

# ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ A OCHRANA SOUKROMÍ (GDPR)

**Resonica s.r.o.**

*Centrum alternativní medicíny*

Verze 1.0

Účinnost od: 1. června 2026

Datum vydání: 15. května 2026

# 1. Úvodní ustanovení

## 1.1 Účel a obsah dokumentu

Tento dokument „Zásady zpracování osobních údajů a ochrana soukromí“ (dále jen „Zásady“) vydává obchodní společnost Resonica s.r.o., IČO 236 41 771, se sídlem Topolská 952, Chrudim II, 537 05 Chrudim (dále jen „Správce“ nebo „my“), jakožto provozovatel centra alternativní medicíny. Účelem těchto Zásad je transparentní a srozumitelný popis toho, jaké osobní údaje subjektů údajů (klientů, zájemců, návštěvníků webu a dalších osob) zpracováváme, na základě jakého právního titulu, k jakým účelům, po jakou dobu, komu je předáváme a jaká práva mají subjekty údajů v souvislosti s tímto zpracováním.

Tyto Zásady jsou koncipovány tak, aby splňovaly informační povinnost Správce dle čl. 13 a 14 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, dále jen „GDPR“ nebo „Nařízení“).

Vzhledem k povaze poskytovaných služeb v oblasti alternativní medicíny dochází u Správce ke zpracování zvláštních kategorií osobních údajů ve smyslu čl. 9 odst. 1 GDPR – zejména údajů o zdravotním stavu klientů (anamnézy, popis obtíží, alergie, užívané léky). Této skutečnosti je v Zásadách věnována zvýšená pozornost a samostatná sekce (viz článek 6 těchto Zásad).

**Poznámka k titulu jednatelky a povaze činnosti Správce.** Statutárním orgánem (jednatelkou) Správce je MUDr. Svatava Tomašulová. „MUDr.“ je akademický titul jednatelky; Resonica s.r.o. však není poskytovatelem zdravotních služeb ve smyslu zákona č. 372/2011 Sb. a jednatelka v rámci činnosti Resonica s.r.o. nevystupuje jako lékař či poskytovatel zdravotní péče. Resonica s.r.o. provozuje volnou živnost a poskytuje wellness služby, poradenství a konzultace v oblasti životního stylu, harmonizační a relaxační procedury a neinvazivní měření v rozsahu oboru „Testování, měření, analýzy a kontroly“.

**Praktický důsledek pro režim zpracování zdravotních údajů (čl. 9 GDPR):** Protože Resonica s.r.o. NENÍ zdravotnickým zařízením, NELZE pro zpracování údajů o zdravotním stavu klientů (anamnézy, popisy obtíží, výsledky screeningů) využít výjimku podle čl. 9 odst. 2 písm. h) GDPR (která se vztahuje na registrované poskytovatele zdravotních služeb). Jediným použitelným právním titulem pro tato zpracování je výslovný písemný souhlas klienta podle čl. 9 odst. 2 písm. a) GDPR. Vzor souhlasu je uveden v Příloze č. 1 těchto Zásad.

## 1.2 Právní rámec

Při zpracování osobních údajů postupuje Správce zejména v souladu s následujícími právními předpisy:

- **Nařízení (EU) 2016/679 (GDPR)** – obecné nařízení o ochraně osobních údajů, použitelné ve všech členských státech EU od 25. 5. 2018;
- **zákon č. 110/2019 Sb.**, o zpracování osobních údajů, ve znění pozdějších předpisů – adaptační zákon ČR k GDPR (dále jen „ZZOÚ“);
- **zákon č. 372/2011 Sb.**, o zdravotních službách – Správce na základě tohoto zákona není poskytovatelem zdravotních služeb (viz dále), proto se na něj nevztahuje výjimka čl. 9 odst. 2 písm. h) GDPR;
- **zákon č. 127/2005 Sb.**, o elektronických komunikacích – zejm. § 89 odst. 3 (cookies a sledovací technologie);
- **zákon č. 480/2004 Sb.**, o některých službách informační společnosti – zejm. § 7 (obchodní sdělení);
- **zákon č. 563/1991 Sb.**, o účetnictví, a zákon č. 235/2004 Sb., o dani z přidané hodnoty – v rozsahu povinnosti archivace daňových a účetních dokladů.

## 1.3 Působnost těchto Zásad

Tyto Zásady se vztahují na veškeré zpracování osobních údajů, které provádí Správce v souvislosti se svou

podnikatelskou činností – tedy zejména v souvislosti s:

- poskytováním služeb alternativní medicíny v provozovně Správce (objednávky, rezervace, anamnézy, samotná sezení, fakturace);
- provozováním internetových stránek [www.resonica.cz](http://www.resonica.cz) (analytika, cookies, kontaktní formuláře, on-line rezervace);
- marketingovou a obchodní komunikací (newsletter, obchodní sdělení, slevové akce);
- plněním zákonných povinností (vedení účetnictví, evidence pro účely DPH, archivace dokladů);
- případnou ochranou bezpečnosti osob a majetku v provozovně (kamerový systém, je-li instalován).

Tyto Zásady jsou veřejně dostupné na internetových stránkách Správce [www.resonica.cz](http://www.resonica.cz) a v tištěné podobě k nahlédnutí v provozovně Topolská 952, Chrudim II, 537 05 Chrudim. Subjekt údajů je s nimi seznámen nejpozději při prvním kontaktu se Správcem (online rezervace, první návštěva).

## 2. Správce osobních údajů

### 2.1 Identifikace Správce

Údaj	Hodnota
Obchodní firma	Resonica s.r.o.
Právní forma	společnost s ručením omezeným
IČO	236 41 771
DIČ	neplátce DPH
Sídlo	Topolská 952, Chrudim II, 537 05 Chrudim
Provozovna	Topolská 952, Chrudim II, 537 05 Chrudim
Zápis v OR	Krajský soud v Hradci Králové, spisová značka C 55197
E-mail	<a href="mailto:info@resonica.cz">info@resonica.cz</a>
Telefon	+420 777 609 376
Web	<a href="http://www.resonica.cz">www.resonica.cz</a>
Datum vzniku	27. srpna 2025

### 2.2 Kontakt pro uplatnění práv dle GDPR

Subjekt údajů může uplatnit svá práva podle těchto Zásad a podle GDPR zejména následujícími způsoby:

- **elektronicky:** na adrese [info@resonica.cz](mailto:info@resonica.cz) (předmět e-mailu: „GDPR – žádost subjektu údajů“);
- **písemně:** doporučeným dopisem na adresu sídla Topolská 952, Chrudim II, 537 05 Chrudim;
- **osobně:** v provozovně Topolská 952, Chrudim II, 537 05 Chrudim po předchozí domluvě (z důvodu ověření totožnosti).

### 2.3 Pověřenec pro ochranu osobních údajů (DPO)

Podle čl. 37 odst. 1 GDPR je správce nebo zpracovatel povinen jmenovat pověřence pro ochranu osobních údajů („DPO“), pokud:

- a) zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů jednajících v rámci své soudní pravomoci;
- b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, rozsahu nebo účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;
- c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů podle čl. 9 GDPR nebo údajů týkajících se rozsudků v trestních věcech a trestných činů podle čl. 10 GDPR.

Společnost Resonica s.r.o. po individuálním posouzení podle čl. 37 odst. 1 GDPR nejmenovala pověřence pro ochranu osobních údajů (DPO). Důvodem je, že Resonica s.r.o. není orgánem veřejné moci ani veřejným subjektem [písm. a)], nezpracovává osobní údaje rozsáhle ani systematicky neprovádí monitorování subjektů [písm. b)] a sice zpracovává zvláštní kategorii údajů (údaje o zdravotním stavu klientů) podle čl. 9 GDPR, avšak nikoli v takovém rozsahu, aby šlo o „hlavní činnost spočívající v rozsáhlém zpracování zvláštních kategorií“ [písm. c)] — počet klientů Resonica s.r.o. odpovídá malému provozovateli wellness služeb. Pokud se v budoucnu charakter nebo rozsah zpracování změní (např. rozšíření klientely, zavedení monitoringu, profilování), společnost Resonica s.r.o. povinnost jmenování DPO znovu posoudí.

Pro veškerou komunikaci ohledně ochrany osobních údajů a uplatňování práv subjektů podle čl. 12–22 GDPR slouží následující kontakt: e-mail [info@resonica.cz](mailto:info@resonica.cz) (do předmětu uvést „GDPR — žádost subjektu údajů“), písemně Resonica s.r.o., Topolská 952, Chrudim II, 537 05 Chrudim, případně osobně v provozovně na téže adrese po předchozí domluvě z důvodu ověření totožnosti.

### 3. Definice pojmů (čl. 4 GDPR)

Pro účely těchto Zásad mají níže uvedené pojmy význam vymezený v čl. 4 GDPR. Pro snazší orientaci uvádíme přehled klíčových definic:

Pojem	Definice
Osobní údaj	veškeré informace o identifikované nebo identifikovatelné fyzické osobě („subjektu údajů“). Identifikovatelnou fyzickou osobou je osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na jméno, identifikační číslo, lokační údaje, on-line identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity (čl. 4 odst. 1 GDPR).
Zvláštní kategorie údajů	osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, dále genetické a biometrické údaje za účelem jedinečné identifikace fyzické osoby a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby (čl. 9 odst. 1 GDPR).
Subjekt údajů	identifikovaná nebo identifikovatelná fyzická osoba, k níž se osobní údaje vztahují (např. klient Správce, zájemce o službu, odběratel newsletteru, návštěvník webu).
Správce	fyzická nebo právnická osoba, která sama nebo společně s jinými určuje účely a prostředky zpracování osobních údajů (čl. 4 odst. 7 GDPR). V tomto dokumentu se jím rozumí Resonica s.r.o..
Zpracovatel	fyzická nebo právnická osoba, která zpracovává osobní údaje pro Správce na základě smlouvy o zpracování dle čl. 28 GDPR (např. poskytovatel rezervačního systému, účetní firma, IT poskytovatel).
Zpracování	jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů – zejména shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či

Pojem	Definice
	zkombinování, omezení, výmaz nebo zničení (čl. 4 odst. 2 GDPR).
Příjemce	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už jde o třetí stranu, či nikoli (čl. 4 odst. 9 GDPR).
Profilování	jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě (čl. 4 odst. 4 GDPR).
Automatizované rozhodování	rozhodnutí založené výhradně na automatizovaném zpracování, včetně profilování, které má pro subjekt údajů právní účinky nebo se ho obdobným způsobem významně dotýká (čl. 22 GDPR).
Pseudonymizace	zpracování osobních údajů tak, že je nelze přiřadit konkrétnímu subjektu údajů bez použití dodatečných informací uchovávaných odděleně (čl. 4 odst. 5 GDPR).
Anonymizace	nevratná úprava osobních údajů takovým způsobem, že již nelze identifikovat konkrétní fyzickou osobu; anonymizované údaje již nepodléhají režimu GDPR.
Porušení zabezpečení	porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů (čl. 4 odst. 12 GDPR; „data breach“).
Souhlas	jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů (čl. 4 odst. 11 GDPR).
Výslovný souhlas	kvalifikovaná forma souhlasu vyžadovaná pro zpracování zvláštních kategorií údajů dle čl. 9 odst. 2 písm. a) GDPR; musí být udělen aktivním jednoznačným úkonem, nejlépe písemně, s přesně vymezeným účelem a rozsahem.
ÚOOÚ	Úřad pro ochranu osobních údajů, dozorový úřad pro ochranu osobních údajů v České republice, se sídlem Pplk. Sochora 27, 170 00 Praha 7, <a href="http://www.uoou.gov.cz">www.uoou.gov.cz</a> .

## 4. Jaké osobní údaje zpracováváme

Správce zpracovává osobní údaje subjektů údajů pouze v rozsahu nezbytném pro stanovené účely. Údaje rozdělujeme do následujících kategorií:

### 4.1 A) Identifikační a kontaktní údaje (běžné osobní údaje)

Jedná se o základní údaje, které jsou nezbytné pro identifikaci subjektu údajů a pro vzájemnou komunikaci:

- jméno a příjmení (případně titul);
- datum narození (pro odlišení klientů stejného jména a pro zdravotně-anamnestické účely);
- adresa bydliště, případně doručovací adresa;
- telefonní číslo;
- e-mailová adresa;
- u klientů – podnikatelů (OSVČ) dále IČO, DIČ, sídlo;
- podpis (na souhlasu se zpracováním, na reklamačním protokolu, na předávacím protokolu apod.).

## 4.2 B) Zdravotní údaje – ZVLÁŠTNÍ KATEGORIE (čl. 9 GDPR)

Tyto údaje patří mezi zvláštní kategorie osobních údajů ve smyslu čl. 9 odst. 1 GDPR a jejich zpracování je možné pouze za splnění některé z výjimek dle čl. 9 odst. 2 GDPR – v případě Správce výhradně na základě výslovného souhlasu subjektu údajů dle čl. 9 odst. 2 písm. a) GDPR (viz podrobně článek 6 těchto Zásad). Konkrétně zpracováváme:

- anamnézu – zdravotní stav v minulosti i současnosti, prodělaná onemocnění, operace, hospitalizace;
- popis aktuálních obtíží a důvodu návštěvy, popis subjektivních pocitů klienta;
- užívané léky, doplňky stravy, bylinné přípravky (název, dávkování);
- alergie a intolerance (potravinové, lékové, kontaktní);
- výsledky screeningových měření prováděných v rámci našich služeb – např. údaje z přístroje Bicom Body Check, měření EAV (elektroakupunktura dle Volla), termografie, iridologie či obdobných nelékařských metod, které slouží výhradně pro orientační vyhodnocení v rámci poskytované služby a nepředstavují lékařskou diagnostiku;
- fotografická dokumentace pleti, vlasů nebo viditelných obtíží (pouze pokud to konkrétní metoda vyžaduje a pouze s výslovným souhlasem klienta);
- záznamy o průběhu jednotlivých sezení, doporučení k dalšímu postupu, poznámky terapeuta;
- kopie zpráv od lékařů a kopie laboratorních výsledků, které se pacient rozhodl poskytnout

k upřesnění svého zdravotního stavu;

- reakce klienta na předchozí sezení (pro vyhodnocení účinnosti).

**Upozornění:** Údaje z výše uvedených metod nejsou diagnostickými údaji ve smyslu zákona č. 372/2011 Sb., o zdravotních službách, a Správce s nimi nakládá výlučně jako s podkladem pro poskytnutí své nelékařské služby. Klient bere na vědomí, že naše služby nenahrazují lékařskou péči.

## 4.3 C) Platební údaje

- číslo bankovního účtu klienta (pokud platí převodem nebo požaduje vrácení platby);
- číslo platební karty / token z platební brány (Správce sám čísla karet neukládá, pracuje s tokenizovanou referencí poskytovatele platební brány);
- údaje uvedené na vystavených fakturách a daňových dokladech (fakturační adresa, IČO, DIČ);
- historie plateb (datum, částka, způsob úhrady, variabilní symbol).

## 4.4 D) Komunikační a transakční údaje

- záznamy o objednávkách a rezervacích (datum, čas, druh služby, místo, případně osoba terapeuta);
- e-mailová komunikace, zprávy v rezervačním systému, SMS, případně chatová komunikace;
- záznamy o uskutečněných telefonních hovorech (datum, čas, telefonní číslo) – Správce hovory standardně nenahrává; pokud by k nahrávání hovorů přistoupil, bude o tom volajícího vždy předem informovat;
- údaje z odběru newsletteru (e-mailová adresa, datum udělení souhlasu, IP adresa, ze které byl souhlas udělen).

## 4.5 E) Údaje z webu a marketingu

- IP adresa návštěvníka, User-Agent (typ a verze prohlížeče), operační systém, rozlišení obrazovky, jazyk;
- cookies a obdobné technologie (viz článek 12 těchto Zásad);
- behaviorální údaje – navštívené stránky, doba strávená na stránce, zdroj návštěvy, kliky (typicky

prostřednictvím nástrojů Google Analytics 4 a/nebo Meta Pixel, pokud uživatel udělil souhlas);

- údaje vyplněné v kontaktním nebo poptávkovém formuláři na webu;
- údaje o otevírání e-mailů z našich obchodních sdělení (open rate, kliky) – v rozsahu, který umožňuje mailingový nástroj.

#### 4.6 F) Údaje z videodohledu (kamerový systém, je-li provozován)

Pokud Správce v provozovně provozuje kamerový systém se záznamem, zpracovává následující údaje:

- obrazový záznam osob vstupujících do prostor provozovny (vstupní zóna, recepce, případně chodby; nikoliv prostory terapie, čekárny ani sociální zařízení);
- datum a čas pořízení záznamu.

O instalaci kamerového systému jsou subjekty údajů informovány prostřednictvím viditelně umístěné informační cedule u vstupu do provozovny, která obsahuje piktogram kamery a odkaz na tyto Zásady. Záznamy jsou uchovávány po dobu maximálně 7 dní a poté automaticky přepisovány.

### 5. Účely a právní základy zpracování (čl. 6 a čl. 9 GDPR)

V souladu se zásadou zákonnosti zpracování dle **čl. 5 odst. 1 písm. a) GDPR** zpracovává Správce osobní údaje výhradně na základě některého z právních titulů uvedených v čl. 6 odst. 1 GDPR, případně v čl. 9 odst. 2 GDPR u zvláštních kategorií údajů. Přehled jednotlivých účelů zpracování a odpovídajících právních titulů uvádíme v následující tabulce:

Účel zpracování	Kategorie údajů	Právní základ	Doba uchování
Rezervace služby a její poskytnutí (vč. komunikace ohledně termínu)	identifikační, kontaktní, transakční	čl. 6 odst. 1 písm. b) GDPR – plnění smlouvy	3 roky od posledního sezení
Vedení anamnézy a zdravotní dokumentace klienta	zvláštní kategorie – zdravotní údaje (čl. 9)	čl. 9 odst. 2 písm. a) GDPR – výslovný souhlas	po dobu trvání souhlasu + 3 roky
Fakturace a vedení účetnictví, daňové povinnosti	identifikační, platební, fakturační	čl. 6 odst. 1 písm. c) GDPR – plnění právní povinnosti (§ 35a ZDPH, § 31 ZÚ)	10 let od konce zdaňovacího období
Marketing vůči stávajícím zákazníkům (vlastní obdobné služby)	kontaktní, transakční	čl. 6 odst. 1 písm. f) GDPR – oprávněný zájem (§ 7 odst. 3 zák. 480/2004 Sb.)	3 roky od poslední objednávky / do odhlášení
Newsletter zájemcům, kteří nejsou zákazníci	kontaktní (e-mail, jméno)	čl. 6 odst. 1 písm. a) GDPR – souhlas	do odvolání souhlasu
Analytické a marketingové cookies	behaviorální, on-line identifikátory	čl. 6 odst. 1 písm. a) GDPR – souhlas (§ 89 odst. 3 zák. 127/2005 Sb.)	1–13 měsíců dle typu
Vyřízení reklamací, řešení sporů, právní obrana	všechny relevantní kategorie	čl. 6 odst. 1 písm. f) GDPR – oprávněný zájem	3 roky od ukončení reklamace / sporu
Kamerový systém v provozovně (je-li instalován)	vizuální záznam, datum, čas	čl. 6 odst. 1 písm. f) GDPR – oprávněný zájem (ochrana majetku a osob)	7 dní
Plnění součinnostní povinnosti vůči orgánům veřejné moci	vše relevantní pro daný účel	čl. 6 odst. 1 písm. c) GDPR – plnění právní povinnosti	dle příslušného zákona

## 5.1 Zásady zpracování dle čl. 5 GDPR

Při všech operacích zpracování dodržuje Správce zásady stanovené v čl. 5 odst. 1 GDPR:

- **zákonnost, korektnost a transparentnost** – zpracování probíhá pouze na základě platného právního titulu a klient je o něm srozumitelně informován;
- **účelové omezení** – údaje jsou shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nejsou dále zpracovávány způsobem neslučitelným s těmito účely;
- **minimalizace údajů** – zpracováváme jen údaje přiměřené, relevantní a omezené na nezbytný rozsah;
- **přesnost** – usilujeme o to, aby údaje byly přesné a v případě potřeby aktualizované;
- **omezení uložení** – údaje uchováváme ve formě umožňující identifikaci subjektů údajů jen po dobu nezbytnou pro účely zpracování;
- **integrita a důvěrnost** – zajišťujeme náležité zabezpečení údajů technickými a organizačními opatřeními (viz článek 11);
- **odpovědnost (accountability)** – jako Správce odpovídáme za dodržení uvedených zásad a jsme schopni jejich dodržení doložit.

## 6. Zvláštní kategorie údajů – zdravotní data (čl. 9 GDPR)

### 6.1 Proč naše služby nejsou zdravotní péčí

Centrum alternativní medicíny provozované Správce **není poskytovatelem zdravotních služeb** ve smyslu zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování. Naše služby nejsou vázány na oprávnění k poskytování zdravotních služeb vydané krajským úřadem, neprovádíme lékařskou diagnostiku, neordinujeme léčbu a nenahrazujeme lékařskou péči. Naše činnost je vykonávána na základě živnostenského oprávnění (volná živnost, případně řemeslné či vázané živnosti v rámci kosmetických, regeneračních a obdobných služeb).

Z této skutečnosti plyne důležitý důsledek: pro zpracování zdravotních údajů klienta **nemůžeme využít výjimky dle čl. 9 odst. 2 písm. h) GDPR** (zpracování pro účely preventivního nebo pracovního lékařství, lékařské diagnostiky, poskytování zdravotní nebo sociální péče), neboť tato výjimka je vyhrazena pouze registrovaným poskytovatelům zdravotních služeb.

### 6.2 Jediný použitelný právní titul – výslovný souhlas

Pro zpracování zdravotních údajů klientů využíváme výhradně výjimku dle **čl. 9 odst. 2 písm. a) GDPR – výslovný souhlas subjektu údajů**. Bez tohoto souhlasu nemůžeme zdravotní údaje zpracovávat, a tedy ani řádně poskytnout službu, jejíž součástí je práce se zdravotními údaji klienta.

### 6.3 Náležitosti výslovného souhlasu

Souhlas se zpracováním zdravotních údajů musí podle čl. 4 odst. 11, čl. 7 a čl. 9 odst. 2 písm. a) GDPR splňovat tyto náležitosti:

- **svobodný** – udělení souhlasu nesmí být podmínkou poskytnutí jiné služby, která se zdravotními údaji nespojuje; odepření nebo odvolání souhlasu nesmí znevýhodnit klienta v jiných oblastech vztahu se Správce;
- **konkrétní** – souhlas se vztahuje na vymezené účely (vedení anamnézy, záznamy o sezeních, vyhodnocení screeningových měření) a pro každý další účel, který není slučitelný s původním, je třeba získat souhlas samostatný;
- **informovaný** – klient před udělením souhlasu obdrží informace dle čl. 13 GDPR (identifikace Správce, účel,

právní základ, doba, příjemci, práva subjektu, možnost odvolání);

- **jednoznačný** – souhlas je udělen aktivním projevem vůle (typicky podpisem formuláře), nikoliv mlčky, předzaškrtnutým políčkem nebo neaktivitou;
- **výslovný** – u zvláštních kategorií údajů je nutná zvýšená forma souhlasu, typicky písemná, oddělená od ostatních smluvních dokumentů;
- **odvolatelný** – klient může souhlas kdykoliv odvolat, a to stejně snadnou cestou, jakou byl udělen; odvolání nemá vliv na zákonnost dříve provedeného zpracování.

## 6.4 Postup udělení souhlasu

Souhlas se zpracováním zdravotních údajů uděluje klient při své první návštěvě prostřednictvím samostatného papírového formuláře (vzor v Příloze č. 1 těchto Zásad). Formulář je oddělený od všeobecných obchodních podmínek a od smlouvy o poskytnutí služby, aby bylo z hlediska transparentnosti zřejmé, čeho se souhlas týká. Klient obdrží kopii podepsaného souhlasu a originál zůstává u Správce.

U klientů, kteří objednávají službu vyžadující práci se zdravotními údaji on-line, je elektronický předběžný souhlas potvrzen při první osobní návštěvě v písemné formě tak, aby byla zachována dokazatelnost.

## 6.5 Postup odvolání souhlasu

Souhlas lze odvolat:

- e-mailem zaslaným na adresu info@resonica.cz (postačí prostá zpráva typu „odvolávám souhlas se zpracováním zdravotních údajů“ s uvedením identifikace);
- písemně na adresu sídla Správce;
- osobně v provozovně.

Po odvolání souhlasu Správce neprodleně ukončí další zpracování zdravotních údajů klienta pro účely, k nimž byl souhlas udělen. Údaje, které je Správce povinen uchovávat na základě jiného právního titulu (zejména pro účely účetnictví, daní, pro právní obranu v případě sporu), nejsou tímto odvoláním dotčeny. Klient bere na vědomí, že odvolání souhlasu může vést k tomu, že Správce nadále nebude moci poskytovat služby, jejichž součástí je práce se zdravotními údaji.

## 7. Práva subjektů údajů (čl. 12–23 GDPR)

Subjekt údajů má v souvislosti se zpracováním svých osobních údajů následující práva:

### 7.1 A) Právo na informace (čl. 13 a 14 GDPR)

Správce má povinnost subjekt údajů informovat o všech podstatných okolnostech zpracování. Tuto povinnost plní Správce primárně prostřednictvím těchto Zásad, dále pak prostřednictvím cookies banneru na webu, krátkých informačních textů u jednotlivých formulářů a osobním poučením při první návštěvě.

### 7.2 B) Právo na přístup k osobním údajům (čl. 15 GDPR)

Subjekt údajů má právo získat od Správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud ano, má právo získat přístup k těmto údajům a k informacím o:

- účelech zpracování;
- kategoriích dotčených osobních údajů;
- příjemcích nebo kategoriích příjemců, kterým údaje byly nebo budou zpřístupněny;
- plánované době, po kterou budou údaje uloženy, nebo není-li ji možné určit, o kritériích pro stanovení této

doby;

- existenci práva požadovat opravu, výmaz, omezení zpracování a vznést námitku;
- právu podat stížnost u dozorového úřadu;
- zdroji údajů (pokud nebyly získány od subjektu údajů);
- existenci automatizovaného rozhodování, včetně profilování.

Na vyžádání Správce poskytne kopii zpracovávaných osobních údajů; první kopie je bezplatná, za další kopie může Správce účtovat přiměřený poplatek na základě administrativních nákladů.

### **7.3 C) Právo na opravu (čl. 16 GDPR)**

Subjekt údajů má právo na opravu nepřesných osobních údajů, které se ho týkají, a s přihlédnutím k účelům zpracování i právo na doplnění neúplných osobních údajů. Správce provádí opravu bez zbytečného odkladu po obdržení žádosti, nejpozději však ve lhůtě 1 měsíce.

### **7.4 D) Právo na výmaz – „právo být zapomenut“ (čl. 17 GDPR)**

Subjekt údajů má právo na to, aby Správce bez zbytečného odkladu vymazal jeho osobní údaje, pokud je dán některý z důvodů uvedených v čl. 17 odst. 1 GDPR (zejména: údaje již nejsou potřebné pro účel, pro který byly shromážděny; subjekt odvolal souhlas a neexistuje jiný právní titul; subjekt vznesl námitku a neexistují převažující oprávněné důvody; údaje byly zpracovány protiprávně; výmaz je vyžadován právní povinností).

Právo na výmaz se neuplatní v případech vymezených v čl. 17 odst. 3 GDPR – zejména pokud je zpracování nezbytné pro:

- splnění právní povinnosti (typicky archivace daňových dokladů 10 let dle § 35a ZDPH – Správce nemůže fakturu vymazat dříve, než uplyne zákonná doba);
- určení, výkon nebo obhajobu právních nároků (např. nedořešená reklamace, soudní spor);
- výkon práva na svobodu projevu a informací;
- účely archivace ve veřejném zájmu, vědeckého a historického výzkumu či pro statistické účely.

### **7.5 E) Právo na omezení zpracování (čl. 18 GDPR)**

Subjekt údajů má právo na to, aby Správce omezil zpracování, zejména pokud popírá přesnost údajů (na dobu potřebnou k ověření), pokud je zpracování protiprávní, ale subjekt nechce výmaz, pokud Správce již údaje nepotřebuje, ale subjekt je požaduje pro určení, výkon nebo obhajobu právních nároků, nebo pokud subjekt vznesl námitku (do doby ověření).

### **7.6 F) Právo na přenositelnost údajů (čl. 20 GDPR)**

Subjekt údajů má právo získat osobní údaje, které poskytl Správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci. Toto právo se uplatní pouze tehdy, je-li zpracování založeno na souhlasu nebo na smlouvě a zároveň probíhá automatizovaně. Na zpracování založené na oprávněném zájmu nebo na právní povinnosti se právo na přenositelnost nevztahuje.

### **7.7 G) Právo vznést námitku (čl. 21 GDPR)**

Subjekt údajů má právo kdykoli vznést námitku proti zpracování, které je založeno na oprávněném zájmu Správce dle čl. 6 odst. 1 písm. f) GDPR. Správce v takovém případě dále neprovádí zpracování, ledaže prokáže závažné oprávněné důvody, které převažují nad zájmy, právy a svobodami subjektu údajů, nebo důvody pro určení, výkon nebo obhajobu právních nároků. Námitku proti zpracování pro účely přímého marketingu je Správce povinen vždy plně respektovat.

## 7.8 H) Právo nebyt předmětem automatizovaného rozhodování (čl. 22 GDPR)

Subjekt údajů má právo nebyt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něj právní účinky nebo se ho obdobným způsobem významně dotýká. Správce prohlašuje, že automatizované rozhodování s právními účinky pro klienty neprovádí. Cookies a webové analytické nástroje neslouží k automatizovanému rozhodování v tomto smyslu.

## 7.9 I) Právo podat stížnost u dozorového úřadu (čl. 77 GDPR)

Subjekt údajů má právo podat stížnost u dozorového úřadu, pokud se domnívá, že zpracováním jeho osobních údajů byly porušeny právní předpisy. V České republice je dozorovým úřadem Úřad pro ochranu osobních údajů:

- Adresa: Plk. Sochora 27, 170 00 Praha 7
- Telefon: +420 234 665 111
- E-mail: [posta@uouu.cz](mailto:posta@uouu.cz)
- Web: <https://www.uouu.gov.cz>

## 7.10 J) Právo odvolat souhlas (čl. 7 odst. 3 GDPR)

Pokud je zpracování založeno na souhlasu, má subjekt údajů právo souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Odvolat souhlas lze stejnou cestou, jakou byl udělen (e-mail, písemně, osobně).

## 7.11 Postup uplatnění práv

Žádost o uplatnění práv lze podat:

- e-mailem na adresu [info@resonica.cz](mailto:info@resonica.cz) (předmět: „GDPR – žádost subjektu údajů“);
- písemně na adresu sídla Topolská 952, Chrudim II, 537 05 Chrudim;
- osobně v provozovně Topolská 952, Chrudim II, 537 05 Chrudim po předchozí domluvě.

Správce vyřídí žádost bez zbytečného odkladu, nejpozději ve lhůtě 1 měsíce od jejího obdržení. Tuto lhůtu lze v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další 2 měsíce; o prodloužení Správce subjekt údajů informuje, a to ve lhůtě 1 měsíce od obdržení žádosti, spolu s důvody pro odklad.

Vyřízení žádosti je bezplatné. Pouze v případě zjevně nedůvodných nebo nepřiměřených žádostí (zejména opakovaných) může Správce požadovat přiměřený poplatek zohledňující administrativní náklady, nebo žádost odmítnout. Před vyřízením žádosti je Správce oprávněn ověřit totožnost žadatele tak, aby zabránil neoprávněnému přístupu k osobním údajům.

Vzor žádosti je k dispozici jako Příloha č. 2 těchto Zásad.

## 8. Příjemci osobních údajů

Osobní údaje předává Správce v nezbytném rozsahu vybraným zpracovatelům a příjemcům, kteří poskytují Správci služby nezbytné pro jeho činnost. Se všemi zpracovateli má Správce v souladu s **čl. 28 GDPR** uzavřenou smlouvu o zpracování osobních údajů, která stanoví předmět a dobu zpracování, povahu a účel zpracování, kategorie osobních údajů a subjektů údajů, povinnosti a práva Správce a povinnosti zpracovatele (zejména povinnost mlčenlivosti, povinnost zabezpečit údaje, povinnost vrátit nebo vymazat údaje po skončení smlouvy, povinnost umožnit kontrolu).

Kategorie příjemce	Účel předání / typičtí poskytovatelé	Kategorie údajů
Účetní kancelář / externí účetní	vedení účetnictví, daňová evidence, mzdy	identifikační, fakturační, platební

Kategorie příjemce	Účel předání / typičtí poskytovatelé	Kategorie údajů
Daňový poradce	daňová optimalizace, příprava daňových přiznání	identifikační, fakturační
Poskytovatel hostingu webu a e-mailu	provoz webových stránek a e-mailových schránek (např. Google Workspace, Wedos, Forpsi, Microsoft 365)	kontaktní, komunikační, technické
Provozovatel rezervačního systému	správa rezervací a klientského kalendáře (např. Reservio, Booksy, Noona, Reenio)	identifikační, kontaktní, transakční
Poskytovatel e-mailingového nástroje	rozesílka newsletterů a obchodních sdělení (např. Mailchimp, Ecomail, SmartEmailing)	kontaktní, behaviorální (otevírání e-mailů)
Banka	Fio banka, a.s. — vede provozní účet Resonica s.r.o. (č. 2603306593/2010)	platební, fakturační
Poskytovatel cloudového úložiště	ukládání pracovních dokumentů (např. Google Drive, OneDrive, Dropbox)	dle obsahu uloženého souboru
CRM systém (je-li používán)	evidence klientů a komunikace	identifikační, kontaktní, transakční
Nástroje webové analytiky a marketingu	analýza návštěvnosti a marketing (např. Google Analytics 4, Meta Pixel) – pouze se souhlasem	on-line identifikátory, behaviorální
Advokátní kancelář / právní zástupce	právní poradenství, zastupování v případě sporu	dle potřeby konkrétního případu
Orgány veřejné moci	plnění zákonných povinností (FÚ, ÚOOÚ, ČOI, soudy, policie ČR)	v rozsahu vyžadovaném zákonem

Správce důsledně dbá na to, aby každý zpracovatel poskytoval dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky GDPR a byla zajištěna ochrana práv subjektů údajů. Aktuální seznam konkrétních zpracovatelů Správce vede ve své interní dokumentaci (Příloha č. 3) a na vyžádání jej sdělí subjektu údajů.

## 9. Předávání osobních údajů do třetích zemí mimo EU

Některé nástroje a služby, které Správce využívá, mohou vést k předávání osobních údajů do třetích zemí mimo Evropský hospodářský prostor (EHP), zejména do Spojených států amerických. Jde především o:

- služby společnosti Google LLC (Google Workspace, Google Analytics 4, Google Ads, YouTube);
- služby společnosti Meta Platforms, Inc. (Facebook, Instagram, Meta Pixel);
- služby společnosti Microsoft Corporation (Microsoft 365, OneDrive);
- další služby, jejichž poskytovatelé sídlí ve třetích zemích.

### 9.1 Záruky pro předání

Předávání probíhá vždy pouze za podmínek stanovených v čl. 44–49 GDPR, zejména s následujícími zárukami:

- **Rozhodnutí o přiměřenosti dle čl. 45 GDPR** – pro USA je od 10. 7. 2023 v platnosti rámec EU-US Data Privacy Framework (DPF). Předání ke společnostem certifikovaným pod DPF je považováno za předání do země s odpovídající úrovní ochrany;
- **Standardní smluvní doložky (SCC) dle čl. 46 odst. 2 písm. c) GDPR** – v případě, že příjemce není certifikován pod DPF, využívá Správce standardní smluvní doložky schválené Evropskou komisí (rozhodnutí (EU) 2021/914);

- **Dodatečná technická a organizační opatření** – tam, kde to vyžaduje aktuální praxe (např. doporučení EDPB k dopadům rozsudku Schrems II), Správce zajišťuje doplňková opatření, jako je šifrování, pseudonymizace či omezení rozsahu předávaných údajů.

Klient má právo si na vyžádání u Správce vyžádat informaci o konkrétních zárukách pro předání jeho osobních údajů do třetí země, případně kopii standardních smluvních doložek.

## 10. Doby uchování osobních údajů

V souladu se zásadou omezení uložení dle **čl. 5 odst. 1 písm. e) GDPR** uchovává Správce osobní údaje pouze po dobu, která je nezbytná pro účely, pro něž jsou zpracovávány, případně po dobu vyžadovanou zákonem. Konkrétní doby uvádí následující tabulka:

Kategorie údajů	Doba uchování	Právní důvod
Anamnézy a záznamy ze sezení (zdravotní údaje)	doba trvání souhlasu + 3 roky po posledním sezení	souhlas + lhůta pro uplatnění práv
Účetní a daňové doklady (faktury, daňové doklady)	10 let od konce zdaňovacího období	§ 35a zák. 235/2004 Sb. (ZDPH)
Účetní knihy, účetní záznamy	5 až 10 let	§ 31 a 32 zák. 563/1991 Sb. (ZÚ)
Rezervační záznamy (jméno, kontakt, termín)	3 roky od posledního sezení	oprávněný zájem / promlčecí lhůta
Marketingové údaje (newsletter, obchodní sdělení)	do odvolání souhlasu / odhlášení	souhlas, § 7 zák. 480/2004 Sb.
Cookies (analytické, marketingové)	1–13 měsíců dle typu	doba platnosti uděleného souhlasu
Kamerové záznamy (je-li systém provozován)	maximálně 7 dní	oprávněný zájem (bezpečnost)
E-mailová a jiná elektronická komunikace	3 roky od posledního kontaktu	oprávněný zájem (právní obrana)
Logy webserveru	maximálně 6 měsíců	oprávněný zájem (bezpečnost a provoz)
Reklamační dokumentace	3 roky od ukončení reklamace	oprávněný zájem / promlčecí lhůta

Po uplynutí uvedených dob jsou osobní údaje bezpečně zlikvidovány (fyzická skartace, nevratné vymazání ze všech systémů a záloh). Anonymizované nebo agregované údaje, ze kterých již nelze identifikovat konkrétní osobu, mohou být uchovávány i déle pro statistické a analytické účely.

## 11. Zabezpečení osobních údajů (čl. 32 GDPR)

Správce zavedl s ohledem na povahu, rozsah, kontext a účely zpracování i na různě pravděpodobná a různě závažná rizika pro práva a svobody fyzických osob vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, jak vyžaduje **čl. 32 GDPR**.

### 11.1 Fyzická bezpečnost

- uzamykatelné prostory provozovny, vstup pouze pro zaměstnance a klienty po ohlášení;
- elektronický zabezpečovací systém (alarm) napojený na PCO;
- papírová dokumentace s anamnézami uložena v uzamykatelných kartotékách / skříních;

- skartace papírových dokumentů s osobními údaji v certifikované skartovači (úroveň P-4 a vyšší);
- omezený přístup do pracovních prostor a serverové místnosti / IT zázemí.

## **11.2 IT bezpečnost**

- silná hesla a vícefaktorové ověřování (2FA) pro přístup ke všem systémům, kde to je možné;
- šifrování pevných disků pracovních počítačů a notebooků (BitLocker / FileVault);
- aktualizovaný antivirový a antimalwarový program;
- firewall na úrovni sítě a koncových zařízení;
- pravidelné aktualizace operačních systémů a aplikací;
- zabezpečení Wi-Fi sítě (WPA2/WPA3), oddělená síť pro hosty;
- šifrovaná komunikace (HTTPS/TLS) na webových stránkách Správce a u všech používaných služeb;
- omezení vzdáleného přístupu (VPN, IP whitelisting).

## **11.3 Zálohování**

- pravidelné automatizované zálohy klíčových systémů (minimálně 1× týdně);
- zálohy ukládány šifrovaně, v oddělené lokalitě (cloud nebo offline médium);
- pravidelné testování obnovitelnosti záloh;
- dodržení pravidla 3-2-1 (3 kopie dat, 2 různá média, 1 mimo provozovnu).

## **11.4 Přístupová oprávnění**

- uplatnění principu „need to know“ a nejmenších privilegií (least privilege);
- individuální uživatelské účty pro každého zaměstnance, žádné sdílené účty;
- pravidelná revize přístupových oprávnění (minimálně 1× ročně);
- okamžité odebrání přístupu při ukončení pracovněprávního vztahu.

## **11.5 Organizační opatření**

- proškolení všech zaměstnanců a spolupracovníků o GDPR a o vnitřních pravidlech zpracování OÚ při nástupu a opakovaně 1× ročně;
- písemné dohody o mlčenlivosti (NDA) se všemi zaměstnanci a spolupracovníky;
- interní směrnice pro práci s osobními údaji a interní postup pro řešení žádostí subjektů údajů a porušení zabezpečení;
- pseudonymizace zdravotních záznamů v elektronických systémech tam, kde to je technicky možné (oddělení identifikačních a obsahových údajů);
- používání zámku obrazovky a automatického odhlášení po nečinnosti.

# **12. Cookies a sledovací technologie**

## **12.1 Co jsou cookies**

Cookies jsou krátké textové soubory, které jsou při návštěvě internetových stránek ukládány do koncového zařízení uživatele (počítač, mobilní telefon, tablet). Cookies plní různé funkce – některé jsou nezbytné pro chod webu (např. udržení přihlášení, obsah košíku, jazyková preference), jiné slouží k měření návštěvnosti, ke zlepšování uživatelského zážitku nebo k cílené reklamě.

## 12.2 Právní rámec

Použití cookies upravuje § 89 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění zákona č. 374/2021 Sb. účinného od 1. 1. 2022. Tato úprava zavedla princip „opt-in“ – pro ukládání cookies (s výjimkou těch technicky nezbytných) je nutný předchozí prokazatelný souhlas uživatele. Souhlas musí splňovat náležitosti dle čl. 4 odst. 11 a čl. 7 GDPR – musí být svobodný, konkrétní, informovaný a jednoznačný, a stejně snadno odvolatelný, jako byl udělen.

## 12.3 Kategorie cookies používaných na webu Správce

Kategorie	Popis	Souhlas
Nezbytné (technické)	Umožňují základní funkce webu – přihlášení, košík, jazyk, bezpečnostní funkce. Bez nich web nemůže správně fungovat.	NE – výjimka § 89 odst. 3
Preferenční	Pamatují si nastavení uživatele – design, jazyk, region, písmo. Slouží ke komfortu, nikoliv k chodu webu.	ANO
Analytické	Měří návštěvnost a chování uživatelů (Google Analytics 4, Hotjar, Microsoft Clarity). Údaje jsou používány pro statistické účely a zlepšování webu.	ANO (opt-in)
Marketingové	Slouží k cílené reklamě a remarketingu (Meta Pixel, Google Ads, LinkedIn Insight Tag). Údaje jsou předávány třetím stranám pro marketingové účely.	ANO (opt-in)

## 12.4 Konkrétní cookies

Aktuální detailní seznam konkrétních cookies, jejich účelu, doby trvání a dodavatele je dostupný v nastavení cookie banneru na webu Správce. Příklad obvykle používaných cookies:

Název	Účel	Doba	Typ
cookie_consent	uložení volby uživatele v cookie banneru	12 měsíců	nezbytné
PHPSESSID / session_id	identifikace přihlášené relace	do konce relace	nezbytné
_ga, _ga_*	Google Analytics 4 – statistika návštěvnosti	13 měsíců	analytické
_gid	Google Analytics – rozlišení uživatelů	24 hodin	analytické
_fbp	Meta Pixel – marketing a remarketing	3 měsíce	marketingové
fr	Meta – reklamní platforma Facebook	3 měsíce	marketingové
_gcl_au	Google Ads – konverzní měření	3 měsíce	marketingové

## 12.5 Cookie banner a správa souhlasu

Při první návštěvě webu se uživateli zobrazí cookie banner, který obsahuje:

- jasnou a srozumitelnou informaci o použití cookies;
- možnost přijmout všechny cookies;
- možnost odmítnout všechny non-essential cookies (tlačítko „Odmítnout vše“ nebo ekvivalent na stejné úrovni viditelnosti jako „Přijmout vše“);
- možnost individuálního nastavení po jednotlivých kategoriích;

- odkaz na tyto Zásady, resp. na samostatnou Cookie Policy.

Uživatel může své rozhodnutí kdykoliv změnit prostřednictvím odkazu „Nastavení cookies“ trvale umístěného v patičce webu, nebo vymazáním cookies ve svém prohlížeči (čímž dojde k zobrazení banneru při příští návštěvě).

## 12.6 Nastavení cookies v prohlížeči

Uživatel může cookies spravovat také přímo v prohlížeči – povolit, omezit, smazat nebo zcela zakázat. Postup se liší podle prohlížeče:

- Google Chrome: Nastavení → Soukromí a zabezpečení → Soubory cookie a další data webů;
- Mozilla Firefox: Nastavení → Soukromí a zabezpečení → Cookies a data stránek;
- Apple Safari: Předvolby → Soukromí → Spravovat data webových stránek;
- Microsoft Edge: Nastavení → Soubory cookie a oprávnění webu.

Upozorňujeme, že omezení nebo zakázání cookies může mít vliv na funkčnost webových stránek, zejména u funkcí vyžadujících nezbytné cookies.

## 13. E-mail marketing a obchodní sdělení

Zasílání obchodních sdělení elektronickými prostředky upravuje **§ 7 zákona č. 480/2004 Sb.**, o některých službách informační společnosti. Správce při své marketingové komunikaci důsledně dodržuje pravidla tohoto zákona a GDPR.

### 13.1 Princip opt-in (souhlas)

Obchodní sdělení (newsletter, nabídky, informace o akcích, slevách a novinkách) zasíláme zájemcům, kteří k tomu udělili souhlas, a to:

- prostřednictvím přihlašovacího formuláře na webu (zadání e-mailu a aktivní zaškrtnutí souhlasu, tzv. double opt-in s potvrzovacím e-mailem);
- na základě papírového formuláře udělením souhlasu při návštěvě v provozovně.

### 13.2 Výjimka pro stávající zákazníky (§ 7 odst. 3 zák. 480/2004 Sb.)

Bez výslovného souhlasu jsme oprávněni zasílat obchodní sdělení osobám, které jsou našimi zákazníky, za současného splnění všech těchto podmínek:

- e-mailovou adresu jsme získali v souvislosti s prodejem vlastní služby;
- obchodní sdělení se týká pouze vlastních obdobných služeb Správce, nikoliv služeb třetích stran;
- zákazník měl možnost odmítnout zasílání obchodních sdělení již při získání kontaktu, a má tuto možnost (jednoduchou a bezplatnou) v každém zaslaném sdělení (odhlašovací odkaz);
- zákazník odběr neodmítl.

### 13.3 Náležitosti obchodních sdělení

Každé obchodní sdělení Správce obsahuje:

- zřetelné označení, že se jedná o obchodní sdělení;
- identifikaci odesílatele – obchodní firmu, IČO, sídlo a kontakt;
- jednoduchý a bezplatný odhlašovací mechanismus (odkaz „Odhlásit se z odběru“ v patičce e-mailu).

## 13.4 Sankce za porušení

Za porušení povinností při zasílání obchodních sdělení může Úřad pro ochranu osobních údajů uložit pokutu až do výše 10 000 000 Kč (§ 11 zák. 480/2004 Sb.). Správce proto věnuje této oblasti zvýšenou pozornost a vede evidenci udělených souhlasů a odhlášení.

## 14. Záznamy o činnostech zpracování (čl. 30 GDPR)

Podle **čl. 30 odst. 1 GDPR** vede každý správce záznamy o činnostech zpracování, za něž odpovídá. Výjimka dle čl. 30 odst. 5 GDPR (pro správce s méně než 250 zaměstnanci) se na Správce **NEUPLATNÍ**, neboť Správce zpracovává zvláštní kategorie údajů ve smyslu čl. 9 GDPR (zdravotní údaje klientů). Záznamy o činnostech zpracování proto Správce vede vždy a v plném rozsahu.

### 14.1 Obsah záznamů

Záznamy vedené Správce podle čl. 30 odst. 1 GDPR obsahují zejména:

- jméno a kontaktní údaje Správce;
- účely zpracování pro každou jednotlivou činnost zpracování;
- popis kategorií subjektů údajů a kategorií osobních údajů;
- kategorie příjemců, kterým byly nebo budou údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
- případné předání osobních údajů do třetí země nebo mezinárodní organizaci, identifikaci dané třetí země a doložení vhodných záruk;
- plánované lhůty pro výmaz jednotlivých kategorií údajů (pokud je možné je určit);
- obecný popis technických a organizačních bezpečnostních opatření podle čl. 32 odst. 1 GDPR.

### 14.2 Forma a dostupnost záznamů

Záznamy jsou vedeny v písemné, případně elektronické podobě. Na vyžádání je Správce předloží dozorovému úřadu (ÚOOÚ). Vzor záznamu o činnostech zpracování pro interní použití tvoří Přílohu č. 4 těchto Zásad.

## 15. Posouzení vlivu na ochranu osobních údajů (DPIA, čl. 35 GDPR)

Podle **čl. 35 odst. 1 GDPR** je správce povinen provést posouzení vlivu na ochranu osobních údajů (DPIA – Data Protection Impact Assessment), pokud je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, zejména při použití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování.

### 15.1 Kdy je DPIA povinná

Podle čl. 35 odst. 3 GDPR a podle seznamu zveřejněného ÚOOÚ je DPIA povinná zejména při:

- systematickém a rozsáhlém vyhodnocování osobních aspektů fyzických osob na základě automatizovaného zpracování, včetně profilování;
- rozsáhlém zpracování zvláštních kategorií údajů dle čl. 9 nebo údajů týkajících se rozsudků v trestních věcech a trestních činů dle čl. 10;
- rozsáhlém systematickém monitorování veřejně přístupných prostorů;
- využití nových technologií s neprověřenými dopady na soukromí (např. biometrie, AI rozhodování).

## 15.2 Posouzení v podmínkách Správce

Správce posoudil, zda jeho zpracování vyžaduje formální DPIA. Vzhledem k tomu, že:

- rozsah zpracování zvláštních kategorií údajů odpovídá běžnému provozu malého wellness centra (řádově desítky až nižší stovky klientů ročně);
- Správce neprovádí profilování ani automatizované rozhodování s právními účinky;
- Správce nevyužívá nové či vysoce rizikové technologie ve smyslu seznamu ÚOOÚ;

dospěl Správce k závěru, že DPIA v současné době povinná není. O tomto posouzení Správce vede písemný záznam, který bude pravidelně aktualizován. Pokud dojde k podstatné změně rozsahu, povahy či účelů zpracování (např. zavedení automatizovaného doporučování, biometrické identifikace klientů, výrazné rozšíření databáze klientů), Správce DPIA neprodleně provede.

## 16. Porušení zabezpečení osobních údajů (čl. 33 a 34 GDPR)

Pod pojmem porušení zabezpečení osobních údajů („data breach“) se rozumí jakékoliv porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů (čl. 4 odst. 12 GDPR). Typicky se jedná o ztrátu nešifrovaného notebooku s daty, odcizení papírové dokumentace, ransomware útok, neoprávněný přístup k databázi, omylem odeslaný e-mail s daty více klientů apod.

### 16.1 Postup při zjištění porušení

Po zjištění porušení zabezpečení Správce postupuje následovně:

- **1) Bezprostřední reakce** – zastavení rozšiřování incidentu (odpojení postiženého systému, změna hesel, zablokování přístupů), zajištění důkazů.
- **2) Vyhodnocení** – posouzení rozsahu incidentu, kategorií dotčených údajů a počtu dotčených subjektů, posouzení míry rizika pro práva a svobody subjektů.
- **3) Ohlášení ÚOOÚ** – pokud porušení pravděpodobně bude mít za následek riziko pro práva a svobody fyzických osob, ohlásí Správce porušení Úřadu pro ochranu osobních údajů, a to bez zbytečného odkladu, nejpozději do 72 hodin od okamžiku, kdy se o něm dozvěděl (čl. 33 odst. 1 GDPR). Pokud není možné ohlášení podat ve lhůtě 72 hodin, je doplněno odůvodnění zpoždění.
- **4) Informování subjektů údajů** – pokud je pravděpodobné, že porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob, Správce dotčené subjekty údajů o porušení informuje bez zbytečného odkladu (čl. 34 GDPR). Informace zahrnuje povahu porušení, kontaktní bod (DPO nebo jinou osobu), pravděpodobné důsledky a přijatá opatření.
- **5) Interní evidence** – všechna porušení zabezpečení Správce dokumentuje (datum, popis, dotčené údaje, důsledky, přijatá opatření) bez ohledu na to, zda byla ohlašována ÚOOÚ. Tato evidence slouží k prokázání souladu s čl. 33 odst. 5 GDPR.

### 16.2 Náležitosti ohlášení ÚOOÚ

Ohlášení dozorovému úřadu musí podle čl. 33 odst. 3 GDPR alespoň:

- popsat povahu daného porušení zabezpečení, včetně, pokud možno, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
- uvést jméno a kontaktní údaje pověřence (pokud je jmenován) nebo jiného kontaktního místa;
- popsat pravděpodobné důsledky porušení;
- popsat opatření, která Správce přijal nebo navrhl k vyřešení porušení a zmírnění jeho možných nepříznivých

účinků.

## 17. Postup pro vyřízení žádostí subjektu údajů

### 17.1 Podání žádosti

Subjekt údajů může uplatnit svá práva podle GDPR a podle těchto Zásad následujícími způsoby:

- e-mailem na adresu info@resonica.cz s předmětem „GDPR – žádost subjektu údajů“;
- písemně doporučeným dopisem na adresu sídla Topolská 952, Chrudim II, 537 05 Chrudim;
- osobně v provozovně Topolská 952, Chrudim II, 537 05 Chrudim po předchozí domluvě.

Pro urychlení vyřízení doporučujeme využít vzor žádosti (Příloha č. 2). Žádost by měla obsahovat: identifikaci žadatele, popis uplatňovaného práva, případně specifikaci údajů, kterých se žádost týká, a kontaktní údaje pro doručení odpovědi.

### 17.2 Ověření totožnosti žadatele

Aby zabránil neoprávněnému přístupu k osobním údajům třetí osoby, je Správce oprávněn před vyřízením žádosti ověřit totožnost žadatele. Ověření může proběhnout vyžádáním dodatečných informací (např. datum poslední objednávky, číslo posledního dokladu), zasláním ověřovacího kódu na e-mail evidovaný u Správce, případně osobním ověřením proti dokladu totožnosti. Pokud Správce nemůže totožnost žadatele rozumně ověřit, je oprávněn žádost odmítnout (čl. 12 odst. 6 GDPR).

### 17.3 Lhůty pro vyřízení

Správce vyřídí žádost bez zbytečného odkladu, nejpozději však do 1 měsíce od jejího obdržení. Tuto lhůtu lze v případě potřeby (s ohledem na složitost nebo počet žádostí) prodloužit o další 2 měsíce, tedy maximálně na 3 měsíce celkem. O prodloužení Správce subjekt údajů informuje do 1 měsíce od podání žádosti, spolu s důvody pro odklad.

### 17.4 Bezplatnost

Vyřízení žádosti je zpravidla bezplatné. V případě zjevně neopodstatněných nebo nepřiměřených žádostí (zejména opakujících se) je Správce oprávněn:

- účtovat přiměřený poplatek odpovídající administrativním nákladům spojeným s vyřízením žádosti; nebo
- odmítnout žádosti vyhovět.

Důkazní břemeno o nepřiměřenosti nebo neopodstatněnosti nese Správce.

### 17.5 Stížnost u dozorového úřadu

Pokud subjekt údajů není spokojen s vyřízením své žádosti nebo má za to, že Správce porušil své povinnosti při zpracování osobních údajů, má právo podat stížnost u Úřadu pro ochranu osobních údajů:

- Adresa: Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7;
- Telefon: +420 234 665 111;
- Datová schránka: qkbaa2n;
- E-mail: posta@uoou.cz;
- Web: <https://www.uoou.gov.cz>

## 18. Změny zásad zpracování osobních údajů

Správce si vyhrazuje právo tyto Zásady jednostranně měnit a doplňovat, zejména v reakci na změny právních předpisů, na vývoj judikatury, na rozhodovací praxi ÚOOÚ a Evropského sboru pro ochranu osobních údajů (EDPB), nebo z důvodu změn ve struktuře a rozsahu zpracování (nové služby, noví zpracovatelé, nové technologie).

Aktuální verze Zásad je vždy zveřejněna na webu Správce [www.resonica.cz](http://www.resonica.cz) a v provozovně k nahlédnutí v tištěné podobě. Datum poslední aktualizace a číslo verze jsou uvedeny v úvodu dokumentu.

O podstatných změnách Zásad budou aktivní klienti informováni – buď e-mailem na poslední známou e-mailovou adresu, nebo viditelným upozorněním na webu nejméně 14 dní před účinností změn. Pokračováním v využívání služeb po datu účinnosti změn vyjadřuje subjekt údajů, že byl se změnami seznámen.

## 19. Účinnost a závěrečná ustanovení

Tyto Zásady byly vydány Správce dne 15. května 2026 a nabývají účinnosti dnem 1. června 2026. Verze: 1.0.

Tyto Zásady ruší a nahrazují veškeré předchozí dokumenty Správce upravující ochranu osobních údajů.

Jednotlivá ustanovení těchto Zásad jsou oddělitelná. Bude-li některé ustanovení shledáno neplatným, nezákonným nebo nevynutitelným, ostatní ustanovení tím nejsou dotčena.

V případě jakýchkoliv dotazů ohledně zpracování osobních údajů, výkladu těchto Zásad nebo uplatnění práv subjektu údajů se obraťte na Správce prostřednictvím kontaktů uvedených v článku 2 těchto Zásad.

*Schválil/za Správce: jednatel společnosti Resonica s.r.o.*

*V Chrudimi, dne 15. května 2026.*

## Přílohy

### Příloha č. 1 – Vzor výslovného souhlasu se zpracováním zdravotních údajů

#### SOUHLAS SE ZPRACOVÁNÍM ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ – ZDRAVOTNÍCH ÚDAJŮ

Já, níže podepsaný/á:

- Jméno a příjmení: .....
- Datum narození: .....
- Adresa: .....
- E-mail: .....
- Telefon: .....

tímto v souladu s čl. 9 odst. 2 písm. a) nařízení (EU) 2016/679 (GDPR) **uděluji výslovný souhlas** správci osobních údajů – obchodní společnosti Resonica s.r.o., IČO 236 41 771, se sídlem Topolská 952, Chrudim II, 537 05 Chrudim (dále jen „Správce“), se zpracováním svých osobních údajů náležejících do zvláštní kategorie údajů – konkrétně údajů o zdravotním stavu – v rozsahu:

- anamnéza, popis aktuálních obtíží, prodělaná onemocnění, operace, hospitalizace;
- užívané léky, doplňky stravy, bylinné přípravky;
- alergie, intolerance, kontraindikace;
- výsledky screeningových měření prováděných v rámci poskytovaných služeb (např. Bicom, Bicom Body Check, EAV, termografie a obdobné nelékařské metody);
- záznamy z jednotlivých sezení, doporučení terapeuta, reakce klienta na předchozí sezení;
- fotografická dokumentace (pouze u metod, které ji vyžadují, a po samostatném souhlasu);
- kopie zpráv od lékařů a kopie laboratorních výsledků, které se pacient rozhodl poskytnout

k upřesnění svého zdravotního stavu.

**Účel zpracování:** poskytnutí služeb alternativní medicíny Správcem, vedení zdravotnické dokumentace klienta, vyhodnocení účinnosti služeb a komunikace v souvislosti s poskytovanou službou.

**Doba zpracování:** po dobu trvání tohoto souhlasu a dále 3 roky po posledním poskytnutém sezení (s ohledem na promlčecí lhůty a možnost právní obrany).

**Beru na vědomí, že:**

- souhlas uděluji svobodně, dobrovolně a vědomě, na základě úplných informací o zpracování;
- mám právo tento souhlas kdykoli odvolat, a to e-mailem na info@resonica.cz, písemně na adrese sídla Správce nebo osobně v provozovně;
- odvoláním souhlasu není dotčena zákonnost zpracování provedeného před jeho odvoláním;
- odvolání souhlasu může vést k tomu, že Správce dále nebude moci poskytovat služby, jejichž součástí je práce se zdravotními údaji;
- mám práva subjektu údajů podle čl. 15–22 GDPR (přístup, oprava, výmaz, omezení, přenositelnost, námitka) a právo podat stížnost u ÚOOÚ;
- podrobné informace o zpracování osobních údajů jsem našel/a v Zásadách zpracování osobních údajů Správce dostupných na [www.resonica.cz](http://www.resonica.cz).

Beru rovněž na vědomí, že služby Správce nejsou zdravotními službami ve smyslu zákona č. 372/2011 Sb. a nenahrazují lékařskou péči.

V ..... dne .....

Podpis klienta: .....

Za Správce převzal/a: .....

**Příloha č. 2 – Vzor žádosti subjektu údajů (přístup / oprava / výmaz / omezení / přenositelnost / námitka)**

**ŽÁDOST SUBJEKTU ÚDAJŮ DLE ČL. 15–22 NAŘÍZENÍ (EU) 2016/679 (GDPR)**

**Adresát:** Resonica s.r.o., IČO 236 41 771, se sídlem Topolská 952, Chrudim II, 537 05 Chrudim, e-mail info@resonica.cz

**Žadatel:**

- Jméno a příjmení: .....
- Datum narození / poslední číslo objednávky (pro ověření totožnosti): .....
- E-mail (pro doručení odpovědi): .....
- Adresa (pokud preferujete písemnou odpověď): .....

**Tímto uplatňuji své právo dle GDPR (zaškrtněte zvolené):**

- Právo na přístup k osobním údajům (čl. 15) – žádám potvrzení, zda Správce zpracovává mé osobní údaje, a v případě že ano, kopii těchto údajů a informace o zpracování;
- Právo na opravu (čl. 16) – žádám opravu/doplnění následujících údajů: .....
- Právo na výmaz (čl. 17) – žádám výmaz následujících údajů: .....
- Právo na omezení zpracování (čl. 18) z důvodu: .....
- Právo na přenositelnost (čl. 20) – žádám předání následujících údajů ve strojově čitelném formátu: .....
- Právo vznést námitku (čl. 21) proti zpracování: .....
- Odvolání souhlasu (čl. 7 odst. 3) k účelu: .....

Doplňující informace / upřesnění žádosti: .....

V ..... dne .....

Podpis žadatele: .....

*Poznámka: Správce vyřídí žádost bez zbytečného odkladu, nejpozději do 1 měsíce od jejího obdržení; tuto lhůtu lze prodloužit o 2 měsíce u složitých žádostí. Vyřízení je zpravidla bezplatné.*

**Příloha č. 3 – Seznam zpracovatelů a třetích zemí (vzor)**

Aktuální seznam je vedený interně a aktualizovaný při každé změně. Subjekt údajů má právo si na vyžádání seznam vyžádat. Vzorová struktura:

Zpracovatel	Účel	Třetí země / záruka	Smlouva čl. 28
Google Ireland Ltd. (Google Workspace)	e-mail, kalendář, cloudové dokumenty	USA – EU-US DPF + SCC	ANO (DPA Google)
Reservio s. r. o.	rezervační systém	EU (ČR)	ANO
Ecomail.cz, s.r.o.	rozesílka newsletteru	EU (ČR)	ANO
Fio banka, a.s.	banka	EU (ČR)	ANO
Externí účetní/daňový poradce	účetnictví, daně	EU (ČR)	ANO
Wedos Internet, a.s.	webhosting	EU (ČR)	ANO
Meta Platforms Ireland Ltd.	Meta Pixel, reklamy (po souhlasu)	USA – EU-US DPF + SCC	ANO (Meta DPA)

**Příloha č. 4 – Záznam o činnostech zpracování dle čl. 30 GDPR (vzor pro interní použití)**

Položka	Obsah
Správce	Resonica s.r.o., IČO 236 41 771, sídlo Topolská 952, Chrudim II, 537 05 Chrudim, e-mail info@resonica.cz
Pověřenec (DPO)	není jmenován; kontakt pro otázky ochrany údajů: info@resonica.cz
Název činnosti zpracování	např. „Vedení anamnézy a zdravotní dokumentace klientů“
Účel zpracování	poskytnutí služeb alternativní medicíny, vedení záznamu o sezeních
Právní základ	čl. 9 odst. 2 písm. a) GDPR – výslovný souhlas
Kategorie subjektů údajů	klienti centra alternativní medicíny
Kategorie údajů	identifikační, kontaktní, zvláštní kategorie (zdravotní)
Kategorie příjemců	účetní kancelář (jen platební údaje), IT poskytovatel (technický přístup), advokát (v případě sporu)
Předání do třetí země	cloudové úložiště – USA – záruka EU-US DPF + SCC
Plánované lhůty výmazu	doba souhlasu + 3 roky
Technická a organizační opatření	uzamykatelná kartotéka, šifrované disky, 2FA, antivirus, zálohy, NDA, školení, viz čl. 11 Zásad

Záznam je veden pro každou jednotlivou činnost zpracování (rezervace, anamnéza, fakturace, marketing, kamerový systém, cookies atd.). Záznamy jsou pravidelně přezkoumávány a aktualizovány.

— Konec dokumentu —