

# ORGANIZAČNÁ SMERNICA PRE SPRACÚVANIE A OCHRANU OSOBNÝCH ÚDAJOV V ORGANIZÁCI

Podľa ustanovení nariadenia európskeho parlamentu a rady (EÚ) 2016/679, z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, (ďalej len GDPR) a podľa ustanovení zákona 18/2018 z.z, z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, (ďalej len ZoOOÚ)

Obsahuje technické a organizačné opatrenia, ktoré sme sa zaviazali dodržiavať, keďže sme podľa článku 24 GDPR s ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb zodpovední, aby sme zabezpečili a boli schopní preukázať, že spracúvanie sa vykonáva v súlade s nariadením GDPR.

## Spoločnosť:

Názov: HORMÓNIA SLNIEČKO OZ

Sídlo: Vrbická 2072/13, 03101 Liptovský Mikuláš

## Dozorný orgán:

Úradu na ochranu osobných údajov Slovenskej republiky Hraničná 12, 820 07 Bratislava 27

Tel: 02/ 32 31 3214

E-mail: statny.dozor@pdp.gov.sk

(ďalej len „dozorný orgán“)

## 1. VYMEDZENIE ZÁKLADNÝCH POJMOV

**dotknutou osobou** každá fyzická osoba, ktorej osobné údaje sa spracúvajú,

**prevádzkovateľom** každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov, **sprostredkovateľom** každý, kto spracúva osobné údaje v mene prevádzkovateľa,

**spracúvaním osobných údajov** spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami,

**súhlasom dotknutej osoby** akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov

**informačným systémom** akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe,

**biometrickými údajmi** osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických

znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje,

**obmedzením spracúvania osobných údajov** označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti,

**profilovaním** akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom,

**pseudonymizáciou** spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe,

**šifrovaním** transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo,

**online identifikátorom** identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiodrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu,

**porušením ochrany osobných údajov** porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov alebo k neoprávnenému prístupu k nim,

**príjemcom** každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov, **treťou stranou** každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje,

## 2. MAPOVANIE OSOBNÝCH ÚDAJOV

Naša spoločnosť sa v tomto kroku rozhodla definovať, aké osobné údaje spracúva, aby bola schopná analyzovať spracúvanie osobných údajov a zabezpečiť súlad s GDPR.

Kategórie osobných údajov :

### IS Klienti

meno, priezvisko, titul, email, telefónny kontakt, typ absolvovaného seminára, dátum a miesto konania absolvovaného seminára, údaje o zdravotnom stave pre potreby pripustenia k absolvovaniu seminára, nakúpený tovar

účel spracovania: registrácia uchádzača o seminár, posúdenie, či zdravotný stav klienta umožňuje absolvovať seminár hormonálnej jogy podľa Dinah Rodrigues a prípadné následné konzultácie s dotknutou osobou a marketingová informačná komunikácia

### **3. ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV (ČLÁNOK 5 GDPR)**

Naša spoločnosť bude dodržiavať nasledovné zásady spracúvania osobných údajov:

#### **3.1. Zákonnosť, spravodlivosť a transparentnosť (článok 5 ods.1 písm. a) GDPR)**

Osobné údaje budú spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe („zákonnosť, spravodlivosť a transparentnosť“);

##### **3.1.1. Zákonnosť spracúvania (článok 6 GDPR)**

Zaviazali sme sa spracúvať údaje len zákonným spôsobom tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

Spracúvanie osobných údajov bude zákonné a to zabezpečením, že sa vykonáva na základe aspoň jedného z týchto právnych základov:

- a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely;
- b) spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy; u nás je takýmto príkladom vyplnenie zdravotného dotazníka, ktorým nám poskytujete údaje o sebe – na účely odporúčania/neodporúčania absolvovať seminár a na účely registrácie na konkrétny seminár.
- c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná (§ 13 ods. 1 písmeno c ZoOOÚ)
- d) spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby;
- e) spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;
- f) spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobou dieťa.

**Právne základy pre jednotlivé účely spracovania osobných údajov sú definované v záznamoch o spracovateľských činnostiach.**

#### **3.2. Zásada obmedzenia účelu (článok 5 ods.1 písm. b) GDPR)**

Získavame osobné údaje len na konkrétne určené, výslovne uvedené a legitímne účely a nebudeme ich ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi. Informujeme dotknutú osobu o účele spracúvania osobných údajov pred ich spracúvaním.

V časti mapovanie osobných údajov sme si stanovili účely spracovania IS Klienti a osobné údaje budeme spracúvať len na účely uvedené v tejto časti.

### **3.3. Zásada minimalizácie osobných údajov (článok 5 ods.1 písm. c) GDPR)**

Spracúvame osobné údaje tak, aby bolo toto spracúvanie primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú. S cieľom zabezpečiť minimalizáciu osobných údajov sme sa rozhodli zanalyzovať, či sú spracúvané údaje primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú.

### **3.4. Zásada správnosti (článok 5 ods.1 písm. d) GDPR)**

Spracúvame osobné údaje tak, aby boli správne a podľa potreby aktualizované; prijímame primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.

Na zabezpečenie zásady správnosti máme v písomnom súhlase so spracovaním osobných údajov nasledovnú formuláciu:

„Dotknutá osoba je povinná poskytnúť pravdivé a aktuálne osobné údaje. V prípade zmeny osobných údajov je dotknutá osoba povinná zmenu bezodkladne oznámiť prevádzkovateľovi.“

### **3.5. Zásada minimalizácie uchovávania (článok 5 ods.1 písm. e) GDPR)**

Osobné údaje uchovávame vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú.

### **3.6. Zásada integrity a dôvernosti (článok 5 ods.1 písm. f) GDPR)**

Osobné údaje spracúvame spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov a to prostredníctvom primeraných technických alebo organizačných opatrení.

#### **3.6.1. Osobné údaje uložené v elektronickej podobe**

Používame antivírus a firewall od spoločnosti ESET.

Údaje ukladáme a zálohujeme na Cloud OneDrive Microsoft. Vstupy na Cloud a nami používané stanice sú chránené heslom.

Na ochranu wifi využívame protokol WPA2. Heslo je pravidelne menené.

Počítač s osobnými údajmi je chránený heslom, ktoré vedia len oprávnené osoby.

Osobné údaje sú uložené na mojom počítači a tento počítač je chránený heslom.

#### **3.6.2. Osobné údaje uložené v papierovej (vytlačenej) podobe**

Fyzické dokumenty (zdravotné dotazníky) sú uložené v obaloch a v šanónoch, čím je zabezpečená ochrana pred poškodením.

Šanóny s fyzickými dokumentami sú uložené:

- v skrinke so zamykaním

Tak je zabezpečené, že sa k týmto dokumentom dostanú len oprávnené osoby

### **3.7. Zásada zodpovednosti (článok 5 ods. 2 GDPR)**

Sme zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať.

## **4. PODMIENKY POSKYTNUTIA SÚHLASU SO SPRACÚVANÍM OSOBNÝCH ÚDAJOV (ČLÁNOK 7 GDPR)**

Zabezpečíme splnenie nasledovných podmienok pri vyjadrení súhlasu dotknutou osobou

- a) súhlas so spracúvaním osobných údajov musí byť vyjadrený slobodne, konkrétne, informovane a jednoznačným prejavom vôle.
- b) žiadosť o vyjadrenie súhlasu musí byť predložená tak, aby bola jasne odlišiteľná od týchto iných skutočností, v zrozumiteľnej a ľahko dostupnej forme a formulovaná jasne a jednoducho.
- c) dotknutá osoba má právo kedykoľvek odvolať svoj súhlas. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania vychádzajúceho zo súhlasu pred jeho odvolaním. Pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Odvolanie súhlasu musí byť také jednoduché ako jeho poskytnutie.

## **5. PODMIENKY UPLATNITEĽNÉ NA SÚHLAS DIEŤAŤA V SÚVISLOSTI SO SLUŽBAMI INFORMAČNEJ SPOLOČNOSTI (ČLÁNOK 8 GDPR)**

Ak sa uplatňuje článok 6 ods. 1 písm. a), v súvislosti s ponukou služieb informačnej spoločnosti adresovanou priamo dieťaťu je spracúvanie osobných údajov dieťaťa zákonné, len ak má dieťa aspoň 16 rokov. Ak má dieťa menej než 16 rokov, takéto spracúvanie je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas vyjadril alebo schválil nositeľ rodičovských práv a povinností.

Vynaložíme primerané úsilie, aby sme v takýchto prípadoch overili, že nositeľ rodičovských práv a povinností vyjadril súhlas alebo ho schválil, pričom zohľadníme dostupnú technológiu.

## **SPRACÚVANIE OSOBITNÝCH KATEGÓRIÍ OSOBNÝCH ÚDAJOV (ČLÁNOK 9 GDPR)**

Podľa GDPR sa zakazuje spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

Tento zákaz sa však neuplatňuje, ak platí niektorá z podmienok článku 9 ods. 2 GDPR písm. a) – j)

Najčastejšie jeden z bodov a) alebo b) článku 9 ods. 2 GDPR:

- a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viacero určených účelov, s výnimkou prípadov, keď sa v práve Únie alebo v práve členského štátu stanovuje, že zákaz uvedený v odseku 1 nemôže dotknutá osoba zrušiť;
- b) spracúvanie je nevyhnutné na účely plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany

My spracúvame údaje týkajúce sa zdravia (tie ktoré nám poskytne klient pri vyplňovaní Zdravotného dotazníka) na základe podmienky článku 9 ods. 2 GDPR písm. a).

Konkrétne ide o:

Údaje poskytnuté klientom pri vyplňovaní Zdravotného dotazníka, výlučne pre potrebu posúdenia, či zdravotný stav klienta umožňuje absolvovať seminár hormonálnej jogy podľa Dinah Rodrigues a pre prípadnú konzultáciu s dotknutou osobou. Posúdenie vykonáva lektorka certifikovaná na túto metódu osobne a len z pohľadu tejto metódy. Údaje tak pozná len lektorka osobne, ktorá ich následne archivuje pre účely novej budúcej konzultácie s konkrétnou dotknutou osobou. Údaje sa žiadnym iným spôsobom nespracovávajú. Za žiadnych okolností sa nezverejňujú, nešíria ani neposielajú akoukoľvek formou vrátane elektronickej. Vaše osobné údaje určené pre registráciu na seminár, informačnú a marketingovú komunikáciu na jednej strane a pre potrebu posúdenia, či zdravotný stav klienta umožňuje absolvovať seminár hormonálnej jogy podľa Dinah Rodrigues a pre prípadnú konzultáciu s dotknutou osobou na druhej strane vedíme a archivujeme osobitne.

Údaje pre potrebu posúdenia, či zdravotný stav klienta umožňuje absolvovať seminár hormonálnej jogy podľa Dinah Rodrigues a pre prípadnú konzultáciu s dotknutou osobou vedíme výlučne písomnou formou v dokumente Zdravotný dotazník a nikdy ich nespracovávame elektronicke.

## **7. PRÁVA DOTKNUTEJ OSOBY (KAPITOLA 3 GDPR)**

Práva dotknutej osoby sú upravené kapitolou 3 GDPR a my sa ich zaväzujeme dodržiavať.

Ide napríklad o nasledovné práva:

### **7.1. Informácie, ktoré sa majú poskytovať pri získavaní osobných údajov od dotknutej osoby (článok 13 GDPR)**

Poskytneme dotknutej osobe pri spracúvaní osobných údajov nasledovné informácie:

- a) údaje o nás
- b) kontaktné údaje prípadnej zodpovednej osoby;
- c) účely spracúvania
- d) právny základ spracúvania
- e) ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) GDPR, oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana;
- f) príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú;
- g) doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;

- h) existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov;
- i) ak je spracúvanie založené na článku 6 ods. 1 písm. a) alebo na článku 9 ods. 2 písm. a) GDPR, existencia práva kedykoľvek svoj súhlas odvolať bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním;
- j) právo podať sťažnosť dozornému orgánu;
- k) informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov;
- l) existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 GDPR a aspoň v týchto prípadoch zmysluplné informácie o použítom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

## **7.2. Informácie, ktoré sa majú poskytnúť, ak osobné údaje neboli získané od dotknutej osoby (článok 14 GDPR)**

Naša spoločnosť poskytne dotknutej osobe, ak tieto osobné údaje neboli získané od nej, všetky informácie uvedené v bode 7.1 tejto organizačnej smernice a tiež z akého zdroja pochádzajú osobné údaje, prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov.

Tieto informácie poskytne naša spoločnosť dotknutej osobe v primeranej lehote po získaní osobných údajov, najneskôr však do jedného mesiaca, pričom zohľadní konkrétne okolnosti, za ktorých sa osobné údaje spracúvajú uvedené v článku 14 ods. 3 GDPR

Naša spoločnosť neposkytne dotknutej osobe tieto informácie v prípadoch uvedených v článku 14 ods. 5 GDPR, najmä ak:

- a) dotknutá osoba má už dané informácie
- b) sa poskytovanie takýchto informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie
- c) sa získanie alebo poskytnutie výslovne stanovuje v práve Únie alebo v práve členského štátu, ktorému prevádzkovateľ podlieha, a v ktorom sa stanovujú primerané opatrenia na ochranu oprávnených záujmov dotknutej osoby Právo dotknutej osoby na prístup k údajom (článok 15 GDPR)

Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom

## **7.3. Právo na opravu (článok 16 GDPR)**

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účely spracúvania má dotknutá osoba právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia.

## **7.4. Právo na vymazanie (právo „na zabudnutie“, článok 17 GDPR)**

Dotknutá osoba má tiež právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, a prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak je splnený niektorý z týchto dôvodov:

- a) osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali;

- b) dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva, podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a), a ak neexistuje iný právny základ pre spracúvanie;
- c) dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 1 a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 2;
- d) osobné údaje sa spracúvali nezákonne;
- e) osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha;
- f) osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1.

### **7.5. Právo na obmedzenie spracúvania (článok 18 GDPR)**

Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie, pokiaľ ide o jeden z týchto prípadov:

- a) dotknutá osoba napadne správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov;
- b) spracúvanie je protizákonné a dotknutá osoba namieta proti vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia;
- c) prevádzkovateľ už nepotrebuje osobné údaje na účely spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov;
- d) dotknutá osoba namietala voči spracúvaniu podľa článku 21 ods. 1, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

### **Oznamovacia povinnosť v súvislosti s opravou alebo vymazaním osobných údajov alebo obmedzením spracúvania (článok 19 GDPR)**

Prevádzkovateľ oznámi každému príjemcovi, ktorému boli osobné údaje poskytnuté, každú opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania uskutočnené podľa článku 16, článku 17 ods. 1 a článku 18, pokiaľ sa to neukáže ako nemožné alebo si to nevyžaduje neprimerané úsilie. Prevádzkovateľ o týchto príjemcoch informuje dotknutú osobu, ak to dotknutá osoba požaduje.

### **7.6. Právo na prenosnosť údajov (článok 20 GDPR)**

Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje ďalšiemu prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému sa tieto osobné údaje poskytl, bránil, ak:

- a) sa spracúvanie zakladá na súhlase podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a), alebo na zmluve podľa článku 6 ods. 1 písm. b), a
- b) ak sa spracúvanie vykonáva automatizovanými prostriedkami.

Dotknutá osoba má pri uplatňovaní svojho práva na prenosnosť údajov podľa odseku 1 právo na prenos osobných údajov priamo od jedného prevádzkovateľa druhému prevádzkovateľovi, pokiaľ je to technicky možné.



## **7.7. Právo namietať (článok 21 GDPR)**

Dotknutá osoba má právo kedykoľvek namietať z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka, ktoré je vykonávané na základe článku 6 ods. 1 písm. e) alebo f) vrátane namietania proti profilovaniu založenému na uvedených ustanoveniach.

## **7.8. Automatizované individuálne rozhodovanie vrátane profilovania (článok 22 GDPR)**

Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.

## **8. ZODPOVEDNOSŤ PREVÁDZKOVATEĽA (ČLÁNOK 24 GDPR)**

My ako prevádzkovateľ sa zaväzujeme dodržiavať nasledovné všeobecné povinnosti:

- a) S ohľadom na povahu, rozsah a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzickej osoby sa zaväzujeme prijať vhodné technické a organizačné opatrenia na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade s GDPR.
- b) Uvedené opatrenia budeme podľa potreby aktualizovať.
- c) Budeme pravidelne preverovať trvanie účelu spracúvania osobných údajov a po jeho splnení bez zbytočného odkladu zabezpečiť výmaz osobných údajov
- d) Naša spoločnosť bude zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.

## **9. ŠPECIFICKY NAVRHNUTÁ A ŠTANDARDNÁ OCHRANA OSOBNÝCH ÚDAJOV (ČLÁNOK 25 GDPR)**

Pred spracúvaním osobných údajov sme zaviedli a počas spracúvania osobných údajov máme zavedenú špecificky navrhnutú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení, na účinné zavedenie primeraných záruk ochrany osobných údajov a dodržiavanie nariadenia GDPR.

Pri špecificky navrhnutej ochrane osobných údajov zohľadňujeme najnovšie poznatky ochrany osobných údajov, náklady na vykonanie opatrení, povahu, rozsah, kontext a účel spracúvania osobných údajov a riziká spracúvania osobných údajov s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie osobných údajov predstavuje pre práva dotknutej osoby.

Zaviedli sme štandardnú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení na zabezpečenie spracúvania osobných údajov len na konkrétny účel, minimalizácie množstva získaných osobných údajov a rozsahu ich spracúvania, doby uchovávania a dostupnosti osobných údajov. Zabezpečujeme, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.

## **10. SPROSTREDKOVATEĽ (ČLÁNOK 28 GDPR)**

Sprostredkovateľ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.

My ako prevádzkovateľ momentálne nevyužívame žiadneho sprostredkovateľa.

Pokiaľ začneme využívať sprostredkovateľov, tak len sprostredkovateľov poskytujúcich dostatočné záruky na to, že sa prijímú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky GDPR a aby sa zabezpečila ochrana práv dotknutej osoby.

## 11. ZÁZNAMY O SPRACOVATEĽSKÝCH ČINNOSTIACH (ČLÁNOK 30 GDPR)

Záznamy o spracovateľských činnostiach prevádzkovateľa/zástupcu prevádzkovateľa										
		identifikačné a kontaktné údaje*	Obchodné meno/meno a priezvisko	IČO (ak bolo prídelené)	Adresa trvalého bydliska/sídlo	PSČ	Obec	Štát	e-mail/telef. kontakt	
		prevádzkovateľ	HORMONYOGA Mírka Mahima Bartošová		Rozvodná 13C	831 01	Bratislava	Slovensko	<a href="mailto:mirka@hormonyoga.sk">mirka@hormonyoga.sk</a>	903129808
		spoločný prevádzkovateľ	x							
		zástupca prevádzkovateľa	x							
		zodpovedná osoba	Mgr. Miroslava Bartošová		dtto	dtto	dtto	dtto	dtto	dtto
		*prevádzkovateľ vyplní políčka, ktoré sú relevantné, napr. ak nemá určenú zodpovednú osobu záznam nebude takúto informáciu obsahovať								
P. č.	IS	Účel spracúvania	Právny základ spracovateľskej činnosti článok 6 ods. 1 GDPR (nepovinné) zákony - v znení neskorších predpisov	Kategórie dotknutých osôb	Kategória osobných údajov	Lehota na výmaz OÚ (podľa možnosti)	Kategória príjemcov	Označenie tretej krajiny alebo medzinárodnej organizácie	Bezpečnostné opatrenia (technické a organizačné)	Minimalizácia údajov (nepovinné)
1		registrácia na seminár	článok 6 ods. 1 písmeno b) GDPR spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy	zákazníci	bežné osobné údaje	počas doby trvania účtu, na ktorý bol súhlas udelený	žiadni príjemcovia			áno
2	IS zákazníci	posúdenie, či zdravotný stav klienta umožňuje absolvovať seminár harmonizácie jogy a prípadne následné konzultácie s dotknutou osobou	článok 9 ods. 2 písmeno a) GDPR dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viaceré určených účelov	zákazníci	údaje o zdravotnom stave	počas doby trvania účtu, na ktorý bol súhlas udelený	žiadni príjemcovia	prenos do tretej krajiny sa neuskutočňuje	uvedené v organizačnej smernici	áno
3		informačná a marketingová komunikácia	článok 6 ods. 1 písmeno a) GDPR dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely	zákazníci	bežné osobné údaje	počas doby trvania účtu, na ktorý bol súhlas udelený	žiadni príjemcovia			áno

### 11.1. Záznamy o spracovateľských činnostiach prevádzkovateľa

My ako prevádzkovateľ vedíme záznamy o spracovateľských činnostiach a na požiadanie ich sprístupníme dozornému orgánu. Tieto záznamy obsahujú nasledovné údaje:

- meno/názov a kontaktné údaje prevádzkovateľa a v príslušnom prípade spoločného prevádzkovateľa, zástupcu prevádzkovateľa a zodpovednej osoby;
- účely spracúvania;
- opis kategórií dotknutých osôb a kategórií osobných údajov;
- kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, vrátane príjemcov v tretích krajinách alebo medzinárodných organizácií; ak by takáto situácia nastala;
- v príslušných prípadoch prenosi osobných údajov do tretej krajiny alebo medzinárodnej organizácii vrátane označenia predmetnej tretej krajiny alebo medzinárodnej organizácie a v prípade prenosov uvedených v článku 49 ods. 1 druhom pododseku GDPR dokumentáciu primeraných záruk; ak by takáto situácia nastala;
- podľa možnosti predpokladané lehoty na vymazanie rôznych kategórií údajov;
- podľa možnosti všeobecný opis technických a organizačných bezpečnostných opatrení uvedených v článku 32 ods. 1. GDPR

### Poverenie spracúvať osobné údaje (článok 32 ods. 4 GDPR)

Podnikli sme kroky na zabezpečenie toho, aby každá fyzická osoba konajúca na základe nášho poverenia, ktorá má prístup k osobným údajom, spracúvala tieto údaje len na základe našich pokynov s výnimkou prípadov, keď sa to od nej vyžaduje podľa práva Únie alebo práva členského štátu.

## **12. OZNÁMENIE PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV DOZORNÉMU ORGÁNU (ČLÁNOK 33 A 34 GDPR)**

V prípade porušenia ochrany osobných údajov, bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvieme, oznámime porušenie ochrany osobných údajov dozornému orgánu.

Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.

Oznámenie o porušení ochrany osobných údajov bude obsahovať aspoň:

- a) opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
- b) kontaktné údaje našej zodpovednej osoby, kde možno získať viac informácií o porušení ochrany osobných údajov;
- c) opis pravdepodobných následkov porušenia ochrany osobných údajov;
- d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Zdokumentujeme každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, bez zbytočného odkladu oznámime porušenie ochrany osobných údajov dotknutej osobe.

## **13. POSÚDENIE VPLYVU NA OCHRANU ÚDAJOV (ČLÁNOK 35)**

Ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov.

Posúdenie vplyvu na ochranu údajov sa vyžaduje najmä v prípadoch:

- a) systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu;
- b) spracúvania vo veľkom rozsahu osobitných kategórií údajov podľa článku 9 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10, alebo
- c) systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

Naše spracovateľské činnosti nezahŕňajú prípady uvedené vyššie, z tohto dôvodu nie je potrebné vykonať posúdenie vplyvu na ochranu osobných údajov.

## 14. URČENIE ZODPOVEDNEJ OSOBY (KAPITOLA 4 ODDIEL 4 GDPR)

Prevádzkovateľ je povinný určiť zodpovednú osobu, ak

- a) spracúvanie osobných údajov vykonáva orgán verejnej moci alebo verejnoprávna inštitúcia okrem súdov pri výkone ich súdnej právomoci,
- b) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutej osoby vo veľkom rozsahu alebo
- c) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií osobných údajov podľa článku 9 GDPR vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa článku 10 GDPR vo veľkom rozsahu.

Nakoľko my nespĺňame ani jednu zo spomenutých podmienok (spracovávame síce údaje o zdravotnom stave, ale nie vo veľkom rozsahu), zodpovednú osobu **neurčujeme**.

## 15. PRENOS OSOBNÝCH ÚDAJOV DO TRETEJ KRAJINY ALEBO MEDZINÁRODNEJ ORGANIZÁCIE

Prenos osobných údajov, ktoré sa spracúvajú alebo sú určené na spracúvanie po prenose do tretej krajiny alebo medzinárodnej organizácie, sa môže uskutočniť len vtedy, ak prevádzkovateľ a sprostredkovateľ dodržiavajú podmienky vrátane podmienok následného prenosu osobných údajov z predmetnej tretej krajiny alebo od predmetnej medzinárodnej organizácie do inej tretej krajiny alebo inej medzinárodnej organizácie.

Úrad na ochranu osobných údajov uverejňuje na svojej webstránke zoznam tretích krajín, území a určených sektorov v danej tretej krajine a medzinárodných organizácií, v prípade ktorých Európska komisia rozhodla, že v nich je zaručená primeraná úroveň ochrany alebo už prestala byť primeraná úroveň ochrany zaručená.

Zoznam je dostupný na stránke <https://dataprotection.gov.sk/uouu/sk/content/prenos-do-krajin-zarucujucich-primeranu-uroven-ochrany>

My tento zoznam pravidelne sledujeme a v prípade, že by sme prenášali osobné údaje do krajín mimo zoznam úradu na ochranu osobných údajov, bude postupovať podľa kapitoly 4 GDPR.

## 16. MLČANLIVOSŤ (§ 79 ZOOOÚ)

Sme povinní zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvame. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.

Sme tiež povinní zaviazat' mlčanlivosťou o osobných údajoch fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa. Povinnosť mlčanlivosti podľa prvej vety musí trvať aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu tejto fyzickej osoby.