

SMLOUVA O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Uzavřená dle čl. 28 Nařízení (EU) 2016/679 (GDPR) a § 1746 odst. 2 občanského zákoníku

I. Smluvní strany

Správce (klient)

Obchodní firma: *[[doplní se]]*

Sídlo: *[[doplní se]]*

IČO / DIČ: *[[doplní se]]*

Jednající: *[[doplní se]]*

(dále jen „Správce“)

Zpracovatel (poskytovatel)

Interactive Marketing, s.r.o.

Sídlo: Komunardů 1091/36, 170 00 Praha 7

IČO: 248 14 075, DIČ: CZ24814075

Zapsána v OR MS Praha, oddíl C, vložka 176709

Jednající: Lukáš Pulda, jednatel

(dále jen „Zpracovatel“)

Správce a Zpracovatel dále společně též „Smluvní strany“.

II. Předmět a účel zpracování

1. Tato smlouva (dále jen „**Smlouva**“) upravuje práva a povinnosti Smluvních stran při zpracování osobních údajů Správce Zpracovatelem v souvislosti s **Hlavní smlouvou o poskytování SMS služeb**; s poskytováním služeb v rámci Všeobecných obchodních podmínek.
2. Zpracování probíhá výhradně za účelem poskytování služeb podle Hlavní smlouvy (dále jen „**Účel**“).
3. V případě rozporu má tato Smlouva přednost před Hlavní smlouvou.

III. Rozsah a kategorie osobních údajů

Kategorie subjektů	Kategorie údajů
Příjemci SMS	Telefonní číslo, text SMS (může obsahovat libovolné osobní údaje)
Kontaktní osoby Správce	Jméno, e-mail, telefon

1. Kategorie subjektů: Příjemci SMS
 - a. kategorie údajů: Telefonní číslo, text SMS (může obsahovat libovolné osobní údaje)
2. Kategorie subjektů: Kontaktní osoby Správce
 - a. Kategorie údajů: Jméno, e-mail, telefonní číslo
3. Zpracování dalších kategorií je možné pouze na základě písemného pokynu Správce.

IV. Doba zpracování

1. Zpracování trvá po dobu účinnosti Hlavní smlouvy a následně po dobu nutnou k plnění povinností dle čl. XIII.

V. Povinnosti Zpracovatele

1. Zajistí vhodná **technická a organizační opatření** dle čl. 32 GDPR, přičemž zohlední povahu, rozsah a rizika Služeb.
2. Udrží elektronický registr záznamů o zpracovatelských činnostech.
3. Bez zbytečného odkladu (nejpozději do 48 h) oznámí Správci porušení zabezpečení osobních údajů prostřednictvím kontaktní e-mailové adresy Správce.
4. Dbá, aby osoby oprávněné ke zpracování byly vázány mlčenlivostí.
5. **Sub-zpracovatelé:** Zpracovatel je oprávněn zapojit další zpracovatele; Správce může do 10 dní od notifikace vznést odůvodněnou námitku. **Pomocné služby** (telekomunikační, hosting, úklid, bezpečnost areálu) se za další zpracování nepovažují.
6. Přeshraniční přenosy do třetích zemí jsou přípustné, je-li to nutné k Účelu a příjemce splňuje podmínky GDPR.
7. Na vyžádání poskytne Správci nezbytnou součinnost při posouzení dopadu na ochranu údajů a při odpovědích subjektům údajů, nepřesáhne-li součinnost 2 hod/rok; další hodiny jsou zpoplatněny dle ceníku.

VI. Povinnosti Správce

1. Zajistí, aby osobní údaje byly získány a předány Zpracovateli zákonným způsobem a byla splněna informační povinnost vůči subjektům údajů.
2. Udělí Zpracovateli pokyny výhradně písemně (portál, e-mail); ústní pokyny musí být do 48 h potvrzeny písemně.
3. Odpovídá za správnost, aktuálnost a přiměřenost osobních údajů.

4. Udržuje aktuální kontaktní e-mail pro hlášení incidentů; nenahlášení změny zprošťuje Zpracovatele odpovědnosti za prodlení s notifikací.

VII. Bezpečnostní opatření

1. Zpracovatel uplatňuje minimálně: šifrování přenosu dat (TLS 1.2+), HA architekturou databází, dvoufaktorovou autentizaci administrátorů, geograficky oddělené zálohy.
2. Detailní popis je uveden v **Příloze 1 – Technická a organizační opatření**, kterou může Zpracovatel jednostranně aktualizovat, nebude-li tím snížena úroveň ochrany.

VIII. Audity

1. Správce je oprávněn provést audit ochrany osobních údajů nejvýše 1× ročně, s 30 denním předstihem, v pracovní době a bez narušení provozu.
2. Audit provede nezávislá osoba vázaná mlčenlivostí.
3. Náklady auditu nese Správce; Zpracovatel účtuje čas své součinnosti nad 1 h podle aktuálního hodinového sazebníku.

IX. Odpovědnost a odškodnění

1. Každá strana odpovídá za újmu způsobenou porušením této Smlouvy podle čl. 82 GDPR.
2. Limit odpovědnosti Zpracovatele vůči Správci za všechny nároky z této Smlouvy v každém kalendářním roce nepřekročí souhrn ročních poplatků uhrazených Správcem za Služby v daném roce.
3. Správce se zavazuje nahradit Zpracovateli veškeré újmy (včetně pokut ÚOOÚ, sankcí jiných orgánů veřejné moci či operátorů), které Zpracovatel uhradí v důsledku porušení povinností Správce, jeho pokynů nebo dat jím poskytnutých.
4. Vylučuje se náhrada ušlého zisku, reputační újmy, správních pokut uložených Správcem a jakýchkoli následných či nepřímých škod.
5. Zpracovatel udržuje pojištění odpovědnosti za škodu způsobenou zpracováním osobních údajů s limitem plnění minimálně odpovídajícím limitu odpovědnosti dle odst. 2. Správce se zavazuje uplatnit své nároky na náhradu újmy primárně z tohoto pojištění. Po vyčerpání pojistného limitu může Správce uplatnit zbývající část svých nároků vůči Zpracovateli pouze do výše limitu stanoveného v odst. 2.

X. Ukončení zpracování

1. Po zániku Hlavní smlouvy nebo na pokyn Správce provede Zpracovatel **bezplatný výmaz** či předání osobních údajů do 30 dnů, pokud právní předpis nestanoví jinak.
2. Správce může zvolit mezi: a) trvalým výmazem, nebo b) exportem ve formátu CSV a následným výmazem.

XI. Doba trvání, změny, ukončení

1. Tato Smlouva se uzavírá na dobu neurčitou a pozbývá platnosti uplynutím 3 let od zániku Hlavní smlouvy.
2. Každá strana může Smlouvu vypovědět s výpovědní lhůtou 30 dnů; výpověď musí být písemná.
3. Zpracovatel může odstoupit s okamžitou účinností, poruší-li Správce podstatně své povinnosti (např. nezaplatí-li služby déle než 30 dnů).

XII. Závěrečná ustanovení

1. Smluvní strany vylučují aplikaci § 1740 odst. 3, § 558 odst. 2, § 1765 odst. 2 a § 1729 odst. 2 OZ.
2. Veškeré změny lze činit pouze písemnými, očíslovanými dodatky.
3. Tato Smlouva je vyhotovena ve dvou stejnopisech s platností originálu.
4. Účinnost nabývá dnem podpisu oběma Smluvními stranami.

V Praze dne

Interactive Marketing, s.r.o.

Lukáš Pulda, jednatel

V Praze dne

[[Správce]]

[[jméno, funkce]]

Příloha 1 – Technická a organizační opatření

Níže uvedená opatření Zpracovatel průběžně aktualizuje v souladu s čl. VII odst. 2 Smlouvy; změny, které by mohly snížit úroveň ochrany, oznámí Správci nejméně 14 dnů před účinností.

1. Řízení přístupu

- Jedinečné administrátorské účty; minimální délka hesla 12 znaků a povinné MFA pro administrátory.
- Role-based access control (RBAC); přístup podle zásady *need-to-know*.

2. Fyzická bezpečnost

- Servery umístěny v datacentrech certifikovaných jako TIER III+
- Přístup na čipové karty, biometrické turnikety, 24/7 CCTV, evidence vstupů.
- Záložní zdroj energie.

3. Šifrování

- Přenos: TLS 1.2+ (směrem k operátorům TLS/IPsec).
- Uložení: AES-256 na úrovni databázových a souborových systémů; managed správa klíčů.

4. Síťová bezpečnost

- Vícevrstvé firewally, ochrana DDoS.
- IDS/IPS a Managed Web Application Firewall.
- Oddělené testovací a produkční prostředí.

5. Zálohování a obnova

- Šifrované denní zálohy na geograficky oddělené lokalitě; retenční doba 30 dnů.
- Obnovení testováno minimálně 1× za rok.

6. Logování a monitoring

- Centralizovaný log; detekce anomálií v reálném čase.
- Retence logů 180 dnů; přístup pouze provozní tým.
- Kritické události (privilege escalation, failed MFA) – alert do 5 min.

7. Management zranitelností

- Automatizovaný vulnerability scan; kritické zranitelnosti (CVSS $\geq$ 9) patch do 72 h.

8. Patch a change management

- Standardní okno údržby mezi 03:00–05:00 CET. Plánované výpadky mimo okno údržby oznámeny nejpozději 72 h předem.
- Každá změna prochází risk assessmentem s možností rollbacku.

9. Ochrana osobních údajů v návrhu

- Pseudonymizace analyticko-provozních dat (hash MSISDN).
- Data minimization: trigger automaticky mažou záznamy starší 12 měsíců, pokud není domluveno jinak.

10. Školení a povědomí

- Povinné školení GDPR a bezpečnosti pro zaměstnance;
- Všichni zaměstnanci podepisují NDA

11. Incident Response

- Postup ve fázích: identifikace < 4 h, oprava < 8 h, obnova, postmortem.

12. Management dodavatelů

- Hodnocení sub-zpracovatelů dle ISO 27001 nebo SOC 2 nebo rovnocenného standardu.

13. Kontinuita podnikání

- Redundantní konektivita pro zajištění služeb do všech destinací.
- Fallback na mezinárodní routing.