

SMĚRNICE NA OCHRANU OSOBNÍCH ÚDAJŮ

1. Úvodní ustanovení

1.1 Účel

Účelem této směrnice je stanovit všeobecně platnou metodiku pro nakládání a zpracování osobních údajů v Cestovní agentuře FITDOVČA tak, aby byly zajištěny podmínky ochrany stanovené nařízením Evropského parlamentu a Rady č. 2016/679 ze dne 27.4.2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení o ochraně osobních údajů“), zákonem č. 101/2000 Sb., o ochraně osobních údajů, a to za účelem zajištění jejich řádné ochrany a zabránění jejich úniku, vyzrazení, zneužití, zničení a zamezení jejich ztrát.

Tato směrnice upravuje postupy Cestovní agentury FITDOVČA při nakládání s osobními údaji, pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů. Směrnice stanovuje hlavní a jednoznačné zásady odpovědnosti, povinnosti a pravomoci při zpracování osobních údajů a nastavení ochrany osobních údajů.

S ohledem na obecné nařízení o ochraně osobních údajů tato směrnice zejména stanovuje povinnost, aby se zpracovávaly pouze ty osobní údaje, které jsou potřeba k výkonu činností Cestovní agentury FITDOVČA. Směrnice dále popisuje proces zpracování osobních údajů tak, aby se vynaložila veškerá péče na snížení rizik zneužití, nesprávného nakládání nebo neoprávněného zpracování osobních údajů.

1.2 Základní pojmy a používané zkratky

Bezpečnostní incident	jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, při které došlo nebo mohlo dojít k porušení ochrany osobních údajů, bez ohledu na závažnost.
Dozorový úřad	V České republice Úřad na ochranu osobních údajů
Nařízení GDPR	Obecné nařízení o ochraně osobních údajů (ang. General Data Protection Regulation neboli GDPR)
Ochrana OÚ	Soubor opatření v oblasti personální, administrativní, fyzické ochrany a informační bezpečnosti potřebných pro zajištění ochrany OÚ.
Osobní údaj (OÚ)	Veškeré informace o identifikované či identifikovatelné fyzické osobě (subjektu údajů); na základě kterých lze konkrétní fyzickou osobu přímo či nepřímo identifikovat; zejména odkazem na určitý identifikátor; například jméno, identifikační číslo, nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.
Souhlas subjektu údajů	Jakýkoli svobodný, konkrétní, informovaný a jednorázový projev vůle, který subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svým OÚ.

Správce OÚ	Pro účely této směrnice je správcem Bc. et. Bc. Anna Vlčková, DiS., spoluprovozovatelka Cestovní agentury FITDOVČA (dále jen „CA FITDOVČA“) – správce OÚ určuje účel a prostředky zpracování OÚ, provádí zpracování a odpovídá za něj. Správce může zmocnit nebo pověřit zpracováním OÚ zpracovatele.
Subjekt údajů	Fyzická osoba, k níž se OÚ vztahují. Subjekt údajů se považuje za identifikovaný, nebo identifikovatelný, jestliže lze na základě jednoho či více OÚ přímo či nepřímo zjistit jeho identitu.
Zpracovatel OÚ	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává OÚ pro správce.
Zpracování OÚ	Jakákoliv operace nebo soubor operací s OÚ nebo soubory OÚ, 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.
Zvláštní kategorie údajů (citlivé údaje)	OÚ, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

2. Odpovědnost, povinnosti a pravomoci

2.1 CA FITDOVČA

CA FITDOVČA je povinna:

- vytvořit, udržovat a řídit systém ochrany osobních údajů v souladu s obecným nařízením o ochraně osobních údajů a zákonem o ochraně osobních údajů,
- stanovit způsoby, účely, prostředky a místa zpracování osobních údajů,
- zajistit zpracovávání pouze přesných osobních údajů výhradně v souladu s účelem, k němuž byly shromážděny, a to v rozsahu nezbytném pro naplnění stanoveného účelu,
- zajistit informování subjektů údajů, popř. získat jejich souhlasy se zpracováním,
- zabezpečit smluvní závazání spolupracujících právnických i fyzických osob (jako jsou např. dodavatelé, spolupracující společnosti), které v rámci své činnosti používají osobní údaje zpracovávané cestovní agenturou a pro její potřeby zpracovávají, a zabezpečit dodržování obecného nařízení o ochraně osobních údajů, zákon o ochraně osobních údajů a souvisejících obecně závazných předpisů a požadavků na ochranu osobních údajů,
- zajistit dodržování technických a organizačních opatření zaměřených na zabezpečení a ochranu osobních údajů,
- zajistit posouzení vlivu na ochranu osobních údajů, pokud je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob,

- zajistit ochranu a bezpečnost osobních údajů, a to od zahájení jejich zpracovávání až do chvíle, kdy jsou likvidovány,
- spolupracovat s dozorovým úřadem a působit jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování osobních údajů,
- vystupovat jako kontaktní místo pro subjekty údajů, které se na něj mohou obracet v případech, kdy došlo k porušení zpracování jejich osobních údajů a v případech výkonu jejich práv podle obecného nařízení o ochraně osobních údajů a zákona o ochraně osobních údajů,
- vést centrální evidenci požadavků subjektů údajů,
- vést centrální evidenci souhlasů se zpracováním osobních údajů,
- vést centrální evidenci neshod a bezpečnostních incidentů,
- řešit a vyšetřovat bezpečnostní incidenty vzniklé v souvislosti s ochranou osobních údajů, analyzovat jejich příčiny a zajišťovat nápravná opatření,
- provádět kontrolu dodržování obecného nařízení o ochraně osobních údajů a zákona o ochraně osobních údajů,
- zajistit, aby CA FITDOVČA byla schopna řádně doložit plnění povinností při ochraně osobních údajů, které vyplývají z právních předpisů.

3. Zpracování osobních údajů

3.1 Subjekty údajů

Subjekty údajů CA FITDOVČA jsou:

- zákazník (zájemce o poskytované služby),
- obchodní partneři – fyzické osoby nebo zástupci právnických osob

V souvislosti s identifikací subjektu údajů je třeba posoudit, jaký je účel zpracovávání a zda je ke zpracovávání nutný souhlas subjektu údajů nebo zda je zpracování osobních údajů možné na základě jiného právního titulu (uzavření nebo plnění smlouvy, plnění právní povinnosti, oprávněný zájem apod.).

Dále je nutné stanovit způsob získávání osobních údajů od subjektu, zejména s ohledem na to, aby nedocházelo k využívání údajů získaných k jinému účelu, případně ke slučování údajů získaných k jiným účelům, a způsob plnění informační povinnosti správce vůči subjektu údajů.

3.2 Účel zpracování osobních údajů

CA FITDOVČA odpovídá za stanovení účelu zpracovávání osobních údajů a rozsah využívaných údajů. Osobní údaje lze zpracovávat pouze s ohledem na platné právní předpisy ČR a obecné nařízení o ochraně osobních údajů v souladu s účelem, k němuž byly shromážděny. Zpracovávat je k jinému účelu je možné jen tehdy, pokud o této změně zpracování byl subjekt údajů informován, a nelze-li takové zpracování provádět na základě právního titulu nevyžadujícího předchozí souhlas, pokud k tomu dal subjekt údajů souhlas.

V rámci CA FITDOVČA jsou zpracovávány osobní údaje za následujícím účelem:

a) zákazník (zájemce o poskytované služby)

- plnění smlouvy a poskytování služeb,
- komunikace se subjekty údajů,
- informování o změnách a novinkách v nabídce služeb a produktů (oprávněný zájem),
- splnění právní povinnosti (archivnictví),
- účetní a daňové účely,
- vedení zákaznické evidence (na základě výslovného souhlasu),
- marketingové a propagační účely (na základě výslovného souhlasu),

b) obchodní partneři

- uzavření a plnění smlouvy,
- komunikace se subjekty údajů,
- splnění právní povinnosti,
- účetní a daňové účely.

3.3 Doba zpracování osobních údajů

Osobní údaje pro tyto činnosti jsou zpracovány po dobu nezbytně nutnou k zajištění vzájemných práv a povinností vyplývajících ze smlouvy o poskytování služeb a po jejím skončení bude s nimi naloženo dle platné právní úpravy, zejména zákona č. 499/2004 Sb. (zákon o archivnictví a spisové služby a o změně některých zákonů). Poté jsou osobní údaje vymazány či anonymizovány.

3.4 Rozsah zpracovávaných osobních údajů

Rozsah zpracovávaných osobních údajů musí být stanoven tak, aby splnil stanovený účel, a přímo nebyly shromažďovány a zpracovávány nadbytečné osobní údaje.

3.5 Zdroje osobních údajů

Osobní údaje jsou získávány především od subjektu údajů, zejména při jednání o smlouvě k provedení opatření před uzavřením smlouvy, při uzavírání smlouvy a v průběhu smluvního vztahu.

3.6 Zpřístupnění osobních údajů a zpracování prostřednictvím zpracovatele

Osobní údaje mohou být pro zajištění výše popsaných účelů vedle CA FITDOVČA zpracovávány také některými dalšími externími společnostmi (tj. zpracovateli). Osobní údaje jsou těmto zpracovatelům předány pouze v tom případě, že splňují definované organizační a technické podmínky k zajištění jejich náležité ochrany. Zpracovatel není oprávněn zpracovávat osobní údaje k jinému účelu a jiným způsobem než smluvně dohodnutým. Podmínkou pro využití externího zpracovatele je uzavření Smlouvy o zpracování osobních údajů mezi správcem a zpracovatelem. Smlouva se zpravidla uzavírá jako samostatný dokument. Smlouva musí obsahovat veškeré náležitosti v souladu s čl. 28 odst. 3 obecného nařízení o ochraně osobních údajů.

4. Souhlas se zpracováním, informace o zpracovávání, ochrana a výkon práv subjektu údajů

4.1 Souhlas subjektu údajů

Pokud jsou osobní údaje zpracovávány na základě obecného nařízení o ochraně osobních údajů dle čl. 6 odst. 1 písm.:

- b) plnění smlouvy,
- c) splnění právní povinnosti,
- d) ochrana životně důležitých zájmů,
- e) veřejný zájem nebo výkon veřejné moci,
- f) oprávněný zájem,

není nutný souhlas subjektu údajů, ale je nutné zajistit informační povinnost vůči subjektu údajů.

V ostatních případech může CA FITDOVČA zpracovávat osobní údaje pouze s předchozím souhlasem subjektu údajů. Souhlas musí být poučený, informovaný a konkrétní, nejlépe v písemné podobě. Souhlas se získává pouze pro konkrétní údaje, na konkrétní dobu a pro konkrétní účel. Subjekt údajů má právo svůj souhlas kdykoli odvolat.

4.2 Informování subjektu údajů

CA FITDOVČA je povinna včas a řádně v souladu s článkem 13 a 14 obecného nařízení o ochraně osobních údajů ve stanoveném rozsahu informovat subjekt údajů o tom, že zpracovává jeho osobní údaje. Současně musí cestovní agentura informovat subjekt údajů o jeho právech vyplývajících mu z obecného nařízení o ochraně osobních údajů. Informační povinnost je naplněna zveřejněním dokument „Informace o zpracování osobních údajů“ na webových stránkách CA FITDOVČA, případně jako součást smlouvy se subjektem údajů.

4.3 Práva subjektu údajů

V souvislosti se zpracováním osobních údajů mají subjekty údajů možnost uplatňovat svá práva (viz dále). Vyřízení žádostí je poskytováno bezplatně, pouze v případě, že jsou žádosti nedůvodné, nebo nepřiměřené, může být uložen přiměřený poplatek.

4.4 Právo na přístup k informacím

Subjekt údajů má právo na jasné, transparentní a srozumitelné informace o tom, jak jsou jeho osobní údaje zpracovávány a jaká jsou jeho práva. K tomuto účelu slouží dokument „Informace o zpracování osobních údajů“. Subjekt údajů má právo na přístup k osobním údajům.

4.5 Právo na opravu osobních údajů

Subjekt údajů má právo na opravu nesprávných a neúplných osobních údajů.

4.6 Právo na výmaz

Subjekt údajů má právo na vymazání svých osobních údajů, především pokud (a) již nejsou dále potřebné pro další zpracování; (b) byl odvolán souhlas k jejich zpracování; (c) subjekt vznesl námitky vůči jejich zpracování, (d) byly zpracovány nezákonně; nebo (e) musejí být vymazány podle právních předpisů. Právo na výmaz nemůže být uplatněno v tom případě, že CA FITDOVČA zpracovává osobní údaje na základě jiného právního titulu, než se souhlasem subjektu (např. pro plnění smlouvy) a pro zpracování osobních údajů stále existuje důvod a účel (např. držení osobních údajů po dobu stanovenou zákonem).

4.7 Právo na přenositelnost údajů

Subjekt údajů má právo získat své osobní údaje a přenést je k jinému poskytovateli služeb.

5. Využívání osobních údajů pro zasílání obchodních sdělení (přímý marketing)

Z důvodu informování o novinkách v nabídce služeb a produktů zasílá CA FITDOVČA obchodní sdělení subjektům údajů za dodržení následujících podmínek:

- ✓ sdělení se týkají pouze vlastních produktů a služeb,
- ✓ sdělení jsou zasílána formou poštovní korespondence, SMS zprávy a e-mailu.

Zpracování osobních údajů za tímto účelem (tj. přímý marketing) je považováno za zpracování prováděné z důvodu oprávněného zájmu CA FITDOVČA. Pokud podá subjekt údajů námitku proti zpracování za účelem přímého marketingu, musí CA FITDOVČA zabezpečit, že danému subjektu údajů již nebudou nadále zasílána obchodní sdělení.

6. Ochrana osobních údajů

Pro zajištění bezpečnosti a důvěrnosti osobních údajů jsou v rámci CA FITDOVČA využívána vhodná technická a organizační opatření zejména na ochranu před neoprávněným přístupem k údajům a jejich zneužitím. Opatření jsou navržena tak, aby odpovídala stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.

6.1 Organizační opatření

Organizační opatření pro zajištění ochrany osobních údajů jsou následující.

- CA FITDOVČA všechny osobní údaje, se kterými nakládá a které zpracovává, chrání vhodnými a dostupnými prostředky před zneužitím. Osobní údaje jsou uchovávány v prostorách, na místech, v prostředí nebo v systému, do kterého má přístup omezený, předem stanovený, známý okruh osob; jiné osoby mohou získat přístup k osobním údajům pouze se svolením pověřené osoby.
- Dokumenty obsahující osobní údaje subjektů údajů jsou trvale uloženy v uzamykatelných skříních. Dokumenty nelze předávat cizím osobám nebo kopírovat a kopie poskytovat neoprávněným osobám.

- CA FITDOVČA alespoň jednou za rok provede zhodnocení postupů při nakládání a zpracování osobních údajů. Zjistí-li se, že některé postupy jsou zastaralé, zbytečné nebo se neosvědčily, učiní bezodkladně nápravu.

6.2 Technická opatření

Technická opatření pro zajištění ochrany osobních údajů jsou následující:

- elektronická evidence osobních údajů je vedena v zabezpečeném informačním systému. Při práci s elektronickou evidencí nesmí oprávněné osoby opouštět počítač bez odhlášení se, nemohou nechat nahlížet žádnou jinou osobu a musí chránit utajení přihlašovacích hesla a v případě nebezpečí jeho vyzrazení jej ihned změnit. Přístupy nastavuje pověřený zaměstnanec – správce sítě, který nastavuje potřebné zabezpečení dat.
- U informačních systémů musí být zajištěno logování, zálohování a obnova dat.