KODEX CHOVÁNÍ SPOLEČNOSTI
VitaLife Shop s.r.o.

ve smyslu nařízení Evropského parlamentu a Rady (EU) 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 „GDPR")

Preambule

Tento Kodex chování společnosti VitaLife Shop s.r.o. (dále jen „Kodex") stanovuje pravidla týkající se ochrany subjektu údajů v souvislosti se zpracováním jejich osobních údajů a dále pravidla týkající se volného pohybu jejich osobních údajů.

Tento Kodex chrání základní práva a svobody subjektu údajů, a zejména jejich právo na ochranu osobních údajů.

Cílem tohoto Kodexu je informovat subjekt údajů o zpracování jejich osobních údajů společností VitaLife Shop s.r.o.; informovat je o jejich právech a povinnostech společnosti VitaLife Shop s.r.o. ve vztahu ke zpracovávaným osobním údajům.

Článek I.
Vymezení základních pojmů

Pro účely GDPR se rozumí

1.1 osobními údaji veškeré informace o identifikované nebo identifikovatelné fyzické osobě, 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;

1.2 zpracováním jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. Bližší určení těchto operací je uvedeno v Příloze č. 1 Kodexu;

1.3 omezením zpracování označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;

1.4 správcem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;

1.5 zpracovatelem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

1.6 příjemcem subjekt, kterému jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoliv;

1.7 souhlasem 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;

1.8 dozorovým úřadem nezávislý orgán veřejné moci, který je pověřen monitorováním dodržování platných právních předpisů v souvislosti s ochranou osobních údajů. V případě České republiky se jedná o Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“);

1.9 oprávněným zaměstnancem takový zaměstnanec, který má na základě rozhodnutí vedoucího zaměstnance (případně jednatele společnosti/správce/oprávněného zástupce) přístup do prostor, kde dochází ke zpracování osobních údajů;

1.10 pověřencem taková osoba, kterou je povinen správce nebo zpracovatel zřídit za účelem poskytování informací a poradenství správci či zpracovateli, a která plní další úkoly ve smyslu čl. V. Kodexu;

1.11 pseudonymizací 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.

Článek II.
Základní zásady zpracování osobních údajů

2.1 Osobní údaje jsou

a) zpracovávány ve vztahu k subjektu údajů korektně a zákonným a transparentním způsobem;

b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely;

c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány;

d) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

2.2 Zákonným způsobem lze zpracovávat osobní údaje jen na základě jednoho z definovaných právních titulů, přičemž souhlas nesmí být v rozporu s právními předpisy.

2.3 Právním titulem mohou být:

a) souhlas subjektu údajů;

b) souvislost s plněním smlouvy;

c) plnění zákonem stanovené povinnosti;

d) ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) plnění úkolů ve veřejném zájmu nebo při výkonu veřejné moci;

f) oprávněné zájmy správce.

2.4 **Korektně a transparentně** jsou zpracovávány osobní údaje, jestliže není zastírán účel, pro který jsou osobní údaje zpracovány. Zároveň správce musí poskytnout informace subjektu údajů o způsobu, rozsahu a předávání osobních údajů.

2.5 **Účelovým omezením** se rozumí, že osobní údaje musí být shromážděny pro určité, výslovně vyjádřené legitimní účely a nesmějí být zpracovány způsobem, který je s těmito účely neslučitelný. K posouzení nezbytnosti zpracování na základě oprávněného zájmu správce je určena Příloha č. 3 Kodexu.

2.6 **Minimalizací údajů** se rozumí, že osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah. Každý zaměstnanec (případně pověřená osoba) je povinen vyhodnotit, zda zpracovávané osobní údaje jsou nezbytné pro stanovené účely.

2.7 **Přesností** se rozumí, že osobní údaje musí být zpracovány v přesné podobě a musí být aktualizované (subjekt údajů má právo na opravu a doplnění).

2.8 **Omezením uložení** se rozumí, že osobní údaje mají být uloženy pouze na nezbytně nutnou dobu (pokud pomine účel zpracování, je třeba osobní údaje bez zbytečného odkladu vymazat nebo zničit).

2.9 **Integritou a důvěrností** se rozumí, že osobní údaje musí být dostatečně zabezpečeny technickými a organizačními opatřeními.

Článek III.
Zpracování a podmínky vyjádření souhlasu

3.1 Správce prohlašuje, že veškeré zpracování osobních údajů subjektů je zákonné a v plném souladu s GDPR, jestliže subjekt udělil souhlas se zpracováním svých osobních údajů, který je správce schopen doložit.

3.2 Příkladem udělení souhlasu je souhlas uvedený v Příloze č. 2 Kodexu.

3.3 Subjekt osobních údajů zpravidla poskytuje tyto údaje:

a) jméno a příjmení;

b) datum narození;

c) bydliště;

d) telefonní číslo a/nebo emailovou adresu.

3.4 Subjekt údajů poskytuje správci písemný souhlas se zpracováním osobních údajů za účelem zasílání nabídkových letáků, reklam, jakož i jiných marketingových účelů, včetně zveřejnění své fotografie v případě výhry ve spotřebitelské soutěži.

3.5 Subjekt údajů má právo svůj souhlas kdykoliv odvolat, přičemž odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním.

3.6 Subjekt údajů prohlašuje, že nezpracovává žádné 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 a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Článek IV.
Správce osobních údajů

4.1 Správcem osobních údajů je společnost VitaLife Shop s.r.o. Správce je povinen:

a) stanovit účel, prostředky a způsob zpracování osobních údajů;

b) vést záznamy o činnostech zpracování podle Přílohy č. 4 Kodexu, za něž odpovídá, a na žádost dozorového úřadu mu je zpřístupnit;

c) zajistit soulad zpracování osobních údajů s GDPR, a být schopen tento soulad prokázat;

d) uzavřít se zpracovatelem osobních údajů písemnou smlouvu o zpracování osobních údajů;

e) na požádání spolupracovat s dozorovým úřadem při plnění jeho úkolů;

f) zavést a přijmout vhodná technická a organizační opatření. Aktualizace „Zdokumentování technických a organizačních opatření k zajištění ochrany osobních údajů“ se provádí nejméně 1x čtvrtletně, případně při změně opatření zabezpečení zpracovávaných osobních údajů. Podrobnosti stanoví Příloha č. 5 Kodexu;

g) při posouzení bezpečnosti zohlednit rizika (zejména zničení, ztrátu, pozměnění, neoprávněné zpřístupnění);

h) zajistit výkon práv subjektu údajů;

i) hlásit dozorovému úřadu porušení zabezpečení osobních údajů bez zbytečného odkladu (pokud možno do 1 týdne), ledaže může v souladu se zásadou odpovědnosti doložit, že je nepravděpodobné, že by dané porušení zabezpečení osobních údajů mělo za následek riziko pro práva a svobody fyzických osob. Zároveň je povinen toto porušení dokumentovat. V rámci společnosti tuto povinnost plní správce;

j) porušení zabezpečení ochrany osobních údajů s vysokým rizikem pro práva a svobody fyzické osoby oznámit subjektu údajů;

k) přijmout vhodná opatření, aby mohl plnit informační povinnost vůči subjektu údajů;

l) provádět posouzení vlivu na ochranu osobních údajů podle GDPR;

m) provádět kontrolu zabezpečení ochrany osobních údajů.

Článek V.
Povinnost mlčenlivosti

5.1 Správce, pověřenec pro ochranu osobních údajů, zpracovatel a příjemce jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, která jsou užívána k ochraně osobních údajů.

5.2 Povinnost mlčenlivosti nelze uplatnit vůči dozorovému úřadu, orgánům činným v trestním řízení, soudu a subjektu údajů. V případě takového předání osobních údajů, musí být dostatečně zabezpečeny a o předání musí být proveden písemný záznam.

Článek VI.
Právo subjektu údajů na přístup k osobním údajům

6.1 Správce se k výzvě subjektu údajů zavazuje poskytnout mu potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má subjekt údajů právo získat přístup k takovým osobním údajům a k následujícím informacím:

a) účelu zpracování;

b) kategorii dotčených osobních údajů;

c) plánovanou dobu, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;

d) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování a/nebo vznést námitku proti tomuto zpracování;

e) právo podat stížnost u dozorového orgánu;

f) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů.

6.2 Správce je povinen k výzvě subjektu údajů poskytnout mu kopii zpracovávaných osobních údajů, přičemž za pořízení kopií je správce oprávněn účtovat přiměřený poplatek.

6.3 Pro případ zaslání kopie zpracovávaných osobních údajů správce tímto stanovuje jednorázový poplatek ve výši 250,-Kč.

Článek VII.

Postup při vyřizování žádosti subjektu údajů

7.1 Pro získání informací o zpracování svých osobních údajů či o jiný výkon svých práv se subjekt údajů obrací na společnost prostřednictvím správce. Posouzení, zda má subjekt údajů právo na přístup k těmto informacím, stanovuje Příloha č. 8 Kodexu.

7.2 Subjektu údajů budou tyto informace poskytnuty bez zbytečného odkladu, a to nejpozději do 1 měsíce od doby, kdy byla přijata jeho písemná žádost.

Článek VIII.
Výkon práv subjektu údajů

8.1 Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím:

a) účelu zpracování;

b) kategorie dotčených osobních údajů;

c) příjemce nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;

d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;

e) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování a/nebo vznést námitku proti tomuto zpracování;

f) právo podat stížnost u dozorového úřadu;

g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;

h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v článku 22 odst. 1,4 GDPR a minimálně v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

8.2 Subjekt údajů má právo na to, aby správce bez zbytečného odkladu **opravil** nepřesné osobní údaje, které se ho týkají.

8.3 Subjekt údajů má rovněž právo na to, aby správce bez zbytečného odkladu **vymazal** osobní údaje, které se daného subjektu týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovávány;

b) subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) GDPR zpracovány, a neexistuje žádný další právní důvod pro zpracování;

c) subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování ve smyslu čl. 21 odst. 2 GDPR;

d) osobní údaje byly zpracovány protiprávně;

e) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo České republiky, které se na správce vztahuje;

f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 GDPR.

8.4 Za lhůtu bez zbytečného odkladu se považuje lhůta do 7 dnů od písemného vyzvání subjektem údajů.

8.5 Subjekt údajů má právo na to, aby správce **omezil zpracování**, v kterémkoliv z těchto případů:

a) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;

b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;

c) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;

d) subjekt údajů vznesl námitku proti zpracování podle článku 21 odst. 1 GDPR, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

8.6 Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil, a to v případě, že:

a) zpracování je založeno na souhlasu podle článku 6 odst. 1 písm. a) GDPR nebo článku 9 odst. 2 písm. a) GDPR nebo na smlouvě podle článku 6 odst. 1 písm. b) GDPR a

b) zpracování se provádí automatizovaně.

8.7 Při výkonu svého práva na přenositelnost údajů podle odstavce 9.6 Kodexu má subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky převoditelné.

8.8 Správce oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s čl. 16, čl. 17 odst. 1 a čl. 18 GDPR, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce informuje subjekt údajů o těchto příjemcích, pokud o to subjekt údajů výslovně požádá.

Článek IX.
Záměrná a standardní ochrana osobních údajů

9.1 Správce prohlašuje, že s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování, zajistil vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je dodržovat zásady ochrany údajů, jako je například minimalizace údajů.

9.2 Správce dále prohlašuje, že zavedl vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Toto ustanovení se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti.

Článek X.
Technická a organizační opatření k zajištění ochrany osobních údajů

10.1 Správce a zpracovatel mají povinnost zavést vhodná technická a organizační opatření pro zajištění požadovaného zabezpečení osobních údajů, včetně:

a) pseudonymizace a šifrování osobních údajů;

b) zajištění důvěrnosti, dostupnosti, integrity a odolnosti systémů a služeb zpracování;

c) zajištění schopnosti obnovit oprávněně zpracovávané osobní údaje a přístup k nim v případě fyzických či technických incidentů;

d) zajištění pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření.

10.2 Technická a organizační opatření k zajištění ochrany osobních údajů musí být ve společnosti přijímána a prováděna v souladu s právními předpisy a tímto Kodexem tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení, ztrátě, neoprávněným přenosům či jinému neoprávněnému zpracování či zneužití. Tato povinnost platí i po ukončení zpracování osobních údajů.

10.3 Přijatá a provedená technická a organizační opatření k zajištění ochrany osobních údajů podle odstavce 11.2 Kodexu musí být zdokumentována v interní dokumentaci společnosti podle Přílohy č. 5 Kodexu.

Článek XI.
Náležitosti technických a organizačních opatření

11.1 Administrativním opatřením se rozumí:

a) zajištění ochrany dokumentů s osobními údaji tak, aby nemohlo dojít k jejich zneužití, poškození nebo zničení;

11.2 Režimovými opatřeními se rozumí:

a) oprávnění ke vstupu do objektu vydává osoba, která může o vstupu rozhodnout podle provozního řádu konkrétního objektu;

b) správce, zpracovatel a příjemce jsou povinni zabezpečit místnosti, kde jsou uloženy osobní údaje (kanceláře) uzamykatelnými dveřmi a zabránit neoprávněnému vniknutí do objektu;

c) přístup do prostor, kde dochází ke zpracování osobních údajů, mají přístup výhradně oprávněné osoby, ostatní osoby mohou do těchto prostor vstupovat pouze za doprovodu oprávněné osoby;

d) klíče od prostor, kde dochází ke zpracování osobních údajů, mohou být přiděleny pouze oprávněnými osobami;

e) zaevidování každé návštěvy místnosti, kde probíhá zpracovávání osobních údajů.

11.3 Fyzickou bezpečností se rozumí:

a) prostory, kde dochází ke zpracování osobních údajů, musí být zabezpečeny takovým způsobem, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení, ztrátě, neoprávněným přenosům, neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů;

b) prostory určené zejména k ukládání nosičů obsahujících osobní údaje musí být zajištěny proti poškození těchto nosičů (např. v důsledku povětrnostních vlivů, zatopení, vlhkosti nebo jiného negativního působení);

c) prostory, kde jsou ve větším rozsahu ukládány dokumenty obsahující osobní údaje, musí být zabezpečeny technicky, zvláště proti požáru.

Článek XII.
Přeprava osobních údajů

12.1 V případě přepravy zásilky, která obsahuje osobní údaje, je potřeba učinit opatření k zabránění přístupu neoprávněné osoby.

12.2 Při přepravě zásilky (obsahující osobní údaje) držitelem poštovní licence je držitel poštovní licence povinen potvrdit odesílateli převzetí zásilky a adresát písemně potvrdí držiteli licence převzetí zásilky.

12.3 Pokud se na doručené zásilce obsahující osobní údaje vyskytne závažná závada (roztržení atp.), je nezbytné informovat subjekt údajů, pokud existuje podezření, že porušení bude mít za následek vysoké riziko pro práva a svobody fyzické osoby. Subjekt údajů se informuje podle článku XVI. Kodexu.

Článek XIII.
Záznamy o činnostech zpracování

13.1 Správce se zavazuje vést záznamy o činnostech zpracování, za něž odpovídá. Záznamy obsahují tyto informace:

a) jméno a kontaktní údaje správce a pověřence pro ochranu osobních údajů;

b) účel zpracování;

c) popis kategorie subjektu údajů a kategorie osobních údajů;

d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny;

e) informace o případném předání osobních údajů do třetí země, včetně identifikace třetí země;

f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;

g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření ve smyslu článku 32 odst. 1 GDPR.

Článek XIV.
Zabezpečení osobních údajů

14.1 Správce zajišťuje ochranu osobních údajů zejména formou pseudonymizace a šifrování osobních údajů a procesem pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření. Veškeré osobní údaje jsou uloženy na zašifrovaných a zabezpečených nosičích, přičemž veškeré nosiče jsou chráněny zejména zašifrovacími hesly.

14.2 Správce má povinnost v případě jakéhokoliv porušení zabezpečení osobních údajů bez zbytečného odkladu a pokud možno do 1 týdne od okamžiku, kdy se o něm dozvěděl, ohlásit uvedenou skutečnost dozorovému orgánu.

14.3 Ohlášení podle odstavce 15.2 Kodexu bude minimálně obsahovat:

a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů;

c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

d) 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.

14.4 Uvedená oznámení v odstavci 15.2 Kodexu není vyžadována, jestliže je splněna kterákoli z těchto podmínek:

a) správce 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, jako je například šifrování;

b) správce přijal následná opatření, která zajistí, že vysoké riziko pro právo a svobody subjektů údajů se již pravděpodobně neprojeví;

c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Článek XV.
Postup při narušení bezpečnosti ochrany osobních údajů

15.1 V případě, že dojde k narušení důvěrnosti, integrity a dostupnosti, bude správce osobních údajů postupovat takto:

a) identifikuje místa, kde k incidentu došlo;

b) bezodkladně po zjištění zamezí dalším škodám;

c) zjistí příčinu incidentu;

d) přijme nezbytná opatření za účelem zabezpečení osobních údajů nebo opatření vedoucí ke zmírnění možných negativních dopadů;

e) zjistí pravděpodobné důsledky a rozsah porušení;

f) povede souhrnnou dokumentaci o případech porušení a nápravných opatřeních;

g) neprodleně informuje pověřence pro ochranu osobních údajů společnosti.

15.2 Pří porušení zabezpečení osobních údajů je správce povinen tuto skutečnost bezodkladně (jeli to možné do 1 týdne), nahlásit dozorovému úřadu po předchozí konzultaci s pověřencem ve formě, kterou stanovuje Příloha č. 9 Kodexu, ledaže může správce v souladu se zásadou odpovědnosti doložit, že je nepravděpodobné, že by dané porušení zabezpečení osobních údajů mělo za následek riziko pro práva a svobody fyzických osob.

15.3 V případě pravděpodobnosti, že porušení bude mít za následek vysoké riziko pro práva a svobody fyzické osoby, je správce povinen porušení zabezpečení oznámit i subjektu údajů. Informace předávané subjektu údajů stanovuje Příloha č. 10 Kodexu.

15.4 Správce ve spolupráci s pověřencem pro ochranu osobních údajů navrhne vhodná opatření k zamezení případného možného opakování incidentu.

Článek XVI.
Právní ochrana, odpovědnost a sankce

16.1 Subjekt údajů má právo podat stížnost u některého dozorového úřadu, pokud se domnívá, že zpracováním jeho osobních údajů je porušeno nařízení GDPR.

16.2 Dozorový úřad, kterému byla stížnost podána, informuje stěžovatele o pokroku v řešení jeho stížnosti a o jeho výsledku, jakož i o možnosti soudní ochrany podle čl. XVIII. Kodexu.

Článek XVII.
Právo na soudní ochranu

17.1 Každý subjekt má právo na soudní ochranu, pokud má za to, že jeho práva podle nařízení GDPR byla porušena v důsledku zpracování jeho osobních údajů v rozporu s tímto nařízením.

17.2 Řízení proti správci nebo zpracovateli se zahajuje u soudů, v němž má daný správce nebo zpracovatel provozovnu.

17.3 Subjekt údajů má právo pověřit neziskový subjekt, organizaci nebo sdružení, jež byly řádně založeny v souladu s právem České republiky, jejichž statutární cíle jsou ve veřejném zájmu a jež vyvíjejí činnost v oblasti ochrany práv a svobod subjektů údajů ohledně ochrany jejich osobních údajů, aby jeho jménem podal stížnost, uplatnil práva ve smyslu čl. 77 až 79 GDPR.

Článek XVIII.
Právo na náhradu újmy

18.1 Kdokoliv, kdo v důsledku porušení nařízení GDPR utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy.

18.2 Správce zapojený do zpracování je odpovědný za újmu, kterou způsobí zpracováním, jež porušuje toto nařízení. Zpracovatel je za újmu způsobenou zpracováním odpovědný pouze v případě, že nesplnil povinnosti stanovené tímto nařízením konkrétně pro zpracovatele nebo že jednal nad rámec zákonných pokynů správce nebo v rozporu s nimi.

18.3 Správce a zpracovatel jsou odpovědnosti podle odstavce 19.1 Kodexu zproštěni, pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

Článek XIX.
Závěrečná ustanovení

19.1 Tento Kodex byl schválen jednatelem společnosti VitaLife Shop s.r.o. a nabývá účinnosti dnem 01.10.2019.

V Praze 01.10.2019.

VitaLife Shop s.r.o. zastoupena jednatelem společnosti
Mariem Rendičem

Příloha č. 8 |Práva subjektu údajů

ČLÁNEK 12 GDPR – PRÁVO SUBJEKTU ÚDAJŮ NA TRANSPARENTNÍ, SROZUMITELNÉ A SNADNO PŘÍSTUPNÝM ZPŮSOBEM DOSTUPNÉ INFORMACE O OSOBNÍCH ÚDAJÍCH, KTERÉ BYLY ZÍSKÁNY SE SOUHLASEM I BEZ SOUHLASU
- Povinnost správce informovat subjekt údajů transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků informace dle čl. 13 až 22 a čl. 34 GDPR; *- Informace o opatřeních přijatých dle čl. 15 – 22 GDPR jsou předávány na základě žádosti.* *Lhůta pro vyřízení žádosti je 1 měsíc, přičemž je možné ji maximálně dvakrát prodloužit.*

ČLÁNEK 13 GDPR – PRÁVO SUBJEKTU ÚDAJŮ NA INFORMACE POSKYTOVANÉ V PŘÍPADĚ, ŽE OSOBNÍ ÚDAJE JSOU ZÍSKÁVÁNY OD SUBJEKTU ÚDAJŮ
Správce musí tyto informace poskytnout v okamžiku získání osobních údajů s výjimkou případů, kdy jimi (osobními údaji) subjekt údajů již disponuje, či v jiných případech podle GDPR (například v případech, kdy jde o ochranu života subjektu údajů).

ČLÁNEK 14 GDPR – PRÁVO SUBJEKTU ÚDAJŮ NA INFORMACE POSKYTOVANÉ V PŘÍPADĚ, ŽE OSOBNÍ ÚDAJE NEBYLY ZÍSKÁNY OD SUBJEKTU ÚDAJŮ
Správce je povinen poskytnout informace o zpracování osobních údajů, přičemž uvedená povinnost neplatí v případě, že: *a) subjekt údajů má tyto informace o zpracování (rozsah, doba, účel, apod.);* *b) poskytnutí údajů by vyžadovalo nepřiměřené úsilí (zejména pro archivaci ve veřejném zájmu, pro vědecký a historický výzkum a pro statistické účely);* *c) získávání je stanoveno právem členského státu nebo právem EU, osobní údaje s ohledem na povinnost zachovávat mlčenlivost musí zůstat důvěrnými.*

ČLÁNEK 15 GDPR – PRÁVO SUBJEKTU ÚDAJŮ NA PŘÍSTUP K OSOBNÍM ÚDAJŮM
Správce vydá potvrzení o tom, zda osobní údaje, které se týkají daného subjektu údajů, jsou, či nejsou zpracovávány, případně mu sdělí informace o tomto zpracování dle článku 15 odst. 1 GDPR. *Správce poskytne kopii zpracovávaných osobních údajů.*

ČLÁNEK 16 GDPR – PRÁVO SUBJEKTU ÚDAJŮ NA OPRAVU, DOPLNĚNÍ NEÚPLNÝCH OSOBNÍCH ÚDAJŮ
Správce bez zbytečného odkladu doplní neúplné a opraví nepřesné osobní údaje, které se týkají subjektu údajů.

ČLÁNEK 17 GDPR – PRÁVO NA VÝMAZ (TZV. PRÁVO BÝT „ZAPOMENUT“)

Správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

a) *osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny neb jinak zpracovávány;*
b) *subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) GDPR zpracovány a neexistuje žádný další právní důvod pro zpracování;*
c) *subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování dle čl. 21 GDPR;*
d) *osobní údaje byly zpracovány protiprávně;*
e) *osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje;*
f) *osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle*

čl. 8 odst. 1 GDPR.

ČLÁNEK 18 GDPR – PRÁVO NA OMEZENÍ ZPRACOVÁNÍ

Správce omezí zpracování v kterémkoliv z těchto níže uvedených případů:

a) *subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;*
b) *zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;*
c) *správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;*
d) *subjekt údajů vznesl námitku proti zpracování podle článku 21 odst. 1 GDPR, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.*

ČLÁNEK 19 GDPR – OZNAMOVACÍ POVINNOST OHLEDNĚ OPRAVY NEBO VÝMAZU OSOBNÍCH ÚDAJŮ NEBO OMEZENÍ ZPRACOVÁNÍ

Správce oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s čl. 16, čl. 17 odst. 1 a čl. 18 GDPR, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje.

ČLÁNEK 20 GDPR – PRÁVO NA PŘENOSITELNOST ÚDAJŮ

Správce má povinnost předat osobní údaje druhému správci (za předpokladu technické převoditelnosti) a pouze za kumulativního splnění těchto podmínek:

a) *zpracování založeno na souhlasu nebo smlouvě a*
b) *jedná se o automatizované zpracování.*

ČLÁNEK 21 GDPR – PRÁVO VZNÉST NÁMITKU

Správce osobní údaje 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.

ČLÁNEK 22 GDPR – PRÁVO NA TO, ABY SUBJEKT ÚDAJŮ NEBYL PŘEDMĚTEM AUTOMATIZOVANÉHO ROZHODOVÁNÍ, VČETNĚ PROFILOVÁNÍ

Správce nesmí provádět výhradně automatizované individuální rozhodování, včetně profilování, s následujícími výjimkami:

a) *je zákonem stanoveno;*
b) *je založeno na souhlasu subjektu;*
c) *je nezbytné pro uzavření smlouvy nebo jejího plnění se subjektem.*

ČLÁNEK 77 A NÁSLEDUJÍCÍ GDPR – DALŠÍ DŮLEŽITÁ PRÁVA SUBJEKTU ÚDAJŮ

Subjekt údajů má dále tyto níže uvedená práva:

a) *právo podat stížnost o dozorového úřadu (správce se stává součástí, resp. předmětem šetření);*
b) *právo na účinnou soudní ochranu vůči dozorovému úřadu;*
c) *právo na účinnou soudní ochranu vůči správci nebo zpracovateli (správce se stává stranou soudního sporu);*
d) *právo na to být zastoupen neziskovým subjektem, organizaci nebo sdružení;*
e) *povinnost správce jednat s takovým subjektem, který zastupuje subjekt údajů (např. v případě podání stížnosti);*
f) *právo na náhradu újmy, vznikne-li subjektu újma, ať již hmotná, či nehmotná.*

Příloha č. 9 | Hlášení o incidentu (porušení zabezpečení osobních údajů)

POPIS POVAHY PŘÍPADU
(Například: neoprávněný přístup, nahodilé zničení, kategorie a přibližné počty dotčených subjektů)

ZPŮSOB PORUŠENÍ ZABEZPEČENÍ
(Například: opakované neoprávněný přístup konkrétní osobu)

Kontaktní údaje: …….

Pověřenec: …….

Adresa: …….

Telefon: …….

Email: …….

Datum a čas zjištění incidentu: …….

POPIS PRAVDĚPODOBNÝCH DŮSLEDKŮ PORUŠENÍ OCHRANY OSOBNÍCH ÚDAJŮ
Povinnost uvést popis důsledků porušení zabezpečení, a zda může následkem úniku dat dojít k fyzické, hmotné, či nehmotné újmě pro subjekt.

POPIS OPATŘENÍ PŘIJATÝCH SPRÁVCEM S CÍLEM VYŘEŠIT DANÉ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ, VČETNĚ PŘIJATÝCH OPATŘENÍ KE ZMÍRNĚNÍ MOŽNÝCH NEPŘÍZNIVÝCH DOPADŮ

DOKUMENTACE PORUŠENÍ ZABEZPEČENÍ *Dokumentace k primárnímu posouzení rizik s následkem dopadu na práva a svobody subjektů údajů (záznamy o všech porušení a skutečnostech)*

Příloha č. 10 | Oznamovací povinnost v případě porušení zabezpečení osobních údajů

VitaLife Shop s.r.o. IČ: 036 45 797 se sídlem
Makovského 1177/1, Řepy, 163 00 Praha
zastoupena jednatelem Mariem Rendičem

jméno a příjmení adresáta []
adresa] [

V *Prahe* dne *01.10.2019*

tímto oznamuje ve smyslu článku 34 odst. 1 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Vážený pane/paní,

v souladu s naší povinností dle článku 34 odst. 1 GDPR Vás v rámci preventivního opatření informujeme o incidentu bezpečnosti dat, který může znamenat/znamená ohrožení Vašich osobních údajů.

Popis povahy porušení:

Pověřenec:
(jméno přímení)

Kontaktní údaje:

Kontaktní místo:

Příloha č. 10 | Oznamovací povinnost v případě porušení zabezpečení osobních údajů

IDENTIFIKACE INCIDENTU *Časové období, celkový popis incidentu, obsah dat, ohrožené/neohrožené údaje.*

POPIS PRAVDĚPODOBNÝCH DŮSLEDKŮ PORUŠENÍ

POPIS PŘIJATÝCH A NAVRŽENÝCH OPATŘENÍ

OPATŘENÍ PŘIJATÁ SPRÁVCEM KE ZMÍRNĚNÍ ÚČINKŮ DOPADU ÚNIKU OSOBNÍCH ÚDAJŮ

DOPORUČENÍ SPRÁVCE K SUBJEKTU ÚDAJŮ *Postup řešení a opatření ke snížení následků dopadu incidentu.*