

2.1 Podmínky zpracování

PPF může zpracovávat osobní údaje pouze v případě, že byla splněna alespoň jedna z těchto podmínek:

- fyzická osoba, jíž se osobní údaje týkají, udělila souhlas se zpracováním,
- zpracování je nezbytné:
 - v souvislosti se smlouvou, kterou fyzická osoba uzavřela, nebo
 - protože fyzická osoba požádala PPF o něco, co je třeba učinit, aby mohla uzavřít smlouvu,
- zpracování je nezbytné z důvodu právní povinnosti PPF (kromě povinností vyplývajících ze smlouvy),
- zpracování je nezbytné pro ochranu „životně důležitých zájmů“ fyzické osoby. Tato podmínka se použije pouze v otázkách života a smrti, například v případech, kdy je po závažném pracovním úrazu sdělena příslušné nemocnici anamnéza fyzické osoby,
- zpracování je nezbytné ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.
- zpracování je nezbytné pro účely oprávněných zájmů PPF (nebo jakékoli třetí osoby, jíž jsou údaje sdělovány) a tyto zájmy nejsou převáženy zájmy ani základními právy fyzických osob, jejichž údaje jsou zpracovávány. (zpracování na základě oprávněného zájmu)

Další pokyny ke každému z těchto důvodů pro zpracování jsou uvedeny v příloze č. 2.

Požadavky na právní důvody pro zpracování citlivých osobních údajů jsou přísnější, takže citlivé osobní údaje mohou být například zpracovávány v případě, že:

- subjekt údajů dal souhlas se zpracováním, nebo
- zpracování je nezbytné pro splnění právní povinnosti.

2.2 Zpracování omezené účelem (zásada účelového omezení)

Osobní údaje mohou být zpracovávány pouze pro konkrétní účely, které byly sděleny subjektu údajů v okamžiku, kdy byly údaje poprvé shromážděny.

To znamená, že osobní údaje nesmějí být shromažďovány pro jeden účel a poté využity pro jiný. Bude-li nutné změnit účel, pro který jsou údaje zpracovávány, jste před jakýmkoli zpracováním povinni o novém účelu informovat subjekt údajů, přičemž může být nezbytné získat jeho předchozí souhlas.

2.3 Transparentní zpracování (zásada transparentnosti)

Fyzickým osobám musí být poskytnuty určité informace o zpracování jejich osobních údajů. Rozsah informací, které je třeba poskytnout, závisí na tom, zda jste osobní údaje získali přímo od fyzických osob.

Tyto informace musí být poskytovány stručným, transparentním, srozumitelným a snadno přístupným způsobem, v jasném a jednoduchém jazyce. PPF nemůže za poskytnutí těchto informací účtovat žádný poplatek.

Následující tabulka shrnuje, jaké informace musí být poskytnuty fyzickým osobám a v jaké fázi.

Jaké informace musí být poskytnuty?	Údaje získány přímo od fyzické osoby	Údaje nezískány přímo od fyzické osoby
Totožnost a kontaktní údaje správce a pověřence pro ochranu osobních údajů (pokud PPF jmenovala pověřence pro ochranu osobních údajů)		
Účel zpracování a právní základ zpracování		
Případně oprávněné zájmy správce nebo třetí osoby		
Kategorie osobních údajů		
Jakýkoli příjemce nebo kategorie příjemců osobních údajů		
Podrobné informace o předání údajů do třetích zemí a o zárukách		
Doba uchovávání nebo kritéria používaná pro stanovení doby uchovávání		
Existence všech práv subjektů údajů (právo na přístup, opravu, výmaz, omezení zpracování jeho osobních údajů apod.)		

Jaké informace musí být poskytnuty?	Údaje získány přímo od fyzické osoby	Údaje nezískány přímo od fyzické osoby
Právo kdykoli odvolat souhlas (je-li relevantní)		
Právo podat stížnost u dozorového úřadu		
Zdroj, ze kterého osobní údaje pocházejí, a informace o tom, zda pocházejí z veřejně dostupných zdrojů		
Zda je poskytnutí osobních údajů součástí právního či smluvního požadavku nebo povinnosti a možné důsledky neposkytnutí osobních údajů		
Existence automatizovaného rozhodování, včetně profilování a informace o rozhodovacím procesu, jeho významu a důsledcích.		

V následující tabulce je uvedeno, kdy je PPF povinna tyto informace poskytnout.

	Údaje získány přímo od fyzické osoby	Údaje nezískány přímo od fyzické osoby
Kdy by měly být informace poskytnuty?	V okamžiku získání údajů od fyzické osoby.	- v přiměřené lhůtě po získání údajů (nejpozději do jednoho měsíce), - nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace, nebo - nejpozději před zpřístupněním osobních údajů, pokud je má správce v úmyslu zpřístupnit jinému příjemci.

2.4 Přiměřené, relevantní a omezené na to, co je nezbytné pro účely zpracování (zásada minimalizace údajů)

Nariadení GDPR vyžaduje, abyste zajistili, že shromažďujete osobní údaje pouze pro účely, které jste uvedli. Jste rovněž povinni zajistit, aby osobní údaje, které shromažďujete, byly pro účely, pro které byly shromažďovány, dostatečné.

Neměli byste uchovávat více osobních údajů, než potřebujete. Uchovávané osobní údaje by také neměly obsahovat nepotřebné informace.

Tuto zásadu shromažďování a uchovávání pouze minimálního nezbytného množství informací je obzvláště nutné dodržovat v případě citlivých osobních údajů.

Pokud potřebujete uchovávat určité informace pouze o některých fyzických osobách, měli byste je shromažďovat pouze ve vztahu k těmto fyzickým osobám – v souvislosti s jinými osobami bude pravděpodobně stejné množství informací nepřiměřené a nepotřebné. Zaměstnavatel například uchovává údaje o krevních skupinách všech svých zaměstnanců. Někteří z nich vykonávají nebezpečnou práci a tyto informace jsou potřebné pro případ nehody. U ostatních pracovníků však budou takové informace pravděpodobně nepotřebné a nepřiměřené.

Neměli byste uchovávat osobní údaje jen pro případ, že by se v budoucnu mohly hodit. Je však přípustné uchovávat informace pro předvídatelné události, které nikdy nemusí nastat, jako v uvedeném příkladu krevních skupin.

2.5 Přesné a v případě potřeby aktualizované (zásada správnosti)

Nařízení GDPR vám ukládá povinnost zajistit přesnost osobních údajů, které zpracováváte. Kde je to třeba, musí být také aktualizovány.

Abyste vyhověli těmto ustanovením, měli byste:

- činit přiměřené kroky k zajištění správnosti veškerých osobních údajů, které získáte,
- zajistit, aby veškeré osobní údaje měly jasný zdroj,
- pečlivě zvážit cokoli, co zpochybňuje přesnost informací, a
- zvážit, zda je nezbytné informace aktualizovat.

2.5.1 Kdy jsou osobní údaje „přesné“ nebo „nepřesné“?

Nařízení GDPR nevymezuje výraz „přesný“, ale uvádí, že osobní údaje jsou nepřesné, pokud jsou v jakémkoli ohledu nesprávné či zavádějící. Obvykle je zřejmé, zda jsou informace správné či nikoli. Například, pokud se fyzická osoba přestěhovala z Budapešti do Prahy, je zřejmé, že záznam uvádějící, že v současnosti žije v Budapešti, je nepřesný. Záznam uvádějící, že tato osoba někdy v minulosti žila v Budapešti, však zůstane i nadále přesný, přestože tam fyzická osoba už nežije. Vždy musí být jasné, co má záznam ukazovat.

2.5.2 Musí být osobní údaje vždy aktuální?

To záleží na tom, k čemu jsou údaje používány. Pokud jsou informace používány k účelu, který spoléhá na jejich aktuálnost, pak je třeba zajistit jejich aktualizaci. Vaše mzdové záznamy by například měly být aktualizovány, pokud dojde ke zvýšení mzdy.

Za jiných okolností bude obdobně zřejmé, že informace aktualizovány být nemusí.

2.5.3 Co jsou „přiměřené kroky“?

Záleží na okolnostech, zejména na povaze osobních údajů a na tom, k čemu jsou používány. Čím důležitější je správnost osobních údajů, tím větší úsilí byste měli věnovat zajištění jejich správnosti. Pokud budete používat údaje k rozhodnutím, která mohou významně ovlivnit dotyčnou fyzickou osobu nebo jiné osoby, musíte vynaložit větší úsilí k zajištění správnosti. To může znamenat, že bude nutné správnost údajů nezávisle ověřit. Většina zaměstnavatelů například musí zkontrolovat přesné podrobnosti o vzdělání, kvalifikaci a pracovních zkušenostech uchazečů o zaměstnání pouze, pokud jsou pro danou pozici zásadní, pokud by bylo třeba získat oficiální ověření.

2.6 Uchovávány jen po dobu nezbytnou pro účely, pro které jsou zpracovávány, a poté zničeny nebo anonymizovány (zásada omezení uchovávání)

Nařízení GDPR nestanoví žádnou konkrétní minimální ani maximální dobu uchovávání osobních údajů. Namísto toho uvádí, že osobní údaje zpracovávané pro konkrétní účel nebo účely nesmí být uchovávány po dobu delší než nezbytně nutnou k tomuto účelu nebo účelům.

V praxi to znamená, že musíte:

- kontrolovat dobu, po kterou osobní údaje uchováváte,
- při zvažování zda (a jak dlouho) údaje uchovávat vzít v potaz účel, pro který tyto údaje uchováváte.
- bezpečně vymazat údaje, které již pro tento účel nebo tyto účely nejsou potřebné, a
- aktualizovat, archivovat nebo bezpečně vymazat zastaralé údaje.

2.7 Zpracovávány v souladu s právy subjektů údajů

Fyzické osoby, jejichž osobní údaje zpracováváte, mají řadu práv.

2.7.1 Právo být informován

Viz kapitolu 2.3.

2.7.2 Právo na přístup k osobním údajům

Fyzické osoby mají právo na:

- potvrzení, zda jsou jejich osobní údaje zpracovávány,
- přístup ke svým osobním údajům a
- další doplňující informace – do značné míry se shodují s informacemi, které by měly být poskytnuty v rámci oznámení o ochraně osobních údajů (viz kapitolu 2.3).

PPF je povinna poskytnout kopii těchto informací bezplatně. PPF je však oprávněna účtovat „přiměřený poplatek“¹:

- je-li žádost zjevně neodůvodněná nebo nepřiměřená, zejména pokud je opakovaná, nebo
- za vyhovění žádosti o další kopie stejných informací. To neznamená, že můžete účtovat veškeré následné žádosti o přístup.

Když obdržíte žádost o přístup, jste povinni poskytnout požadované informace neprodleně, a to nejpozději do jednoho měsíce od doručení žádosti.²

Pokud jsou žádosti zjevně neopodstatněné nebo nepřiměřené, zejména proto, že se opakují, PPF je oprávněna:

¹ Tento poplatek se musí zakládat na administrativních nákladech spojených s poskytnutím informací.

² Toto období můžete prodloužit o další dva měsíce, pokud jsou žádosti složité nebo četné. V takovém případě jste povinni informovat fyzickou osobu do jednoho měsíce od doručení žádosti a vysvětlit, proč je odklad nezbytný.

- účtovat přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací, nebo
- odmítnout vyhovět žádosti. Odmítnete-li žádosti vyhovět, musíte fyzické osobě vysvětlit důvod a upozornit ji, že má právo podat stížnost příslušnému orgánu dozoru pro ochranu osobních údajů nebo zahájit soudní řízení. PPF musí tyto informace poskytnout bez zbytečného odkladu, nejpozději ve lhůtě jednoho měsíce.

Když obdržíte žádost o přístup, musíte nejprve ověřit totožnost osoby, která žádost podala, např. tak, že požádáte subjekt údajů o poskytnutí naskenované kopie dokladu totožnosti.

Pokud je žádost podána elektronicky, měli byste informace poskytnout v běžně používaném elektronickém formátu (např. formát Word, Excel, PDF).

2.7.3 Právo na opravu

Fyzické osoby mohou požádat PPF, aby opravila osobní údaje, které o nich uchovává, pokud jsou údaje nepřesné nebo neúplné. Pokud fyzická osoba požádá PPF o opravu svých osobních údajů a pokud PPF sdělila dotčené osobní údaje třetím osobám (např. nesprávný věk jednatele zmíněný ve výročním přehledu PPF), je povinna informovat fyzickou osobu:

- o opravě, pokud je to možné, a
- případně o třetích osobách, jimž byly údaje sděleny.

PPF musí na žádost o opravu reagovat do jednoho měsíce.³

Pokud na základě žádosti o opravu nebudete přijímat žádná opatření, musíte fyzické osobě vysvětlit důvod a upozornit ji, že má právo podat stížnost příslušnému orgánu dozoru pro ochranu osobních údajů nebo zahájit soudní řízení.

2.7.4 Právo na výmaz

Právo na výmaz je rovněž označováno jako „právo být zapomenut“. Základním principem tohoto práva je umožnit fyzické osobě požadovat výmaz nebo odstranění osobních údajů, není-li žádný závažný důvod k tomu, aby PPF osobní údaje nadále zpracovávala.

Právo na výmaz neposkytuje absolutní „právo být zapomenut“. Fyzické osoby mají právo na výmaz osobních údajů a na zamezení jejich zpracování za určitých okolností:

- pokud již osobní údaje nejsou potřebné k účelu, pro který je PPF původně shromáždila/zpracovala,
- pokud fyzická osoba odvolá souhlas,
- pokud fyzická osoba vznesl námitku proti zpracování a neexistuje převažující oprávněný zájem PPF na dalším zpracování osobních údajů,
- pokud byly osobní údaje zpracovány protiprávně,
- pokud musí být osobní údaje vymazány za účelem splnění právní povinnosti,
- pokud jsou osobní údaje zpracovávány v souvislosti s online nabídkou služeb nebo produktů nezletilé osobě.

³ Tuto lhůtu je možno prodloužit o dva měsíce, pokud je žádost o opravu složitá.

Existují určité konkrétní okolnosti, kdy se právo na výmaz neuplatní a PPF může odmítnout žádosti vyhovět. PPF může například odmítnout vyhovět žádosti o výmaz, pokud jsou osobní údaje zpracovávány k následujícím účelům:

- splnění právní povinnosti (např. pokud je PPF povinna zpracovávat údaje o zaměstnancích za účelem splnění úkolu, který je PPF povinna plnit podle vnitrostátních právních předpisů v oblasti sociálního zabezpečení v České republice, Maďarsku, Nizozemsku, Polsku, Slovensku, Švédsku, Itálii, Německu),
- splnění úkolu prováděného ve veřejném zájmu nebo výkon veřejné moci, nebo
- výkon nebo obhajoba právních nároků.

2.7.5 Právo na omezení zpracování

Fyzické osoby mohou požádat PPF, aby omezila zpracování jejich osobních údajů. Když je zpracování omezeno, PPF je oprávněna osobní údaje uchovávat, nikoli však dále zpracovávat. PPF si poté může o fyzické osobě ponechat právě tolik informací, aby zajistila, že bude toto omezení v budoucnu dodržováno.

PPF bude povinna omezit zpracování osobních údajů za těchto okolností:

- pokud fyzická osoba zpochybní správnost svých osobních údajů, PPF by měla omezit jejich zpracování, dokud jejich správnost neověří.
- pokud fyzická osoba vznesla námitku proti zpracování (pokud bylo zpracování nezbytné ke splnění úkolu ve veřejném zájmu nebo pro účely oprávněných zájmů), a vy zvažujete, zda oprávněné důvody PPF převažují nad zájmy fyzické osoby,
- pokud je zpracování protiprávní a fyzická osoba nesouhlasí s výmazem a žádá místo toho o omezení,
- pokud PPF osobní údaje už nepotřebuje, ale fyzická osoba požaduje osobní údaje k uplatnění, výkonu či obraně právního nároku.

2.7.6 Právo na přenositelnost údajů

Právo na přenositelnost údajů umožňuje fyzickým osobám získat a opětovně použít své osobní údaje pro vlastní účely napříč různými službami. To jim umožňuje jednoduše a bezpečně přesunout, kopírovat nebo předávat osobní údaje z jednoho IT prostředí do jiného, aniž by tím byla omezena použitelnost.

Právo na přenositelnost údajů se uplatní (každé z těchto tří kritérií musí být splněno):

- pouze na osobní údaje, které fyzická osoba poskytla správci,
- pouze pokud je zpracování založeno na souhlasu fyzické osoby nebo na plnění smlouvy a
- pouze pokud se zpracování provádí automatizovanými prostředky⁴.

Když PPF obdrží žádost o výkon práva na přenositelnost údajů, je povinna poskytnout osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu. K otevřeným formátům patří soubory CSV, XML nebo JSON. Strojově čitelným formátem se rozumí to, že jsou tyto informace strukturovány tak, aby z nich bylo možné softwarově extrahovat specifické prvky.

⁴ Další informace o „automatizovaných prostředcích“ naleznete v oddíle 1.4.

Pokud o to fyzická osoba požádá, může být PPF povinna předat osobní údaje přímo jiné organizaci, je-li to technicky proveditelné. PPF však není povinna přijmout nebo používat systémy zpracování, které jsou technicky slučitelné se systémy jiných organizací.

2.7.7 Právo vznést námitku

Fyzické osoby mají právo vznést námitku proti:

- zpracování na základě oprávněných zájmů nebo plnění úkolu ve veřejném zájmu/výkonu veřejné moci,
- přímému marketingu (včetně profilování) a
- zpracování pro účely vědeckého/historického výzkumu a statistiky.

Jak má PPF vyhovět vznesené námitce?

- i) *Pokud PPF zpracovává osobní údaje pro účely právního úkolu nebo oprávněných zájmů PPF*

Fyzické osoby musí vznést námitku z „důvodů týkajících se jejich konkrétní situace“. V takovém případě musí PPF ukončit zpracování osobních údajů, leda že:

- můžete prokázat závažné oprávněné důvody pro zpracování, které převažují nad zájmy, právy a svobodami dotčené osoby, nebo
- údaje jsou zpracovávány za účelem určení, výkonu nebo obrany právních nároků.

PPF je povinna informovat fyzické osoby o tom, že mají právo vznést námitku, v okamžiku první komunikace s dotčenou osobou a v oznámení o ochraně osobních údajů.

Fyzickou osobu je třeba na tuto skutečnost výslovně upozornit, a to jasně a odděleně od jakýchkoli jiných informací poskytovaných fyzické osobě.

- ii) *Pokud PPF zpracovává osobní údaje pro účely přímého marketingu*

PPF musí přestat zpracovávat osobní údaje pro účely přímého marketingu, jakmile obdrží námitku. Neexistují žádné výjimky ani důvody, na jejichž základě by mohla odmítnout.

PPF musí vyřídit námitku proti zpracování pro účely přímého marketingu kdykoli a bezplatně.

PPF je povinna informovat fyzické osoby o tom, že mají právo vznést námitku, v okamžiku první komunikace s dotčenou osobou a v oznámení o ochraně osobních údajů.

Fyzickou osobu je třeba na tuto skutečnost výslovně upozornit, a to jasně a odděleně od jakýchkoli jiných informací poskytovaných fyzické osobě.

2.7.8 Práva související s automatizovaným rozhodováním včetně profilování

Právní předpisy o ochraně osobních údajů chrání fyzické osoby před rozhodnutím prováděným bez jakéhokoli lidského zásahu, které by mohlo mít negativní důsledky.

Fyzické osoby mají právo nebýt podřízeny rozhodnutí:

- pokud je rozhodnutí založeno na automatizovaném zpracování a
- má právní účinky nebo má na fyzickou osobu obdobně významný vliv.

Příkladem výše uvedeného by byla situace zaměstnance, jehož mzda je přímo spojena s jeho produktivitou a jehož produktivita je měřena zcela automatizovanými prostředky.

PPF musí zajistit, aby fyzické osoby měly možnost:

- zajistit si lidský zásah,
- vyjádřit svůj názor,
- získat odůvodnění rozhodnutí a napadnout jej.

Toto právo se nevztahuje na rozhodnutí:

- nezbytná k uzavření nebo plnění smlouvy mezi PPF a fyzickou osobou,
- dovolená zákonem (např. pro účely předcházení podvodům nebo daňovým únikům), nebo
- na základě výslovného souhlasu.

Právo se navíc nevztahuje na případy, kdy rozhodnutí na nikoho nemá právní či obdobně významné účinky.

Co ještě říká nařízení GDPR o profilování?

Právní předpisy o ochraně osobních údajů omezují také „profilování“ fyzických osob. Profilování je jakákoli forma automatizovaného zpracování údajů, jejímž účelem je vyhodnotit některé osobní aspekty fyzické osoby, zejména analyzovat nebo předvídat prvky jako jsou například:

- pracovní výkon,
- ekonomická situace,
- zdravotní stav,
- osobní preference,
- spolehlivost, nebo
- chování.

Při zpracování osobních údajů pro účely profilování musí PPF zajistit zavedení vhodných záruk. Ty zahrnují přinejmenším záruku:

- poskytnout fyzické osobě smysluplné informace o použitém postupu, o významu a předpokládaných důsledcích,
- používat k profilování vhodné matematické nebo statistické postupy,
- zavést vhodná technická a organizační opatření, aby bylo možno opravovat nepřesnosti a minimalizovat riziko chyb,
- zabezpečit osobní údaje způsobem, který je přiměřený riziku hrozícímu zájmům a právům fyzické osoby a zabrání diskriminujícím dopadům.

Automatizovaná rozhodnutí se nesmí zakládat na zpracování citlivých osobních údajů, pokud PPF nezíská od fyzické osoby výslovný souhlas.

2.7.9 Způsoby řešení žádostí subjektů údajů

Na každou žádost subjektu údajů, která se týká jeho práva na přístup, opravu, výmaz, omezení zpracování či námitek proti zpracování svých osobních údajů, jakož i na jakékoli uplatnění práv souvisejících s přenositelností údajů a automatizovaným rozhodováním (včetně profilování) (viz oddíly 2.7.2 až 2.7.8 výše), je třeba reagovat podle následujících pokynů:

- informace musí být poskytnuty písemně, případně elektronicky,
- informace musí být poskytnuty bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti,
- bude-li lhůta jednoho měsíce překročena, lze ji s přihlédnutím ke složitosti a počtu žádostí prodloužit až o další dva měsíce, pokud je subjekt údajů o prodloužení a důvodech prodloužení informován,
- rozhodne-li se PPF nepřijmout v reakci na žádost žádné opatření, musí to subjektu údajů zdůvodnit, a to bez zbytečného odkladu, v každém případě do jednoho měsíce od podání žádosti,
- informace musí být poskytnuty subjektu údajů bezplatně (s výjimkou případů, kdy je žádost zjevně nedůvodná nebo nepřiměřená, např. je-li opakovaná).

2.7.10 Oznámení příjemcům osobních údajů

Kdykoli subjekt údajů požádá PPF o opravu, výmaz nebo omezení zpracování svých osobních údajů (viz články 2.7.3 až 2.7.5 výše), musí PPF o této žádosti informovat příjemce takových osobních údajů, je-li to možné a nebude-li to vyžadovat nepřiměřené úsilí.

Například o žádosti bývalého zaměstnance, který žádá PPF o výmaz svých osobních údajů, je PPF povinna informovat:

- interní účetní oddělení PPF, pokud jsou osobní údaje zpracovávány prostřednictvím samostatné účetní databáze, a
- nezávislého poskytovatele cloudových služeb, který poskytuje PPF služby personálního oddělení a/nebo mzdové účtárny.

PPF je povinna subjektu údajů na žádost poskytnout seznam příjemců.

2.8 Zpracovávání bezpečně a důvěrně (zásada integrity a důvěrnosti)

2.8.1 Povinnost zavést bezpečnostní opatření

Osobní údaje podléhají povinnosti zachovávat důvěrnost. Jakékoli neoprávněné shromažďování, zpracování nebo užití takových údajů zaměstnanci je zakázáno. Jakékoli zpracování údajů prováděné zaměstnancem, který není oprávněn osobní údaje zpracovávat v rámci svých povinností, je neoprávněné. Zaměstnanci mohou mít přístup k osobním údajům pouze v rozsahu přiměřeném vzhledem k typu a rozsahu daného úkolu. Zaměstnancům je zakázáno používat osobní údaje pro soukromé či obchodní účely, sdělit je neoprávněným osobám nebo je jinak zpřístupnit.

Nařízení GDPR vyžaduje zavedení vhodných technických a organizačních opatření, aby byla zajištěna úroveň zabezpečení odpovídající riziku, které vyplývá ze zpracování (např. náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněné zpřístupnění nebo přístup k osobním údajům). Tato opatření zahrnují například:

- pseudonymizaci a šifrování osobních údajů,

- schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,
- schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů,
- proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Tato povinnost zůstává v platnosti i po skončení pracovního poměru. To platí bez ohledu na to, zda jsou údaje zpracovávány elektronicky nebo v tištěné podobě. Před zavedením nových metod zpracování údajů, zejména nových počítačových systémů, je třeba definovat a zavést technická a organizační opatření na ochranu osobních údajů.

Kdy jsou bezpečnostní opatření vhodná?

Nařízení GDPR nestanoví podrobná pravidla pro určení, zda jsou bezpečnostní opatření vhodná.

Při rozhodování o této záležitosti musíte zohlednit následující kritéria:

- stav techniky v oblasti bezpečnostních technologií a postupů,
- náklady na provedení opatření,
- povahu, rozsah, kontext a účel zpracování údajů

Co je to porušení zabezpečení osobních údajů?

Jakékoli porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění osobních údajů přenášených, uložených nebo jinak zpracovávaných PPF. To znamená, že porušením zabezpečení není jen ztráta osobních údajů.

2.8.2 povinnost hlásit případy porušení zabezpečení osobních údajů.

PPF je povinna ohlásit některé druhy porušení zabezpečení osobních údajů příslušnému dozorovému úřadu pro ochranu osobních údajů a v některých případech i dotčeným fyzickým osobám.

Příklady porušení zabezpečení osobních údajů:

- *Ztráta nebo odcizení dat nebo zařízení, na kterých jsou údaje uchovávány.* Například: před opuštěním pracoviště si zaměstnanec stáhne tabulky s kontaktními údaji zákazníků (včetně jmen, e-mailových adres a telefonních čísel kontaktních osob u vašich zákazníků) na USB disk. Když dorazí domů, uvědomí si, že USB disk ztratil ve vlaku.
- *Nevhodné způsoby kontroly přístupu, které umožňují neoprávněné užití.* Například: místní personální oddělení uložilo osobní údaje zaměstnanců (včetně údajů o mzdě apod.) na veřejný disk. Dokumenty byly dobu dvou týdnů k dispozici všem zaměstnancům PPF. Alespoň dva zaměstnanci PPF k údajům získali přístup a jeden z nich si je zkopíroval, když ukončoval pracovní poměr.

- *Selhání vybavení.* Například: došlo k fyzickému poškození serverů jednoho z externích poskytovatelů cloudových služeb PPF, což vedlo ke ztrátě některých osobních údajů zaměstnanců PPF.
- *Lidská chyba.* Například: váš externí poskytovatel služeb mzdové účtárny omylem zaslal dokumenty o zaměstnancích PPF (včetně údajů o mzdě atd.) jinému zákazníkovi, přičemž nebyl dodržen běžný postup pro předávání údajů.
- *Útok hackerů na vaše počítačové systémy nebo počítačové systémy provozované externím poskytovatelem služeb, který nakládá s osobními údaji vašim jménem.* Například: externí poskytovatel cloudových služeb, který poskytuje hosting vaší databáze CRM, se stal obětí rozsáhlého hackerského útoku.
- *Spoofingový útok, kde jsou informace získány uvedením v omyl.* Například: zaměstnanec je uveden v omyl a klikne na odkaz v podvodné e-mailové zprávě, čímž umožní hackerovi na dálku zkopírovat celou databázi CRM.

PPF je povinna o porušení zabezpečení informovat příslušný dozorový úřad pro ochranu osobních údajů, pokud je pravděpodobné, že toto porušení bude mít za následek riziko pro práva a svobody fyzických osob. Pokud by nebylo vyřešeno, mohlo by vyústit v závažné nepříznivé dopady na fyzické osoby, například diskriminaci, poškození pověsti, finanční ztrátu, ztráty důvěrnosti nebo jakékoli jiné významné hospodářské či sociální znevýhodnění.

Toto je třeba řešit v každém případě jednotlivě. Pokud například dojde ke ztrátě osobních údajů zákazníků, které může vyústit v možnost krádeže identity fyzických osob, je PPF povinna informovat příslušný dozorový úřad pro ochranu osobních údajů.

Kromě toho, pokud je pravděpodobné, že porušení vyúští ve vysoké riziko pro práva a svobody fyzických osob, musí PPF informovat přímo dotčené osoby. Z použitého termínu „vysoké riziko“ vyplývá, že úroveň rizika, při kterém je nutné informovat příslušnou fyzickou osobu, je vyšší než v případě dozorového orgánu.

Jak oznámit porušení zabezpečení?

Pokud se dozvíte o porušení zabezpečení osobních údajů, které se může dotknout osobních údajů zpracovávaných PPF nebo jejím jménem, měli byste okamžitě informovat svého nadřízeného a právní oddělení.

PPF je povinna oznamovat případy porušení zabezpečení osobních údajů v pevně stanovených lhůtách (do 72 hodin příslušnému dozorovému úřadu pro ochranu osobních údajů a bez zbytečného odkladu dotčeným fyzickým osobám). Proto musíte jakékoli porušení zabezpečení osobních údajů, o němž se dozvíte, oznámit co nejdříve.

2.9 Předávání příjemcům mimo EU pouze, pokud jsou splněny určité podmínky

2.9.1 Co je to předávání osobních údajů?

Předávání údajů zahrnuje:

- zasílání osobních údajů z jedné země do jiné (například: dceřiná společnost v Maďarsku zašle personální údaje společnosti PPF v Nizozemsku), nebo

- umožnění osobě v jedné zemi přístup k osobním údajům uchovávaným v jiné zemi (například: PPF umožňuje poskytovatelům služeb IT ze Spojených států vzdálený přístup do databáze CRM⁵ v Maďarsku za účelem provedení určitých kroků v souvislosti s údaji uvedenými v databázi CRM).

2.9.2 Předávání osobních údajů v rámci EHP

Osobní údaje mohou být volně předávány mezi subjekty na území EHP⁶. Je tedy přípustné, aby spřízněná osoba (např. v České republice, Nizozemsku, Polsku nebo na Slovensku) zasílala personální údaje do ústředí společnosti v Maďarsku (za předpokladu, že spřízněná osoba splnila své ostatní povinnosti týkající se ochrany osobních údajů).

2.9.3 Předávání údajů z EU příjemcům mimo EHP

Správce je oprávněn předávat osobní údaje pouze do zemí mimo EHP (**třetí země**), které poskytují odpovídající úroveň ochrany údajů. Rozhodnutí, zda země poskytuje odpovídající úroveň ochrany údajů, může správce založit na rozhodnutí Evropské komise. Na základě určitých podmínek Evropská komise shledala, že odpovídající úroveň ochrany poskytují Andora, Argentina, Faerské ostrovy, Guernsey, Izrael, Jersey, Kanada, Ostrov Man, Nový Zéland, Švýcarsko, Uruguay.⁷

Neposkytuje-li třetí země odpovídající úroveň ochrany údajů, není správce oprávněn předávat osobní údaje žádné osobě usazené v této třetí zemi (**dovozce údajů**), s výjimkou případů, kdy:

- fyzická osoba udělila svůj výslovný souhlas s navrhovaným předáním poté, co byla informována o možných rizicích takového předávání,
- předání je nezbytné pro splnění smlouvy mezi fyzickou osobou a organizací nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost fyzické osoby,
- předání je nezbytné pro splnění smlouvy, která byla uzavřena v zájmu fyzické osoby mezi správcem a jinou osobou,
- předání je nezbytné z důležitých důvodů veřejného zájmu,
- předání je nezbytné pro určení, výkon nebo obhajobu právních nároků. Účelem této výjimky je například usnadnit předávání osobních údajů od správce usazeného v EHP správci usazenému ve Spojených státech v případě, že je takové předání nezbytné k tomu, aby správce mohl stanovit nebo vykonat právní nárok nebo se bránit proti právnímu nároku vznesenému třetí osobou. Upozorňujeme, že se opravdu jedná o výjimku. Proto nelze touto výjimkou odůvodnit systematické předávání osobních údajů správci usazenému v USA založené pouze na tom, že může někdy v budoucnu dojít k soudnímu řízení,
- předání je nezbytné k ochraně životně důležitých zájmů subjektu údajů nebo jiných osob v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit svůj souhlas,
- jsou předávány údaje z rejstříku, který je podle vnitrostátních (tj. českých, maďarských, nizozemských, polských, slovenských, švédština, italština, němčina) právních předpisů nebo práva Evropské unie určen k poskytování informací veřejnosti (a je přístupný široké veřejnosti, nebo osobám, které mohou prokázat oprávněný zájem pro nahlédnutí do rejstříku),

⁵ Ačkoli jsou zákazníci PPF právníckými (a nikoli fyzickými) osobami, bude databáze CRM pravděpodobně obsahovat kontaktní údaje osob pracujících pro zákazníky PPF. Tyto kontaktní údaje budou osobními údaji.

⁶ Do EHP patří členské státy EU, Island, Lichtenštejnsko a Norsko.

⁷ Aktuální seznam takzvaných „rozhodnutí o odpovídající ochraně“ naleznete na [internetových stránkách Evropské komise](#).

- správce a dovozce údajů (jednající jako správce nebo zpracovatel předávaných osobních údajů) uzavřeli smlouvu o poskytnutí dostatečných smluvních záruk. Dne 4. června 2021 vydala Komise modernizované standardní smluvní doložky podle GDPR pro předávání údajů od správců nebo zpracovatelů v EU/EHP (nebo jinak podléhajících GDPR) správcům nebo zpracovatelům usazeným mimo EU/EHP (a nepodléhajících GDPR). Vzorové doložky jsou dostupné na [internetových stránkách Evropské komise](#).
- v rámci skupiny lze využít také jednostranné závazky (tzv. **závazná interní pravidla**). Závazná interní pravidla jsou souborem závazných pravidel, která mohou být zavedena, aby nadnárodní skupiny mohly předávat osobní údaje, kterými disponují, z EHP svým spřízněným osobám mimo EHP v souladu s vnitrostátními a evropskými právními předpisy o ochraně osobních údajů. Závazná interní pravidla se nevztahují na předávání osobních údajů mimo skupinu.

Existují také další výjimky. Ty však pro PPF nejsou příliš relevantní.

3. ODPOVĚDNÝ PŘÍSTUP K OCHRANĚ SOUKROMÍ

3.1 Zásada odpovědného přístupu k ochraně soukromí

Nařízení GDPR od společností vyžaduje odpovědný přístup k ochraně soukromí. To znamená, že PPF není jen povinná dodržovat nařízení GDPR, ale musí také být kdykoli schopna dodržování předpisů doložit.

Jak můžete doložit, že dodržujete předpisy? Nařízení GDPR vyžaduje, aby společnosti zavedly vhodná technická a organizační opatření, kterými zajistí a doloží dodržování předpisů:

- zavedení interních zásad ochrany osobních údajů (např. zásady ochrany osobních údajů personálního oddělení)
- organizování školení na téma ochrany osobních údajů pro zaměstnance, kteří pracují s osobními údaji
- provádění interních auditů činností zpracování
- vedení příslušné dokumentace o činnostech zpracování
- v případě potřeby jmenování pověřence pro ochranu osobních údajů
- zavedení opatření, která splňují principy záměrné a standardní ochrany osobních údajů. Tato opatření mohou zahrnovat:
 - minimalizaci údajů,
 - pseudonymizaci,
 - transparentnost a
 - průběžné vytváření a zlepšování bezpečnostních prvků
- je-li to vhodné a nutné, posouzení vlivu na ochranu osobních údajů.

Níže naleznete podrobnější informace o některých výše uvedených opatřeních.

3.2 Vedení záznamů o činnostech zpracování

PPF je povinná vést interní záznamy o činnostech zpracování údajů.

Interní záznamy musí obsahovat tyto informace:

- jméno a údaje PPF (a případně jiných správců) a vašeho pověřence pro ochranu osobních údajů
- různé účely, pro něž PPF zpracovává osobní údaje
- popis kategorií fyzických osob a kategorií osobních údajů, které PPF zpracovává
- kategorie příjemců, s nimiž PPF sdílí osobní údaje (např. externí poskytovatelé služeb IT, externí poskytovatelé personálních služeb (headhunteri, společnosti poskytující služby výběru a naboru pracovníků apod.),
- podrobnosti předávání do třetích zemí včetně dokumentace souvisejících ochranných mechanismů (např. použití vzorových doložek),
- plány uchovávání záznam,
- popis technických a organizačních bezpečnostních opatření k ochraně údajů.

PPF může mít povinnost zpřístupnit tyto záznamy příslušnému dozorovému úřadu pro ochranu osobních údajů pro účely šetření.

3.3 Záměrná a standardní ochrana osobních údajů

Záměrnou ochranou osobních údajů se rozumí, že do každé fáze vývoje nového systému nebo procesu, který bude využívat osobní údaje (a do celého cyklu zpracování údajů) musíte začlenit dostatečné záruky ochrany soukromí (jako je pseudonymizace a minimalizace údajů).

Pro vyhodnocení „dostatečnosti“ záruk je třeba zohlednit následující kritéria:

- stav techniky
- náklady na začlenění záruk
- povahu, rozsah, kontext a účel zpracování údajů. Například pokud je nový systém určen k zpracování velkých objemů osobních údajů, musí být ochranná opatření na ochranu soukromí přesnější a přísnější než u zpracování v menším rozsahu.
- rizika pro fyzické osoby, která mohou být způsobena zpracováním. Například pokud je nový systém určen k zpracování citlivých osobních údajů fyzických osob, musí být ochranná opatření na ochranu soukromí přesnější a přísnější, než kdyby zpracovávání údajů novým systémem bylo méně invazivní.

Standardní ochranou osobních údajů se rozumí, že pokud systém poskytuje uživateli možnost volby ve vztahu ke zpracování jeho údajů a uživatel volbu žádným způsobem nevyužije, bude systém zpracovávat osobní údaje nejméně invazivním způsobem. Tato povinnost se týká množství osobních údajů shromážděných systémem, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti.

3.4 Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů (**posouzení nebo DPIA**) (označované také jako posouzení vlivu na soukromí nebo PIA) je nástrojem, který umožňuje PPF určit nejúčinnější způsob, jak splnit povinnosti v oblasti ochrany osobních údajů a splnit očekávání fyzických osob ohledně ochrany jejich soukromí. Účinné posouzení umožní PPF identifikovat a řešit problémy v rané fázi, snížit související náklady a zamezit poškození pověsti, k němuž by jinak mohlo dojít.

PPF musí posouzení provést, pokud:

- používá nové technologie a

- je pravděpodobné, že zpracování bude představovat velké riziko pro práva a svobody fyzických osob Příklady vysoce rizikového zpracování:
 - systematické a rozsáhlé hodnocení fyzických osob, které je založeno na automatizovaném zpracování a které se používá pro přijímání rozhodnutí s právními účinky (nebo obdobně významné účinky pro fyzickou osobu),
 - rozsáhlé zpracování citlivých osobních údajů (např. údaje o zdravotním stavu nebo osobní údaje týkající se rozsudků v trestních věcech nebo trestných činů),
 - systematické monitorování veřejných prostor ve velkém rozsahu (kamerový systém).

Každé posouzení musí obsahovat:

- popis operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce,
- posouzení nezbytnosti a přiměřenosti zpracování z hlediska účelů,
- posouzení rizik pro fyzické osoby a
- opatření zavedená ke zmírnění rizik pro fyzické osoby včetně bezpečnostních opatření a doložení souladu s právními předpisy o ochraně osobních údajů.

4. CO SE STANE, KDYŽ PŘEDPISY NEDODRŽÍTE?

Od 25. května 2018 se výrazně zvýšily pokuty. Bude existovat dvouúrovňový systém správních pokut, který bude uplatnitelný na správce i zpracovatele.

Za některé typy porušení (například ustanovení týkající se vedení záznamů o zpracování – viz článek 3.2) lze uložit pokutu ve výši až 10,000,000 EUR nebo až 2 % celosvětového ročního obratu PPF v předchozím účetním období, podle toho, která hodnota je vyšší.

Jiné typy porušení (např. porušení podmínek zpracování/podmínek pro získání souhlasu) podléhají vyšším pokutám ve výši až 20,000,000 EUR nebo až 4 % celosvětového ročního obratu PPF v předchozím účetním období, podle toho, která hodnota je vyšší.

Úřady pro ochranu osobních údajů mohou prosazovat dodržování nařízení také jinými způsoby stanovenými vnitrostátními právními předpisy, které se v současnosti ve členských státech EU výrazně liší. Úřady pro ochranu osobních údajů jsou oprávněny do zpracování zasahovat, například vydáním stanoviska před tím, než zpracování proběhne, nebo nařízením ukončení zpracování, výmazu a zničení údajů. Úřady pro ochranu osobních údajů mohou rovněž provádět audity a stíhat porušení nařízení GDPR. Obecně budou vymáhací pravomoci harmonizovány podle nařízení GDPR (ačkoli trestní stíhání je přeneseno na členské státy EU). Mezi vymáhací pravomoci patří pravomoc vydávat upozornění, napomenutí a nařízení správcům a zpracovatelům, ukládat dočasné nebo trvalé zákazy zpracování, nařídit přerušování toků údajů do zahraničí nebo nařídit opravu nebo výmaz osobních údajů.

Soudy mohou nařídit:

- zabavení jakýchkoli nosičů, které obsahují zpracované osobní údaje,
- soud může nařídit PPF výmaz jakýchkoli dotčených osobních údajů nebo mu zakázat zpracování jakýchkoli dotčených osobních údajů,
- občanskoprávní odpovědnost za škodu způsobenou porušením povinností v oblasti ochrany osobních údajů.

Zprávy o jakémkoli porušení ochrany osobních údajů, které může být relevantní pro veřejnost, mohou rovněž zveřejnit média.

5. **SCHVÁLENÍ, OBDOBÍ PŘEZKUMU, MONITOROVÁNÍ**

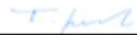
Tyto Zásady byly přezkoumány, projednány a schváleny Výkonným výborem PPF. Zásady by měly být pravidelně revidovány a aktualizovány, nejméně však jednou ročně.

V případě porušení Zásad společnost PPF vynaloží veškeré prostředky k jejich odstranění a přijme nezbytná právní a jiná disciplinární opatření, která jsou povolena příslušnými právními řády.

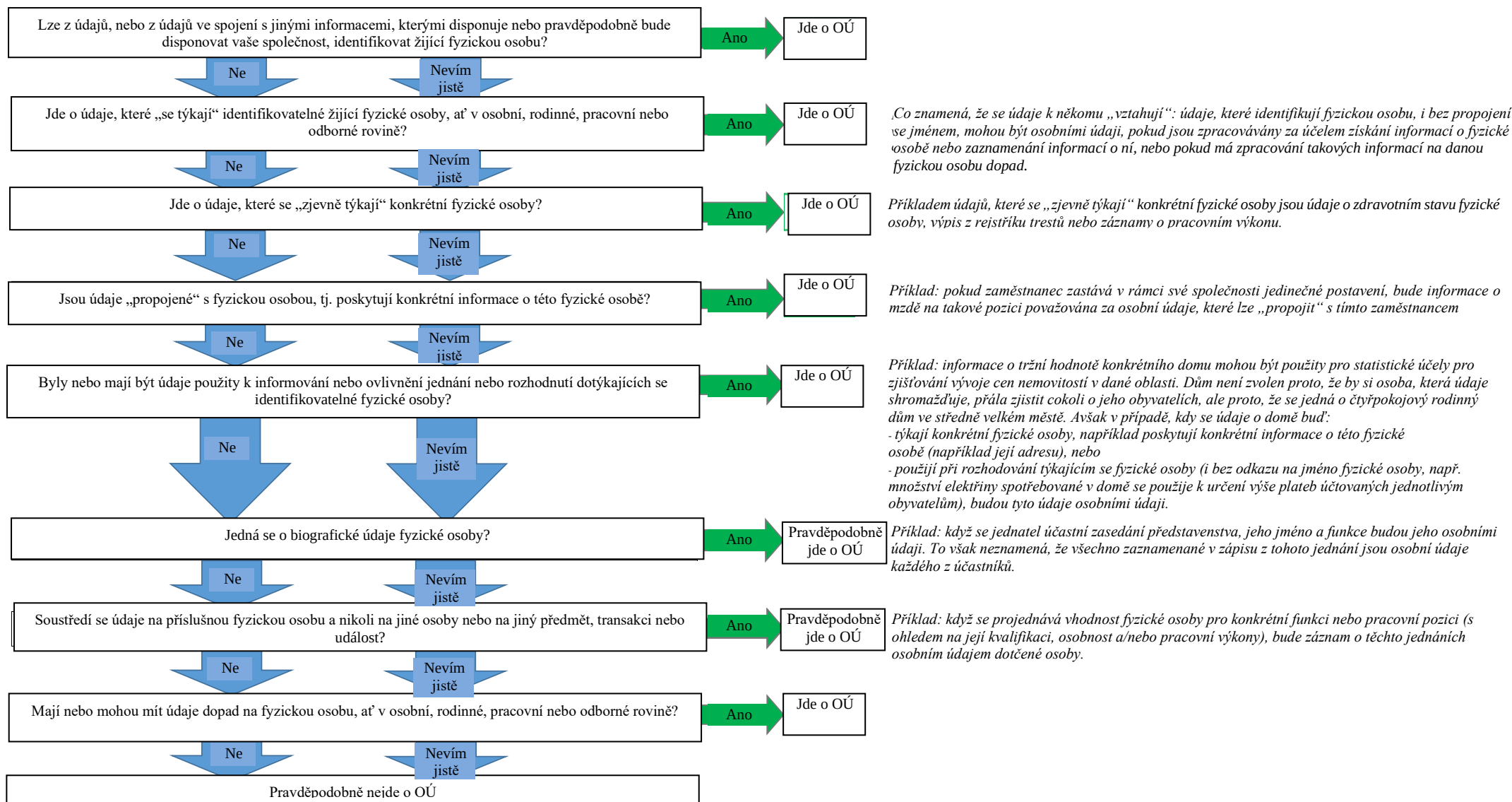

GERALD KÜHR
CEO


MARIEKE HOORNEMAN
CHIEF PEOPLE OFFICER


STÉPHANE RE
CFO


TORSTEN JACOBS
COO

PŘÍLOHA Č. 1 – SCHÉMA – CO JSOU OSOBNÍ ÚDAJE (OÚ)?



PŘÍLOHA Č. 2 – DALŠÍ POKYNY OHLEDNĚ PODMÍNEK ZPRACOVÁNÍ

<i>Právní důvody pro zpracování osobních údajů (kromě citlivých osobních údajů)</i>	<i>Další pokyny</i>
Souhlas dotčené osoby	Souhlas musí představovat svobodný, konkrétní, informovaný a jednoznačný projev vůle fyzické osoby. Jinak řečeno souhlas vyžaduje nějakou formu jednoznačného potvrzení. Mlčení, předem zaškrtnutá políčka nebo nečinnost nemohou být považovány za souhlas. Souhlas musí být ověřitelný. To znamená, že musíte nějakým způsobem vést záznamy o tom, jak a kdy byl souhlas udělen. Prohlášení o souhlasu musíte pro účely vedení záznamů získat v písemné nebo elektronické podobě. Při zahájení pracovního poměru můžete osobní údaje uchazečů zpracovávat na základě jejich souhlasu. Odmítne-li PPF uchazeče, musíte své údaje v souladu s požadovanou dobou uchovávání vymazat, ledaže by uchazeč souhlasil s tím, že o něm záznamy nadále povedete pro budoucí výběrová řízení. V případě, že bude během výběrového řízení nutné získat informace o uchazeči od třetí osoby, musíte dodržovat požadavky příslušných vnitrostátních právních předpisů. V případě pochybností si musíte od uchazeče vyžádat souhlas. Fyzické osoby mají právo souhlas kdykoli odvolat. Nezapomeňte, že zpracování může probíhat i na jiném právním základě, například v případech, kdy je nezbytné pro účely oprávněných zájmů PPF nebo oprávněných zájmů třetí osoby.
Zpracování je nezbytné pro plnění smlouvy s fyzickou osobou nebo pro provedení opatření s cílem uzavřít smlouvu	To se vztahuje pouze na zpracování, které je nezbytně nutné pro plnění smlouvy. Samotná skutečnost, že zpracování údajů souvisí se smlouvou nebo je obsaženo v podmínkách smlouvy, nemusí nutně znamenat, že je zpracování pro plnění smlouvy nezbytně nutné.

Právní důvody pro zpracování osobních údajů (kromě citlivých osobních údajů)	Další pokyny
	Položte si otázku: může PPF plnit smlouvu, aniž by údaje zpracovala? Pokud je odpověď kladná, není zpracování údajů k plnění smlouvy nutné. V pracovněprávních vztazích je PPF oprávněna zpracovávat osobní údaje, je-li to nezbytné k uzavření, plnění nebo ukončení pracovní smlouvy. PPF například musí znát čísla bankovních účtů svých zaměstnanců, aby mohla plnit své povinnosti vyplývající z pracovních smluv, které s nimi uzavřela. Jinak řečeno PPF nemůže plnit své závazky vyplývající z těchto pracovních smluv, aniž by zpracovala čísla bankovních účtů zaměstnanců. Pokud jde o stávající pracovní poměr a neuplatní se žádná z okolností pro oprávněné zpracování údajů, musí se zpracování údajů vždy týkat účelu pracovní smlouvy. PPF je oprávněna zpracovávat osobní údaje příslušných potenciálních a stávajících zákazníků a partnerů za účelem sjednání, podpisu a ukončení smlouvy. Před uzavřením smlouvy – během fáze jednání o smlouvě – je PPF oprávněna zpracovávat osobní údaje za účelem přípravy nabídek nebo objednávek nebo splnění jiných požadavků potenciálních zákazníků, které se týkají uzavření smlouvy. PPF je oprávněna v průběhu přípravy smlouvy potenciální zákazníky kontaktovat s využitím informací, které jí poskytl. PPF musí dodržovat jakákoli omezení, která si potenciální zákazníci vyžádají. Pro zpracování osobních údajů, které souvisí s pracovním poměrem, ale nebylo původně součástí plnění pracovní smlouvy, musí existovat zákonné oprávnění. To může spočívat v právních požadavcích, kolektivních smlouvách se zástupci zaměstnanců, souhlasu zaměstnance nebo oprávněném zájmu společnosti.
Zpracování je nezbytné z důvodu právní povinnosti PPF (kromě povinností vyplývajících ze smlouvy).	Sem patří pouze jednoznačné a konkrétní právní povinnosti vyplývající z evropských právních předpisů, vnitrostátních (českých, maďarských, nizozemských, polských, slovenských, švédský, italský, německý) zákonů nebo zákonů jiného členského státu EU. V případě nezávazných pokynů (například regulačních orgánů) nebo v případě právní povinnosti vyplývající se zákonů jiného státu (např. Spojených států) zvažte, zda může PPF vycházet z legitimního zájmu.

<i>Právní důvody pro zpracování osobních údajů (kromě citlivých osobních údajů)</i>	<i>Další pokyny</i>
Zpracování je nezbytné pro ochranu životně důležitých zájmů fyzické osoby.	Tato podmínka se použije pouze v otázkách života a smrti, například v případech, kdy je po závažném pracovním úrazu sdělena příslušné nemocnici anamnéza fyzické osoby.
Zpracování je nezbytné pro účely oprávněných zájmů PPF (nebo jakékoli třetí osoby, již jsou údaje sdělovány) a tyto zájmy nejsou převáženy zájmy ani základními právy fyzických osob, jejichž údaje jsou zpracovávány.	Pokud se PPF nebude moci dovolávat žádného z výše uvedených právních důvodů zpracování údajů (souhlas, plnění smlouvy, právní povinnost apod.), zvažte, zda se může PPF dovolávat oprávněného zájmu. Oprávněné zájmy jsou obecně právní (např. vymáhání splatných pohledávek) nebo obchodní povahy (např. předcházení porušení smlouvy). Příloha č. 3 k těmto Zásadám ochrany osobních údajů obsahuje kontrolní seznam, který vám pomůže zjistit, zda se můžete tohoto základu pro zpracování dovolávat.

PŘÍLOHA Č. 3 – KDY SE MŮŽETE DOVOLÁVAT OPRÁVNĚNÉHO ZÁJMU?

Následující kroky vám pomohou posoudit, zda se může PPF dovolávat oprávněného zájmu:

⇒ **Krok 1** – ověřte, zda je váš zájem:

- v souladu s evropskými právními předpisy, vnitrostátními (českými, maďarskými, nizozemskými, polskými, slovenskými, švédský, italský, německý) zákony nebo zákony jiného členského státu EU a
- dostatečně jasné formulovaný, aby bylo možné ověřit jeho vyváženost proti zájmům a základním právům fyzické osoby (tj. dostatečně konkrétní) a
- skutečný a aktuální (tj. není spekulativní).

⇒ **Krok 2** – zvažte, zda existují jiné méně invazivní prostředky k dosažení stejného účelu a splnění zájmu.

⇒ **Krok 3** – posuďte, zda nad zájmem správce nepřevažují základní práva nebo zájmy fyzických osob. Při tomto posuzování zohledněte tyto skutečnosti:

- případné znevýhodnění PPF (a/nebo třetích osob), pokud by ke zpracování osobních údajů nedošlo
- povahu údajů, které hodláte zpracovávat (citlivé údaje? „běžné“ údaje?)
- status fyzické osoby (nezletilý, zaměstnanec, zákazník atd.)
- způsob zpracování údajů (velký rozsah, vytěžování dat, pokročilá analýza, profilování, sdělení velkého počtu osob nebo zveřejnění)
- přiměřená očekávání fyzické osoby
- porovnejte dopad zpracování na danou fyzickou osobu s přínosem, který má ze zpracování mít PPF

⇒ **Krok 4** – pokud váš zájem nepřeváží nad zájmem fyzické osoby, zaveďte další vhodná ochranná opatření, aby byla zachována rovnováha zájmů. Taková ochranná opatření mohou zahrnovat například:

- minimalizaci údajů (např. přísné omezení shromažďování údajů nebo okamžité vymazání údajů po použití),

- technická a organizační opatření, která zajistí, aby údaje nemohly být použity k podniknutí jiných kroků týkajících se fyzických osob („funkční oddělení“),
- rozsáhlé využívání anonymizačních technik, agregace údajů, technologií zvyšujících ochranu soukromí, záměrnou ochranu osobních údajů,
- zvýšení transparentnosti (tj. poskytnutí podrobných informací o způsobu, jakým bude PPF údaje zpracovávat; vysvětlíte důvody, proč se domníváte, že vaše zájmy nejsou převáženy zájmy fyzické osoby),
- poskytnutí bezpodmínečného práva zpracování odmítnout (opt-out), pokud není stanoveno platnými právními předpisy o ochraně osobních údajů.

Podrobnosti o revizích a aktualizacích zásad

Název:	Zásady ochrany osobních údajů Skupiny PPF
Číslo verze:	V3
Datum účinnosti této verze:	1. listopadu 2024
Autorizováno:	Výkonný výbor PPF
Rozsah:	Všechny společnosti Skupiny PPF a jejich zaměstnanci
Cyklus revize:	Každoročně ode dne účinnosti
Odpovědnost za přezkumný cyklus:	Právní poradce

Historie revizí:	
Datum: 1. srpna 2018 Schváleno:	Vytvoření V1 Zásad ochrany osobních údajů Skupiny PPF Výkonný výbor PPF
Datum: 1. srpna 2023 Schváleno:	Nabytí účinnosti V2 Zásad ochrany osobních údajů Skupiny PPF Výkonný výbor PPF
Datum: 1. listopadu 2024 Schváleno:	Dodatek k Chief People Officer (V3) Výkonný výbor PPF