SMLOUVA O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

uzavřená dle čl. 28 Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR) a § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník

I. Smluvní strany

Smluvní strany jsou definovány Všeobecnými smluvními podmínkami

II. Úvodní ustanovení a předmět smlouvy

1) Zákazník je v postavení správce osobních údajů (dále jen „Osobní údaje“) ve vztahu ke všem osobním údajům, které v souvislosti s užíváním služeb Provozovatele sám ukládá, zpracovává, přenáší nebo jinak spravuje prostřednictvím svého webhostingu, e-mailových schránek, virtuálního serveru (VPS) a/nebo cloudových služeb (dále jen „Služby“).

2) Provozovatel poskytuje Služby jako technickou infrastrukturu a nemá žádnou povinnost ani oprávnění seznamovat se s obsahem dat, která Zákazník prostřednictvím Služeb ukládá, přijímá nebo odesílá. Rozsah role Provozovatele coby zpracovatele je pro jednotlivé Služby odlišný a je upraven v přílohách této Smlouvy (Příloha 1 – Webhosting, Příloha 2 – E-mailové služby, Příloha 3 – VPS, Příloha 4 – Cloudové služby).

3) Účelem této Smlouvy je vymezit vzájemná práva a povinnosti Stran při zpracování osobních údajů v souladu s čl. 28 GDPR, a to v rozsahu, který odpovídá technické povaze poskytovaných Služeb a reálným možnostem Provozovatele.

III. Definice

1) „Osobními údaji“ se rozumí veškeré informace ve smyslu čl. 4 odst. 1 GDPR, které Zákazník ukládá, zpracovává nebo přenáší prostřednictvím Služeb.

2) „Zpracováním“ se rozumí zpracování ve smyslu čl. 4 odst. 2 GDPR.

3) „Obsahem“ se rozumí data uložená, přenášená či zpracovávaná Zákazníkem prostřednictvím Služby (soubory, databáze, e-mailové zprávy), jejichž věcný obsah, strukturu ani povahu Provozovatel nezná a aktivně nezjišťuje.

4) „Infrastrukturní úrovní“ se rozumí technické a organizační zabezpečení platformy, na které jsou Služby provozovány (fyzická bezpečnost datacentra, síťová bezpečnost, řízení přístupu zaměstnanců, zálohování na úrovni systému), na rozdíl od zabezpečení nebo úprav samotného Obsahu.

5) „Smlouvou o službách“ se rozumí příslušné smluvní podmínky a další dokumenty umístěné na https://www.forpsi.com/agreements/ , a které zákazník odsouhlasil při objednávce/prodloužení služby.

IV. Předmět, povaha, účel a doba zpracování

1) Konkrétní předmět, povaha, účel, doba trvání zpracování, kategorie subjektů údajů a kategorie osobních údajů jsou pro jednotlivé Služby specifikovány v Přílohách 1–4. Zákazník bere na vědomí, že Provozovatel nemá možnost tyto kategorie sám určit ani ověřit, neboť neprovádí obsahovou kontrolu dat.

2) Zákazník bere na vědomí, že Provozovatel nemůže provádět opatření vyžadující znalost Obsahu, zejména: klasifikaci, pseudonymizaci, anonymizaci nebo šifrování konkrétních osobních údajů v rámci Obsahu, jejich selektivní mazání či opravu. Odpovědnost za tato opatření na aplikační/obsahové úrovni nese Zákazník.

3) Zpracování trvá po dobu účinnosti Smlouvy o službách pro danou Službu a končí jejím ukončením.

4) Doloženými pokyny Zákazníka ve smyslu čl. 28 odst. 3 písm. a) GDPR se rozumí Smlouva o službách, tato Smlouva o zpracování a konfigurace Služby provedená Zákazníkem v uživatelském rozhraní / administraci Provozovatel e. Jiné pokyny je Provozovatel oprávněn, nikoli povinen akceptovat

V. Povinnosti Provozovatele jako zpracovatele

Provozovatel se v rozsahu, v jakém je dle příslušné Přílohy zpracovatelem, zavazuje:

1) Zpracovávat osobní údaje pouze na základě doložených pokynů Zákazníka dle čl. 3.4 a pouze za účelem poskytování Služby; nepoužívat Obsah k žádnému jinému účelu, zejména jej neanalyzovat, nekopírovat mimo rámec nezbytný pro provoz a zálohování Služby ani jej nezpřístupňovat třetím osobám mimo případy dle této Smlouvy nebo zákona.
2) Zajistit, aby se osoby oprávněné zpracovávat osobní údaje (zaměstnanci, spolupracovníci Provozovatel e) zavázaly k mlčenlivosti, případně aby se na ně vztahovala zákonná povinnost mlčenlivosti.
3) Přijmout přiměřená technická a organizační opatření dle čl. 32 GDPR na Infrastrukturní úrovni, zejména:
    a. fyzické zabezpečení datacentra a řízení přístupu do něj;
    b. síťová bezpečnost, firewall, ochrana proti neoprávněnému přístupu zvenčí;
    c. řízení přístupových oprávnění zaměstnanců Provozovatele k infrastruktuře;
    d. pravidelné zálohování na úrovni systému/platformy dle standardních parametrů dané Služby;
    e. evidence a monitoring bezpečnostních incidentů na úrovni infrastruktury.
4) V mezích technických možností popsaných v Přílohách poskytnout Zákazníkovi součinnost při plnění jeho povinnosti reagovat na žádosti subjektů údajů dle kapitoly III GDPR a při plnění povinností dle čl. 32–36 GDPR. Strany se dohodly, že tato součinnost je omezena na úkony proveditelné na Infrastrukturní úrovni (např. úplné smazání účtu, schránky, poskytnutí exportu celého Obsahu či znemožnění přístupu) a nezahrnuje identifikaci, vyhledání ani selektivní úpravu konkrétních osobních údajů v rámci Obsahu, kterou může provést pouze Zákazník.
5) Oznámit Zákazníkovi bez zbytečného odkladu poté, co se o něm dozví, jakékoli porušení zabezpečení osobních údajů, které Provozovatel zjistí na Infrastrukturní úrovni (např. neoprávněný přístup k systémům Provozovatel e). Strany berou na vědomí, že Provozovatel nemá technickou možnost odhalit porušení zabezpečení, k němuž dojde výlučně na úrovni Obsahu nebo aplikace Zákazníka (např. únik dat způsobený zranitelností aplikace provozované Zákazníkem, kompromitace přístupových údajů Zákazníka apod.), a za tato porušení Provozovatel neodpovídá.
6) Po ukončení poskytování příslušné Služby veškerá data vymazat; standardní lhůta pro výmaz po ukončení je 60 dní od ukončení Služby plus 6 dní pro výmaz ze záloh.
7) Umožnit Zákazníkovi a jím pověřenému auditorovi provedení auditu či inspekce nezbytné k doložení souladu s povinnostmi dle čl. 28 GDPR, a to v přiměřeném rozsahu, s předstihem alespoň 30 dní, mimo běžnou provozní dobu a maximálně 1x ročně, nejde-li o šetření podnětu dozorového úřadu; náklady auditu nese Zákazník. Provozovatel může tuto povinnost alternativně plnit předložením aktuálního nezávislého auditu/certifikace.

VI. Povinnosti a odpovědnost Zákazníka jako správce

1) Zákazník odpovídá za to, že veškeré zpracování osobních údajů prostřednictvím Služeb má právní základ dle čl. 6, resp. čl. 9 GDPR, a že Provozovateli poskytuje pouze takové pokyny, jejichž plnění je v souladu s GDPR.
2) Zákazník bere na vědomí a souhlasí s tím, že Provozovatel neprovádí a není povinen provádět obsahovou kontrolu, klasifikaci ani filtrování dat ukládaných či přenášených prostřednictvím Služeb, a že za určení, jaké osobní údaje a v jakém rozsahu jsou prostřednictvím Služeb zpracovávány, odpovídá výlučně Zákazník.
3) Zákazník je povinen na úrovni svého Obsahu a vlastní aplikační logiky sám zajistit taková opatření (šifrování, pseudonymizaci, řízení přístupu, zálohování obsahu, mazání konkrétních záznamů apod.), která odpovídají rizikům spojeným se zpracováním jím ukládaných osobních údajů.
4) Zákazník je povinen sám vyřizovat žádosti subjektů údajů v rozsahu, který vyžaduje znalost Obsahu, a k tomu využívat součinnost Provozovatele dle čl. 4.4 pouze v rozsahu tam popsaném.

VII. Vztah k VPS, cloudovým a dalším neřízeným službám

1) Strany výslovně potvrzují, že u Služeb specifikovaných v Přílohách 3 – VPS a 4 – Cloudové služby Provozovatel nemá přístup k datům uloženým, zpracovávaným nebo přenášeným Zákazníkem v rámci virtuálního serveru či virtuální infrastruktury, s výjimkou situací uvedených v Příloze 3 a 4
2) S ohledem na uvedené Strany shodně konstatují, že ve vztahu k obsahu VPS Provozovatel neprovádí zpracování osobních údajů ve smyslu čl. 4 odst. 2 GDPR a nevystupuje jako zpracovatel; ustanovení této Smlouvy se na tuto Službu vztahují pouze přiměřeně, v rozsahu Přílohy 3 a 4, a to zejména jako deklarace rozsahu přístupu a bezpečnostních opatření na Infrastrukturní úrovni.

VIII. Mezinárodní předávání údajů

V souvislosti se sub-zpracovateli nedochází k předávání osobních údajů mimo Evropský hospodářský prostor. Informace o sub-zpracovatelích a umístění datacenter jsou uvedeny v Příloze 5.

IX. Doba trvání a ukončení

1) Tato Smlouva o zpracování je uzavřena na dobu trvání Smlouvy o službách a řídí se stejnou dobou trvání a výpovědními důvody jako Smlouva o službách, není-li dále uvedeno jinak.
2) Ukončením této Smlouvy nejsou dotčeny povinnosti Provozovatele dle čl. 4.6 (výmaz dat) a povinnost mlčenlivosti.

X. Závěrečná ustanovení

1) V případě rozporu mezi touto Smlouvou o zpracování a Smlouvou o službách má ve věcech ochrany osobních údajů přednost tato Smlouva o zpracování.
2) Tato Smlouva se řídí právním řádem České republiky. Případné spory budou Strany řešit přednostně smírně.
3) Tato Smlouva nabývá účinnosti okamžikem akceptace Zákazníkem a je nedílnou součástí Smlouvy o službách.

Příloha 1 - Webhosting

Popis Služby	Poskytnutí prostoru na serveru pro provoz webových stránek/aplikací Zákazníka, včetně databází.
Rozsah přístupu Provozovatele	Provozovatel má technickou možnost přístupu k datům uloženým na hostingu (správa serveru, technická podpora, zálohování), ale obsah aktivně neprohlíží, s výjimkou nezbytného rozsahu při řešení technického problému na žádost Zákazníka nebo za účelem odvrácení bezprostředního ohrožení provozu.
Povaha a účel zpracování	Uložení, přenos a zálohování dat na úrovni souborového systému a databáze za účelem provozu webu/aplikace Zákazníka.
Kategorie subjektů údajů	Určuje výlučně Zákazník dle povahy provozované aplikace (typicky např. návštěvníci webu, zákazníci e-shopu apod.); Provozovateli nejsou známy.
Kategorie osobních údajů	Určuje výlučně Zákazník; Provozovateli nejsou známy, jelikož neprovádí obsahovou kontrolu.
Doba zpracování	Po dobu trvání Služby webhostingu.
Technická opatření Provozovatele	Zabezpečení serveru a sítě, řízení přístupu, pravidelné zálohování na úrovni systému dle parametrů tarifu, šifrovaný přenos (TLS/SSL) je-li součástí Služby.

Příloha 2 - E-mailové služby

Popis Služby	Provoz e-mailových schránek a přenos e-mailových zpráv Zákazníka (příjem, odesílání, ukládání).
Rozsah přístupu Provozovatele	Provozovatel má technickou možnost přístupu k obsahu e-mailových schránek (správa serveru, technická podpora), ale obsah aktivně neprohlíží, s výjimkou automatizovaného zpracování za účelem ochrany proti spamu/malwaru a s výjimkou nezbytného rozsahu při řešení technického problému na žádost Zákazníka.
Povaha a účel zpracování	Ukládání, přenos a doručování e-mailových zpráv a příloh.
Kategorie subjektů údajů	Určuje výlučně Zákazník (odesílatelé a příjemci e-mailové komunikace); Provozovateli nejsou známy.
Kategorie osobních údajů	Určuje výlučně Zákazník; obsah zpráv a příloh může zahrnovat jakékoli osobní údaje dle rozhodnutí uživatelů schránky.
Doba zpracování	Po dobu trvání e-mailové Služby, resp. do vymazání zprávy uživatelem.
Technická opatření Provozovatele	Zabezpečení serveru a sítě, šifrovaný přenos (TLS), antispamová a antivirová kontrola.

Příloha 3 – VPS

Popis Služby	Poskytnutí virtuálního serveru (VPS) do plné správy Zákazníka, včetně operačního systému a veškerých aplikací a dat, které si Zákazník na VPS sám nainstaluje a spravuje.
Rozsah přístupu Provozovatele	Provozovatel nemá přístup k operačnímu systému, aplikacím ani datům uvnitř VPS. Provozovatel spravuje pouze virtualizační a síťovou infrastrukturu (hypervisor, síť, napájení, fyzický hardware).
Právní kvalifikace	Ve vztahu k obsahu VPS Provozovatel není zpracovatelem osobních údajů ve smyslu čl. 4 odst. 2 a čl. 28 GDPR – viz čl. 6 této Smlouvy.
Kategorie subjektů a osobních údajů	Neurčuje se – Provozovatel nemá přístup ani vědomost o obsahu.
Odpovědnost za zabezpečení obsahu	Výlučně Zákazník (aktualizace operačního systému a aplikací, konfigurace firewallu na úrovni VPS, zálohování obsahu, šifrování dat, správa přístupových údajů).
Technická opatření Provozovatele	Fyzické zabezpečení datacentra, zabezpečení hypervisoru a síťové infrastruktury, oddělení jednotlivých VPS instancí, dostupnost dle SLA, pokud je uzavřeno. Zálohování obsahu VPS zajišťuje Zákazník, není-li v tarifu výslovně sjednána služba zálohování.
Výjimečný přístup Provozovatele	Provozovatel je oprávněn přistoupit k VPS pouze na výslovnou žádost Zákazníka v rámci placené technické podpory.

Příloha 4 – Cloudové služby

Popis Služby	Poskytnutí virtuální infrastruktury a dalších cloudových služeb (IaaS, PaaS)) do plné správy Zákazníka, včetně operačního systému, konfigurace virtuální infrastruktury a veškerých aplikací a dat, které si Zákazník do virtuální infrastruktury sám nainstaluje a spravuje.
Rozsah přístupu Provozovatele	Provozovatel nemá přístup k operačnímu systému, aplikacím ani datům uvnitř virtuální infrastruktury. Provozovatel spravuje pouze virtualizační a síťovou infrastrukturu (hypervisor, síť, napájení, fyzický hardware).
Právní kvalifikace	Ve vztahu k obsahu VPS Provozovatel není zpracovatelem osobních údajů ve smyslu čl. 4 odst. 2 a čl. 28 GDPR – viz čl. 6 této Smlouvy.
Kategorie subjektů a osobních údajů	Neurčuje se – Provozovatel nemá přístup ani vědomost o obsahu.
Odpovědnost za zabezpečení obsahu	Výlučně Zákazník (aktualizace operačního systému a aplikací, konfigurace firewallu na úrovni virtuální infrastruktury, zálohování obsahu, šifrování dat, správa přístupových údajů).
Technická opatření Provozovatele	Fyzické zabezpečení datacentra, zabezpečení hypervisoru a síťové infrastruktury, oddělení jednotlivých instancí virtuální infrastruktury, dostupnost dle SLA, pokud je uzavřeno. Zálohování obsahu virtuální infrastruktury zajišťuje Zákazník, není-li v tarifu výslovně sjednána služba zálohování.
Výjimečný přístup Provozovatele	Provozovatel je oprávněn přistoupit k virtuální infrastruktuře pouze na výslovnou žádost Zákazníka v rámci placené technické podpory.

Příloha 5 – Seznam sub-zpracovatelů a datacenter

Sub-zpracovatelé	• Aruba S.p.A., Via San Clemente 53 - 24036 Ponte San Pietro, Itálie
Datacentra	• DC IT1 Arezzo, Itálie • DC IT2 Arezzo, Itálie • DC IT3 Ponte San Pietro, Itálie • DC IT4 Řím, Itálie • DC CZ1 Praha, Česká republika • DC CZ2 Ktiš, Česká republika • DC FR1 Paříž, Francie • DC DE1 Frankfurt, Německo • DC UK1 Londýn, Velká Británie • DC PL1 Varšava, Polsko