

ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV

Vzorová dokumentácia pre web / portfólio a zmluvné vzťahy s klientmi

1. Prevádzkovateľ: [meno, IČO, adresa, e-mail]. Zodpovedná osoba: [určená / neurčená] — povinnosť určenia posudzujte podľa § 44 (18/2018 Z. z.).

2. Aké údaje a na akom právnom základe: Každý účel spracúvania musí mať právny základ podľa § 13 (18/2018 Z. z.):

Účel	Kategórie údajov	Právny základ	Doba uchovávania
Kontaktný formulár, dopyt	meno, e-mail, tel., obsah správy	predzmluvné vzťahy / oprávnený záujem	1 rok od poslednej komunikácie
Uzavretie a plnenie zmluvy	identifikačné, fakturačné, kontaktné	plnenie zmluvy	trvanie zmluvy
Účtovníctvo a daňové doklady	fakturačné údaje	zákonná povinnosť	10 rokov
Newsletter	e-mail, meno	súhlas	do odvolania súhlasu
Analytika a marketingové cookies	ID zariadenia, IP, správanie	súhlas	podľa cookie lišty
Uplatnenie / obrana právnych nárokov	podľa prípadu	oprávnený záujem	premlčacie lehoty

3. Súhlas: Súhlas musí byť slobodný, konkrétny, informovaný a preukázateľný a je kedykoľvek odvolateľný rovnakým spôsobom, ako bol udelený (§ 14 zákona č. 18/2018 Z. z.). Pri službách informačnej spoločnosti ponúkaných dieťaťu platia osobitné podmienky podľa § 15 (18/2018 Z. z.).

4. Prijemcovia: hosting [___], e-mailing [___], analytika [___], účtovník [___], platobná brána [___]. Prenos do tretej krajiny: [nie / áno — na základe štandardných zmluvných doložiek] (§ 48 zákona č. 18/2018 Z. z.).

5. Práva dotknutej osoby: prístup, oprava, výmaz, obmedzenie spracúvania, prenosnosť, namietanie (najmä proti priamemu marketingu), odvolanie súhlasu, právo podať návrh na začatie konania na Úrad na ochranu osobných údajov SR (Hraničná 12, Bratislava). Uplatnenie: [e-mail]. Odpovedáme do 1 mesiaca.

6. Bezpečnosť: prijímame primerané technické a organizačné opatrenia (šifrovanie prenosu TLS, riadenie prístupov, MFA, šifrované zálohy, logovanie, pravidelné aktualizácie) podľa § 39 (18/2018 Z. z.).

7. Automatizované rozhodovanie a profilovanie: [nevykonáva sa / opis].

COOKIES A COOKIE LIŠTA

Kto ukladá alebo získava prístup k informáciám v koncovom zariadení užívateľa, je na to oprávnený iba s preukázateľným súhlasom užívateľa. Výnimkou je technické uloženie alebo prístup, ktorých jediným účelom je prenos správy, alebo ktoré sú bezpodmienečne potrebné na poskytnutie služby výslovne požadovanej užívateľom (§ 109 zákona č. 452/2021 Z. z.).

ZMLUVA O SPRACÚVANÍ OSOBNÝCH ÚDAJOV

(Sprostredkovateľská zmluva podľa § 34 zákona č. 18/2018 Z. z.)

Zmluvné strany: Prevádzkovateľ (Klient) — Sprostredkovateľ (Poskytovateľ).

Preambula: Prevádzkovateľ môže poveriť len sprostredkovateľa poskytujúceho dostatočné záruky primeraných technických a organizačných opatrení; súhlas dotknutej osoby sa na poverenie nevyžaduje (§ 34 zákona č. 18/2018 Z. z.).

Čl. I – Predmet, povaha, účel a doba spracúvania

- **Predmet:** [správa a údržba webovej aplikácie, hosting, technická podpora, migrácia dát].
- **Povaha a účel:** technická prevádzka a údržba informačného systému Prevádzkovateľa.
- **Doba:** počas trvania hlavnej zmluvy.
- **Kategórie dotknutých osôb:** zákazníci, návštevníci webu, registrovaní používatelia, zamestnanci Prevádzkovateľa.
- **Rozsah údajov:** meno, priezvisko, e-mail, telefón, adresa, objednávky, IP adresa, logy [osobitné kategórie: nie].

Čl. II – Povinnosti Sprostredkovateľa

Sprostredkovateľ sa zaväzuje dodržiavať nasledujúce zákonné minimálne povinnosti:

- **a)** spracúvať údaje len na základe písomných pokynov Prevádzkovateľa vrátane prenosu do tretej krajiny;
- **b)** zabezpečiť mlčanlivosť oprávnených osôb;
- **c)** prijať bezpečnostné opatrenia podľa § 39 (18/2018 Z. z.);
- **d)** dodržiavať podmienky zapojenia ďalšieho sprostredkovateľa — nesmie ho poveriť bez predchádzajúceho osobitného alebo všeobecného písomného súhlasu a je povinný vopred informovať o zmenách (§ 34);
- **e)** poskytovať súčinnosť pri vybavovaní žiadostí dotknutých osôb;
- **f)** poskytovať súčinnosť pri bezpečnosti, oznamovaní porušení ochrany údajov a posúdení vplyvu (DPIA);
- **g)** po skončení spracúvania údaje podľa voľby Prevádzkovateľa vymazať alebo vrátiť a vymazať existujúce kópie, ak právo neukladá ich uchovanie;
- **h)** poskytnúť Prevádzkovateľovi informácie potrebné na preukázanie splnenia povinností a umožniť audit;
- **i)** informovať Prevádzkovateľa, ak sa pokyn podľa jeho názoru prieči zákonu.

Čl. III – Schválení ďalší sprostredkovatelia (Príloha č. 1)

hosting [___], CDN [___], e-mailing [___], monitoring [___], zálohovanie [___]. Zmenu oznámi Sprostredkovateľ [30] dní vopred; Prevádzkovateľ môže namietiť.

Čl. IV – Bezpečnostné opatrenia (Príloha č. 2)

Šifrovanie prenosu a záloh, oddelené dev/prod prostredia, zákaz produkčných dát v testovacom prostredí (alebo pseudonymizácia), riadenie prístupov a MFA, logovanie, pravidelné aktualizácie a patch management, incident response.

Čl. V – Porušenie ochrany údajov

Sprostredkovateľ oznámi Prevádzkovateľovi porušenie bez zbytočného odkladu, najneskôr do 24 hodín od zistenia, s opisom, rozsahom a prijatými opatreniami.

Čl. VI – Zodpovednosť za škodu, sankcie a vysporiadanie nárokov

6.1 Zásada zodpovednosti a preukázateľnosť: Každá zmluvná strana zodpovedá za dodržiavanie právnych predpisov o ochrane osobných údajov v rozsahu svojich povinností a je povinná súlad vedieť preukázať (§ 12 zákona č. 18/2018 Z. z.). Sprostredkovateľ vedie a na výzvu predloží najmä: zoznam oprávnených osôb, záväzky mlčanlivosti, opis bezpečnostných opatrení, evidenciu incidentov, evidenciu pokynov Prevádzkovateľa a zoznam ďalších sprostredkovateľov.

6.2 Zodpovednosť voči dotknutej osobe: Zákonný rámec, ktorý strany nemôžu zmluvne vylúčiť:

- **6.2.1** Osoba, ktorej vznikla majetková alebo nemajetková ujma v dôsledku porušenia predpisov o ochrane osobných údajov, má právo na náhradu škody od Prevádzkovateľa alebo od Sprostredkovateľa (§ 38).
- **6.2.2** Sprostredkovateľ zodpovedá dotknutej osobe len vtedy, ak nesplnil povinnosti, ktoré zákon ukladá priamo sprostredkovateľovi (§ 34 až 37, § 39, § 40 ods. 3, § 44, § 45, § 51 ods. 3), alebo ak konal nad rámec alebo v rozpore s pokynmi Prevádzkovateľa, ktoré boli v súlade so zákonom (§ 38).
- **6.2.3** Zodpovednosti sa strana zbaví, ak preukáže, že vznik škody nezavinila (§ 38).
- **6.2.4** Ak sa na tom istom spracúvaní zúčastnili obe strany, zodpovedajú dotknutej osobe spoločne a nerozdielne; strana, ktorá uhradila náhradu v plnej výške, má právo na regres voči druhej strane v rozsahu jej podielu zodpovednosti (§ 38).
- **6.2.5** Strany si na účely regresu podľa bodu 6.2.4 dojednávajú, že podiel zodpovednosti sa určí podľa toho, ktorá strana porušila svoju povinnosť, a ak porušili obe, podľa miery ich zavinenia; v pochybnostiach v pomere [50 : 50].

6.3 Vnútročné vysporiadanie medzi stranami: Regres a indemnita medzi zmluvnými stranami:

- **6.3.1** Ak Prevádzkovateľ uhradí dotknutej osobe náhradu škody, zaplatí pokutu alebo vynaloží účelné náklady (právne zastúpenie, forenzná analýza, notifikácia dotknutých osôb, kredit monitoring), ktoré vznikli výlučne v dôsledku porušenia povinností Sprostredkovateľa podľa tejto zmluvy alebo zákona, je Sprostredkovateľ povinný ich Prevádzkovateľovi nahradiť do [30] dní od doručenia vyúčtovania s dokladmi.
- **6.3.2** Opačná indemnita (ochrana programátora/poskytovateľa): Ak Sprostredkovateľ spracúval osobné údaje v súlade s doloženými pokynmi Prevádzkovateľa a ujma, pokuta alebo náklad vznikli z toho, že pokyn, právny základ, informačná povinnosť, súhlas, doba uchovávanía alebo samotný účel spracúvania určený Prevádzkovateľom boli v rozpore so zákonom, nahradí ich Prevádzkovateľ Sprostredkovateľovi v plnom rozsahu, vrátane nákladov právneho zastúpenia.
- **6.3.3** Sprostredkovateľ nezodpovedá za obsah, správnosť, aktuálnosť a zákonnosť získania osobných údajov, ktoré mu Prevádzkovateľ odovzdal alebo ktoré Prevádzkovateľ vložil do systému.
- **6.3.4** Podmienkou uplatnenia indemnity je, že dotknutá strana bez zbytočného odkladu, najneskôr do [5] pracovných dní informuje druhú stranu o uplatnenom nároku, umožní jej vyjadriť sa k obrane a bez jej súhlasu neuzavrie zmier ani neuzná nárok.

6.4 Zodpovednosť za ďalších sprostredkovateľov: Pravidlá pre subdodávateľov:

- **6.4.1** Ak Sprostredkovateľ zapojí ďalšieho sprostredkovateľa, je povinný uložiť mu rovnaké povinnosti, aké má sám podľa tejto zmluvy, a zodpovedá Prevádzkovateľovi za jeho konanie, akoby konal sám.
- **6.4.2** Zapojenie ďalšieho sprostredkovateľa bez predchádzajúceho osobitného alebo všeobecného písomného súhlasu Prevádzkovateľa, resp. bez predchádzajúceho informovania o zmene pri všeobecnom súhlase, je podstatným porušením tejto zmluvy (§ 34).
- **6.4.3** Zodpovednosť za osobu, ktorej strana zverila plnenie svojej povinnosti, sa spravuje § 375 Obchodného zákonníka — Sprostredkovateľ sa jej nezbaví len tým, že plnenie zveril tretej osobe.

6.5 Pokuty uložené dozorným orgánom: Pravidlá pre verejnoprávne sankcie:

- **6.5.1** Strany berú na vedomie, že Úrad na ochranu osobných údajov SR môže uložiť pokutu do 10 000 000 € alebo do 2 % celkového svetového ročného obratu za porušenie povinností sprostredkovateľa a bezpečnostných povinností (§ 34, § 35, § 37, § 39 až 45, § 79) a do 20 000 000 € alebo do 4 % obratu za porušenie základných zásad spracúvania, podmienok súhlasu a práv dotknutých osôb (§ 104).
- **6.5.2** Dôležité obmedzenie: Verejnoprávnu sankciu nemožno zmluvne „preniesť“ na inú osobu — pokutu vždy platí subjekt, ktorému bola uložená. Dojednanie podľa bodu 6.3 preto pôsobí len ako súkromnoprávny regresný nárok na náhradu škody medzi stranami, nie ako zmena adresáta sankcie.
- **6.5.3** Uhradená pokuta sa považuje za škodu podľa bodu 6.3 len v rozsahu, v akom bola uložená za porušenie pripísateľné druhej strane a v akom sa poškodená strana proti nej primerane bránila (podanie odvolania/rozkladu, ak bolo dôvodné).

6.6 Bezpečnostné opatrenia ako meradlo zodpovednosti: Aplikácia bezpečnostných štandardov:

- **6.6.1** Sprostredkovateľ je povinný prijať primerané technické a organizačné opatrenia so zreteľom na najnovšie poznatky, náklady, povahu, rozsah, kontext a účel spracúvania a na riziká; opatrenia môžu zahŕňať najmä pseudonymizáciu a šifrovanie, zabezpečenie dôvernosti, integrity, dostupnosti a odolnosti systémov, proces obnovy dostupnosti údajov po incidente a proces pravidelného testovania účinnosti opatrení (§ 39).
- **6.6.2** Sprostredkovateľ zabezpečí, aby fyzická osoba konajúca za neho, ktorá má prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov Prevádzkovateľa (§ 39).
- **6.6.3** Konkrétny katalóg opatrení je v Prílohe č. 2. Nesplnenie opatrení uvedených v Prílohe č. 2 sa považuje za porušenie povinnosti podľa bodu 6.2.2.

6.7 Bezpečnostný incident – lehoty a rozdelenie úloh: Postupy pri zistení incidentu:

- **6.7.1** Sprostredkovateľ je povinný oznámiť porušenie ochrany osobných údajov Prevádzkovateľovi bez zbytočného odkladu po tom, ako sa o ňom dozvedel (§ 40); strany si túto lehotu spresňujú na najneskôr 24 hodín, aby Prevádzkovateľ stihol vlastnú 72-hodinovú lehotu voči úradu.
- **6.7.2** Oznámenie obsahuje aspoň: opis povahy porušenia vrátane kategórií a približného počtu dotknutých osôb a záznamov, kontaktné miesto, opis pravdepodobných následkov a opis prijatých alebo navrhovaných nápravných opatrení (§ 40); ak časť informácií nie je známa, doplní ich bezodkladne.
- **6.7.3** Oznámenie úradu do 72 hodín a prípadné oznámenie dotknutým osobám pri vysokom riziku vykonáva Prevádzkovateľ (§ 40, § 41); Sprostredkovateľ poskytne všetku potrebnú súčinnosť, logy a forenzné podklady bezodplatne, ak incident zavinil.
- **6.7.4** Strany berú na vedomie, že oznámenie dotknutej osobe sa nevyžaduje najmä vtedy, ak boli údaje šifrované alebo inak nečitateľné pre neoprávnené osoby (§ 41) — preto je šifrovanie v pokoji aj pri prenose povinným opatrením podľa Prílohy č. 2.

6.8 Limitácia náhrady škody medzi stranami: Dojednania o rozsahu náhrady škody:

- **6.8.1** Strany berú na vedomie, že nároku na náhradu škody sa nemožno vzdať pred porušením povinnosti (§ 386 Obchodného zákonníka); akékoľvek „vylúčenie zodpovednosti“ by bolo neplatné.
- **6.8.2** Strany preto zhodne vyhlasujú, že s prihliadnutím na povahu a hodnotu plnenia je pri porušení povinností Sprostredkovateľa predvídateľná škoda maximálne do výšky [] € / do výšky odmeny uhradenej za posledných 12 mesiacov a že škoda nad tento rozsah nebola pri uzavretí zmluvy predvídateľná (§ 379 ObZ). Škoda sa nahrádza ako skutočná škoda a ušlý zisk (§ 373 ObZ).
- **6.8.3** Limit podľa bodu 6.8.2 sa neuplatní pri: (a) úmyselnom porušení alebo hrubej nedbanlivosti, (b) porušení mlčanlivosti podľa Čl. VII, (c) spracúvaní nad rámec alebo v rozpore s pokynmi Prevádzkovateľa, (d) neoprávnenom zapojení ďalšieho sprostredkovateľa, (e) nárokoch dotknutých osôb podľa bodu 6.2 a pokutách podľa bodu 6.5.
- **6.8.4** Strana sa zbaví zodpovednosti, ak preukáže okolnosti vylučujúce zodpovednosť (§ 374 ObZ). Strany sa výslovne dohodli, že za takúto okolnosť sa nepovažuje kybernetický útok, únik údajov ani výpadok, ktorým bolo možné predísť riadnym plnením opatrení podľa Prílohy č. 2, ani omeškanie subdodávateľa Sprostredkovateľa.

6.9 Poistenie: Sprostredkovateľ sa zaväzuje počas trvania zmluvy udržiavať poistenie zodpovednosti za škodu spôsobenú pri výkone podnikania (prípadne kybernetické poistenie) s limitom plnenia najmenej [] € a na výzvu predložiť poistnú zmluvu alebo certifikát.

6.10 Audit, kontrola a súčinnosť: Pravidlá pre audity a kontrolné mechanizmy:

- **6.10.1** Sprostredkovateľ poskytne Prevádzkovateľovi informácie potrebné na preukázanie splnenia povinností a umožní audit vrátane kontroly na mieste (§ 34); audit sa oznamuje [15] dní vopred, najviac [1]× ročne, mimo mimoriadnych prípadov (incident, podnet úradu).
- **6.10.2** Náklady auditu znáša Prevádzkovateľ; ak audit preukáže podstatné porušenie na strane Sprostredkovateľa, znáša ich Sprostredkovateľ.

- **6.10.3** Sprostredkovateľ je povinný informovať Prevádzkovateľa, ak sa jeho pokyn podľa názoru Sprostredkovateľa prieči zákonu; do vyriešenia je oprávnený vykonanie pokynu odložiť a nie je v omeškaní.
- **6.10.4** Za neposkytnutie súčinnosti pri vybavovaní žiadosti dotknutej osoby v lehote [5] pracovných dní od výzvy sa dojednáva zmluvná pokuta [___] € za každý prípad.

Čl. VII – MLČANLIVOSŤ

7.1 Zákonná povinnosť mlčanlivosti: Pravidlá ochrany dôverných informácií a osobných údajov:

- **7.1.1** Prevádzkovateľ aj Sprostredkovateľ sú povinní zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú; táto povinnosť trvá aj po ukončení spracúvania osobných údajov (§ 79 zákona č. 18/2018 Z. z.).
- **7.1.2** Sprostredkovateľ je povinný zaviazť mlčanlivosťou všetky fyzické osoby, ktoré prídu do styku s osobnými údajmi, pričom táto povinnosť musí trvať aj po skončení ich pracovného pomeru alebo obdobného vzťahu (§ 79); to zodpovedá aj povinnosti zabezpečiť záväzok mlčanlivosti oprávnených osôb podľa § 34.
- **7.1.3** Sprostredkovateľ vedie aktuálny zoznam oprávnených osôb a uchováva podpísané záväzky mlčanlivosti (vzor — Príloha č. 3) po dobu [3] rokov od skončenia oprávnenia; na výzvu ich predloží.

7.2 Rozsah dôverných informácií: Za dôverné sa považujú najmä: osobné údaje a ich exporty, databázové dumpy a zálohy, prístupové údaje, kľúče, tokeny a certifikáty, konfigurácie serverov, logy, zdrojový kód, bezpečnostné opatrenia, zistené zraniteľnosti, obchodné a technické informácie tvoriace obchodné tajomstvo (§ 17 ObZ), ktorému patrí právna ochrana proti porušeniu alebo ohrozeniu (§ 20 ObZ), ako aj informácie označené ako dôverné pri rokovaní o zmluve (§ 271 ObZ).

7.3 Konkrétne povinnosti Sprostredkovateľa: Povinnosti Sprostredkovateľa pri nakladaní s údajmi:

- **a)** neposkytnúť ani nesprístupniť osobné údaje tretej osobe bez pokynu Prevádzkovateľa alebo bez zákonnej povinnosti;
- **b)** nepoužiť osobné údaje na vlastné účely, na testovanie, tréning modelov, marketing, analytiku ani na referencie;
- **c)** zákaz kopírovania produkčných dát do vývojového alebo testovacieho prostredia; ak je to nevyhnutné, len po anonymizácii/pseudonymizácii a s písomným súhlasom;
- **d)** zákaz uchovávania osobných údajov na súkromných zariadeniach, v súkromných cloudových účtoch a zasielania nešifrovaným e-mailom;
- **e)** prístup podľa zásady need-to-know a najmenších privilégií, individuálne účty, viacfaktorové overenie, evidencia prístupov, okamžité odobratie prístupov pri skončení spolupráce;
- **f)** zachovávať mlčanlivosť o zistených zraniteľnostiach a neverejniť ich pred ich odstránením;
- **g)** sprístupniť dôverné informácie ďalšiemu sprostredkovateľovi len po jeho písomnom zaviazaní mlčanlivosťou v rovnakom rozsahu.

7.4 Výnimky z mlčanlivosti: Povinnosť mlčanlivosti neplatí, ak:

- **(a)** je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona (§ 79);
- **(b)** ide o vzťah k Úradu na ochranu osobných údajov SR pri plnení jeho úloh (§ 79);
- **(c)** informácia je verejne dostupná bez porušenia tejto zmluvy;
- **(d)** druhá strana dala písomný súhlas;
- **(e)** ide o poskytnutie právneho, daňového alebo audítorského poradcovi viazanému mlčanlivosťou. O poskytnutí podľa písm. (a) strana druhú stranu informuje, ak to zákon nezakazuje.

7.5 Trvanie: Mlčanlivosť o osobných údajoch je časovo neobmedzená a trvá aj po ukončení spracúvania a po zániku tejto zmluvy (§ 79). Mlčanlivosť o ostatných dôverných informáciách trvá [5] rokov od skončenia zmluvy.

7.6 Zmluvná pokuta za porušenie mlčanlivosti: Sankčné mechanizmy:

- **7.6.1** Za každé jednotlivé porušenie povinnosti podľa Čl. VII sa dojednáva zmluvná pokuta [___] €, splatná do [15] dní od doručenia výzvy. Dojednanie má písomnú formu a určuje výšku pokuty, ako to vyžaduje zákon (§ 544 OZ).
- **7.6.2** Strany sa výslovne dohodli, že popri zmluvnej pokute má oprávnená strana nárok aj na náhradu škody v plnom rozsahu, a to aj v časti presahujúcej zmluvnú pokutu. (Táto veta je nevyhnutná — bez nej by veriteľ nemal nárok na náhradu škody krytej pokutou ani na jej presahujúcu časť podľa § 545 OZ.)
- **7.6.3** Zaplatením zmluvnej pokuty nezaniká porušená povinnosť (§ 545 OZ).
- **7.6.4** Okolnosti vylučujúce zodpovednosť nemajú vplyv na povinnosť platiť zmluvnú pokutu (§ 300 ObZ); odstúpenie od zmluvy sa nedotýka nároku na jej zaplatenie (§ 302 ObZ).
- **7.6.5** Strany berú na vedomie, že neprimerane vysokú zmluvnú pokutu môže súd znížiť (§ 301 ObZ) — pokutu preto odporúčam nastaviť primerane (spravidla v pásme jednej až trojnásobku mesačnej odmeny, nie „exemplárne“ sumy).

7.7 Vrátenie a výmaz dôverných informácií: Po skončení spracúvania Sprostredkovateľ podľa voľby Prevádzkovateľa osobné údaje vymaže alebo vráti a vymaže existujúce kópie vrátane záloh, ak právny predpis neukladá ich uchovanie (§ 34). O vykonaní výmazu vydá písomné potvrdenie do [15] dní vrátane uvedenia dátumu, rozsahu a spôsobu výmazu a lehoty rotácie záloh. Prístupy a poverenia sa deaktivujú do [3] pracovných dní.