Vnitropodniková směrnice o ochraně osobních údajů

1. Úvod

Tato směrnice, v souladu s nařízením Evropského parlamentu a Rady 2016/679/EU o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů), upravuje způsoby nakládání s osobními údaji při jejich zpracování (dále jen **GDPR**).

2. Působnost směrnice

Tato směrnice je vnitřním předpisem společnosti Zdravotnické prodejny Eliška s.r.o. (dále správce), která je ve smyslu GDPR **správcem osobních údajů**.

Upravuje postup členů orgánů, zaměstnanců, spolupracujících osob a dalších pověřených osob při zpracování a ochraně osobních údajů fyzických osob, pro naplnění právních povinností stanovených GDPR.

3. Vymezení základních pojmů

- **Osobní údaj** – veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen "**subjekt údajů**"). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor. Osobními údaji jsou např. jméno a příjmení, adresa(y), datum narození, místo narození, rodné číslo, telefonní číslo, e-mail, síťový identifikátor, evidenční číslo zákazníka, dále pak jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby např. věk, pohlaví, národnost, rodinný stav, vzdělání, zaměstnání, majetkové poměry, příjmy a výdaje, počet dětí, údaje o chování, preferencích apod. (Data jsou osobními údaji až tehdy, kdy je možné je spárovat s konkrétní osobou.)
- **Zvláštní kategorie osobních údajů** - osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby či údaje o sexuálním životě nebo sexuální orientaci fyzické osoby a také údaje o **zdravotním stavu.**
- **Údaje o zdravotním stavu** – jsou osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.
- **Subjekt údajů** – jakákoli **fyzická osoba**, jejíž osobní údaje jsou zpracovávány
- **Správce osobních údajů** – podle GDPR každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí za jím stanoveným účelem jejich shromažďování, zpracování a uchování.
- **Zpracovatel osobních údajů** – jakákoli fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který jménem správce zpracovává osobní údaje
- **Příjemce osobních údajů** – jakákoli fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli (orgány veřejné moci, které mohou získávat osobní údaje na základě zákona v rámci zvláštního šetření se za příjemce nepovažují)
- **Zpracování osobních údajů** – jakýkoli úkon nebo soubor úkonů, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky (shromažďování, zaznamenání, uspořádání, strukturování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, nahlédnutí, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace)

- **Souhlas subjektu údajů** – jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů
- **Profilování** – jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů fyzické osoby (např. k rozboru či odhadu pracovního výkonu, ekonomické situace, zdravotního stavu, preferencí, zájmů, spolehlivosti, chování, místa pobytu nebo pohybu)
- **Pseudonymizace** – zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě
- **Porušením zabezpečení osobních údajů** – porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.
- **Dozorový úřad** – orgán veřejné moci v ČR, určeným pro kontrolu nakládání s osobními údaji, Úřad pro ochranu osobních údajů - ÚOOÚ, se sídlem Pplk. Sochora 727/27, Holešovice, 170 00, Praha 7, telefon: +420 234 665 111, web: www.uoou.cz

4. Zásady zpracování osobních údajů

Správce při zpracování osobních údajů dodržuje tyto zásady [čl. 5 GDPR]:

- **Zákonnost, korektnost a transparentnost**: osobní údaje ve vztahu k subjektu údajů jsou zpracovávány korektně a zákonným a transparentním způsobem.
- **Účelové omezení**: shromažďovány jsou osobní údaje pro určité, výslovně vyjádřené a legitimní účely a nejsou dále zpracovávány způsobem, který je s těmito účely neslučitelný (další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se nepovažuje za neslučitelné s původními účely).
- **Minimalizace údajů**: zpracování osobních údajů je přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.
- **Přesnost**: zpracování osobních údajů je přesné a v případě potřeby aktualizované, jsou přijímána veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.
- **Omezení uložení**: zpracovávané osobní údaje jsou uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány, po delší dobu jsou ukládány, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných GDPR s cílem zaručit práva a svobody subjektu údajů.
- **Integrita a důvěrnost**: osobní údaje jsou zpracovávány způsobem, který zajišťuje jejich náležité zabezpečení, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

5. PRÁVNÍ TITULY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Správce zpracovává osobní údaje pouze na základě těchto právních titulů [čl. 6 GDPR]:

- Subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů.

- Zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů.
- Zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje.
- Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.
- Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce.
- Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

6. ZÁZNAM O ČINNOSTECH ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Jméno a kontaktní údaje správce (kontaktní osoba pověřená ochranou osobních údajů):

- Eliška Daňková – jednatel – telefon 284 842 000

Pověřené osoby, které jsou oprávněny zpracovávat osobní údaje:

- členové statutárního orgánu (případně prokuristé) správce, ředitelé a osoby ve funkcích
- zaměstnanci správce
- osoby, které zabezpečují informační systémy pro zpracování osobních údajů
- jiné osoby mající oprávnění na základě uzavřené smlouvy o zpracování osobních údajů

Detail viz. Příloha.

7. PRÁVA SUBJEKTŮ OSOBNÍCH ÚDAJŮ

Správce garantuje subjektům osobních údajů tato práva:

Právo na informace a přístup k osobním údajům [čl. 12, 13 a 14 GDPR]:

Správce poskytuje subjektům ve stanovených lhůtách stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků zejména tyto informace:

- totožnost a kontaktní údaje správce, jeho zástupce (případně DPO),
- kategorie zpracovávaných osobních údajů
- zdroje zpracovávaných osobních údajů včetně případného údaje o původu z veřejně dostupných zdrojů
- účely zpracování, pro které jsou osobní údaje určeny
- právní základ (titul) pro zpracování
- oprávněné zájmy správce nebo třetí strany jsou-li právním titulem pro zpracování
- příjemce zpracovávaných osobních údajů
- případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci
- dobu po kterou budou osobní údaje zpracovávány či uloženy nebo způsob jejího určení
- existenci práva požadovat: přístup k osobním údajům, jejich opravu nebo výmaz, omezení jejich zpracování, vznést námitku proti zpracování, přenositelnost údajů

- existenci práva odvolat kdykoli souhlas se zpracováním je-li právním titulem pro zpracování, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním
- existenci práva podat stížnost u dozorového úřadu
- zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů
- že dochází k automatizovanému rozhodování či profilování, použité postupy a význam předpokládaných důsledků takového zpracování pro subjekt údajů
- záměr správce použít osobní údaje pro jiný účel, než pro který byly shromážděny

Právo na přístup k osobním údajům [čl. 15 GDPR]:

Správce garantuje subjektům právo získat potvrzení, zda osobní údaje týkající se subjektu jsou či nejsou zpracovávány, a pokud ano, garantuje subjektu právo získat přístup k těmto osobním údajům a k následujícím informacím

- účely zpracování
- kategorie dotčených osobních údajů
- příjemce nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny
- plánovanou dobu, po kterou budou osobní údaje uloženy nebo kritéria použitá ke stanovení této doby
- existenci práva požadovat od správce opravu nebo výmaz osobních údajů, nebo omezení jejich zpracování, nebo vznést námitku proti tomuto zpracování
- existenci práva podat stížnost u dozorového úřadu
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu
- že dochází k automatizovanému rozhodování či profilování, použité postupy a význam předpokládaných důsledků takového zpracování pro subjekt údajů
- pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci informaci o vhodných zárukách, které se na předání vztahují

Správce poskytne subjektu kopii zpracovávaných údajů, které se subjektu týkají.

Právo na opravu [čl. 16 GDPR]:

Správce bez zbytečného odkladu po žádosti subjektu provede opravu nebo doplnění nesprávných nebo neúplných osobních údajů, které o něm zpracovává.

Právo na výmaz [čl. 17 GDPR]:

Správce bez zbytečného odkladu po žádosti subjektu provede výmaz jeho osobních údajů, pokud:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány
- subjekt odvolá souhlas, na jehož základě byly údaje zpracovány a neexistuje žádný další právní důvod pro zpracování
- subjekt vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování, nebo subjekt údajů vznese námitky proti zpracování údajů pro účely přímého marketingu
- osobní údaje byly zpracovány protiprávně

- osobní údaje musí být vymazány ke splnění právní povinnosti
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti

Správce však výmaz osobních údajů neprovede, pokud je zpracování nezbytné:

- pro výkon práva na svobodu projevu a informace
- pro splnění právní povinnosti, jež vyžaduje zpracování nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen
- z důvodů veřejného zájmu v oblasti veřejného zdraví
- pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely, pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo cíle zpracování
- pro určení, výkon nebo obhajobu právních nároků

Právo na omezení zpracování [čl. 18 GDPR]:

Správce na žádost subjektu omezí zpracování jeho osobních údajů pokud:

- subjekt popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů, ale žádá místo toho o omezení jejich použití
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků
- subjekt z důvodů týkajících se jeho konkrétní situace vznesl námitku proti zpracování údajů zpracovávaných pro splnění úkolu
- ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce nebo pro účely oprávněných zájmů správce či třetí strany, a to na dobu, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu

Oznamovací povinnost ohledně opravy, výmazu nebo omezení zpracování [čl. 19 GDPR]:

Správce oznamuje příjemcům, jimž byly zpřístupněny osobní údaje, veškeré opravy, výmazy nebo omezení zpracování údajů s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt požaduje.

Právo na přenositelnost [čl. 20 GDPR]

Správce na žádost subjektu předá subjektu jeho osobní údaje, které zpracovává, ve strukturovaném, běžně používaném a strojově čitelném formátu a předá je jinému, subjektem určenému správci, pokud:

- je zpracování údajů založeno na souhlasu subjektu (s výjimkou případů, kdy podle práva nemůže být souhlas subjektem zrušen) nebo na plnění smlouvy uzavřené mezi správcem a subjektem či pro provedení opatření přijatých před uzavřením takové smlouvy a zpracování se provádí automatizovaně.

Správce přenos osobních údajů neumožní, pokud by tím byla nepříznivě dotčena práva a svobody jiných osob.

Právo vznést námitku [čl. 21 GDPR]:

Pokud subjekt z důvodů týkajících se jeho konkrétní situace vznese vůči správci námitku proti zpracování svých osobních údajů zpracovávaných správcem ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce nebo pro účely oprávněných zájmů příslušného správce či třetí strany (včetně profilování založeného na těchto důvodech), správce osobní údaje subjektu dále nezpracovává, pokud neprokáže závažné

oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků správce.

Pokud subjekt vznese námitku proti zpracování svých osobních údajů pro účely přímého marketingu (včetně profilování těchto údajů), nebude správce tyto osobní údaje pro účely přímého marketingu dále zpracovávat.

Právo na přezkum automatizovaného zpracování a profilování [čl. 22 GDPR]:

Správce umožní subjektu na jeho žádost, aby nebyl předmětem výhradně automatizovaného zpracování svých osobních údajů (včetně profilování) a umožní mu, aby zpracování (i profilování) jeho osobních údajů bylo přezkoumáno člověkem, pokud:

- automatizované zpracování (či profilování) není nezbytné k uzavření či plnění smlouvy mezi správcem a subjektem
- automatizované zpracování (či profilování) není povoleno závazným právním předpisem
- automatizované zpracování (či profilování) není založeno na výslovném souhlasu subjektu

Právo odvolat souhlas se zpracováním osobních údajů [čl. 7, odst. (2) GDPR]:

Pokud jsou osobní údaje zpracovávány na základě souhlasu subjektu [čl. 6 odst. (1) písm. a) nebo čl. 9 odst. (2) písm. a) GDPR] má subjekt právo svůj kdykoli odvolat, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním.

Právo podat stížnost u dozorového orgánu [čl. 77 GDPR]:

Správce, bez ohledu na jiná práva a jiné prostředky ochrany, informuje subjekty osobních údajů o právu podat proti porušení práv při zpracování jeho osobních údajů stížnost u dozorového úřadu, kterým je v České republice Úřad pro ochranu osobních údajů - ÚOOÚ,

se sídlem Pplk. Sochora 727/27, Holešovice, 170 00, Praha 7, telefon: +420 234 665 111, web: www.uoou.cz.

Subjekt údajů může svá práva vůči správci uplatnit podáním k těmto kontaktům:

statutární orgán správce: Eliška Daňková – jednatel

kontaktní osoba (případně DPO):

8. OHLAŠOVÁNÍ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Jakékoli porušení zabezpečení osobních údajů, je-li pravděpodobné, že toto porušení může mít za

následek riziko pro práva a svobody fyzických osob, správce bez zbytečného odkladu a pokud možno do 72

hodin od okamžiku, kdy se o něm dozvěděl, ohlásí Úřadu pro ochranu osobních údajů [čl. 33 GDPR]. V

ohlášení správce uvede nejméně tyto údaje:

- Popis povahy daného případu porušení zabezpečení osobních údajů včetně (pokud je to možné) kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů.
- Jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace.
- Popis pravděpodobných důsledků porušení zabezpečení osobních údajů
- Popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Pro ohlášení porušení zabezpečení osobních údajů dozorovému úřadu správce může využít formulář v příloze této směrnice.

Správce dokumentuje a uchovává veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů [čl. 34 GDPR]. V oznámení subjektu správce uvede:

- Jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace.
- Popis pravděpodobných důsledků porušení zabezpečení osobních údajů.
- Popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Oznámení porušení zabezpečení osobních údajů subjektu údajů správce neučiní, pokud:

- Zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup (například šifrování).
- Přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví.
- Oznámení by vyžadovalo nepřiměřené úsilí; v takovém případě budou subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

9. KONTROLA DODRŽOVÁNÍ SMĚRNICE

Správce zajišťuje prostřednictvím svého statutárního orgánu nebo jiné pověřené osoby (případně DPO) průběžnou kontrolu dodržování této směrnice. Její porušení ze strany svých zaměstnanců vyhodnocuje správce jako porušení právních povinností vztahujících se k vykonávané práci s následky uvedenými ve zvláštním zákoně.

10. PLATNOST A ÚČINNOST SMĚRNICE

Tato směrnice nabývá platnosti a účinnosti dnem 25. 5. 2018.

Správce je oprávněn a povinen obsah směrnice přizpůsobovat zněním rozhodných právních předpisů, vývoji poznatků v oblasti ochrany osobních údajů a faktickým změnám v činnosti a vybavení správce.

Účinné znění směrnice je vždy to, které je zveřejněno na internetových stránkách správce v okamžiku rozhodném pro vznik příslušných práv a povinností.