Zmluva o spracúvaní osobných údajov služby NASIT eFaktúra

Verzia 1.2 | Účinná od 4. 11. 2026 | NASIT, s.r.o., IČO 51 479 923

Článok 1 Strany a roly

1.1 Táto zmluva podľa čl. 28 GDPR (ďalej „DPA“) je súčasťou Zmluvy podľa VOP NASIT eFaktúra. Zmluvnými stranami sú Klient identifikovaný v prijatej objednávke alebo zázname o uzavretí Zmluvy a NASIT, s.r.o., Havlíčkova 6794/4A, 811 04 Bratislava, IČO 51 479 923, Mestský súd Bratislava III, oddiel Sro, vložka 200711/B. Konkrétna rola Klienta sa určuje podľa bodu 1.2; NASIT je v dohodnutom rozsahu sprostredkovateľom alebo ďalším sprostredkovateľom (ďalej spoločne „Sprostredkovateľ“).

1.2 Ak Klient určuje účely a prostriedky spracúvania svojich Dokladov, je prevádzkovateľom. Ak účtovník alebo iný Klient spracúva Doklady v mene zákazníckej Firmy ako jej sprostredkovateľ, NASIT koná ako jeho ďalší sprostredkovateľ; Klient zabezpečí povolenie tohto zapojenia, oprávnenie dávať pokyny a prenos príslušných povinností. Ak je Firma priamou zmluvnou stranou NASIT a účtovník len jej používateľom, pokyny vychádzajú z oprávnení tejto Firmy. Pre každú Firmu sa eviduje príslušný zmluvný a poverovací reťazec.

1.3 DPA sa uzatvára preukázateľne spolu so Zmluvou alebo samostatne v elektronickej písomnej forme. Za oprávnenie prijať DPA a dávať pokyny nezodpovedá automaticky každý používateľ v technickej role OWNER. Pojmy sa vykladajú podľa GDPR a VOP; v ochrane údajov má DPA prednosť pred VOP.

1.4 DPA pokrýva spracúvanie na pokyn Klienta. Nevylučuje také spracúvanie plošne len preto, že ide o správu účtu, podporu alebo bezpečnosť. NASIT je samostatným prevádzkovateľom iba pre vlastné preukázané účely a právne povinnosti, najmä vlastný zmluvný a účtovný vzťah, ochranu svojich systémov a príslušné zákonné oznámenia. Tieto úlohy, ich právne základy a lehoty vysvetľujú Zásady ochrany osobných údajov. Samotná zmluva s Peppol autoritou neurčuje automaticky všetky roly voči Klientom.

Článok 2 Predmet a rozsah spracúvania

2.1 Predmetom je spracúvanie osobných údajov obsiahnutých v Dokladoch, prílohách a súvisiacich údajoch pri poskytovaní NASIT eFaktúra. Operácie zahŕňajú príjem a nahratie, antivírusovú kontrolu, OCR a extrakciu údajov, vytváranie a úpravy na pokyn, validáciu, transformáciu a zobrazenie, odosielanie a prijímanie cez aktivované rozhrania, ukladanie, verziovanie, zabezpečenie, sprístupnenie oprávneným osobám, export, vrátenie a výmaz. Nevyhnutný podporný prístup sa obmedzí na konkrétny účel a zaznamená.

2.2 Účelom je poskytovať objednanú Službu podľa zdokumentovaných pokynov. Obsah Dokladov sa nepoužíva na marketing, tvorbu obchodných databáz o partneroch Klienta ani trénovanie všeobecných modelov umelej inteligencie. OCR nie je súhlasom s takým ďalším použitím. Produktová analytika NASIT je samostatne opísaná v Zásadách a nesmie obchádzať zákaz použitia obsahu Dokladov.

2.3 Spracúvanie trvá počas príslušnej Služby, dohodnutej archivácie, prechodného a exportného obdobia a kontrolovaného odstraňovania kópií podľa článku 6. DPA zostáva účinná, kým NASIT spracúva údaje v tejto role, aj po skončení predplatného.

2.4 Kategórie údajov: mená, funkcie a kontakty osôb; údaje fyzických osôb podnikateľov vrátane IČO, DIČ a IČ DPH; adresy a fakturačné údaje; IBAN, platobné referencie a sumy; položky, ceny,

poznámky a obsah príloh; podpisové alebo pečiatkové obrázky vložené Klientom; technické identifikátory, revízie, časy a výsledky spracovania a doručovania. Obrázok podpisu sa nepoužíva na biometrickú identifikáciu.

2.5 Dotknutými osobami sú najmä zamestnanci a zástupcovia Klienta a Firmy, odberatelia, dodávatelia, živnostníci a kontaktné či iné osoby uvedené v Dokladoch. Klient minimalizuje rozsah osobných údajov a zabezpečí zákonnosť ich vloženia a ďalšieho spracúvania.

2.6 Služba nie je osobitne určená na spracúvanie osobitných kategórií podľa čl. 9 alebo údajov podľa čl. 10 GDPR. Klient ich nesmie vkladať bez preukázaného právneho dôvodu a primeraného posúdenia ochrany; ak ich Doklad nevyhnutne obsahuje, oznámi bezpečným spôsobom potrebu osobitných opatrení bez zbytočného ďalšieho šírenia. Strany dohodnú primeraný režim alebo spracovanie obmedzia. Náhodný výskyt takých údajov sa nepovažuje za dôkaz, že sa technicky vôbec nespracúvajú. NASIT pri zistení postupuje bezpečne a neposiela obsah do bežných logov alebo analytiky.

Článok 3 Pokyny a povinnosti

3.1 Pokynmi sú Zmluva, táto DPA a oprávnené úkony v aplikácii alebo API a overené podporné žiadosti. Pokyn na zmenu oprávnení, odovzdanie údajov alebo výmaz sa overí podľa identity, roly a poverenia; obyčajný e-mail z neoverenej adresy nestačí. Pokyny sa vzťahujú aj na prenosy do tretích krajín. Ak spracúvanie prikazuje právo, NASIT o tom Klienta vopred informuje, ak mu to zákon nezakazuje.

3.2 NASIT zabezpečí mlčanlivosť oprávnených osôb, primerané technické a organizačné opatrenia podľa čl. 32 GDPR a prílohy A, riadenie ďalších sprostredkovateľov, potrebnú pomoc pri právach osôb a povinnostiach podľa čl. 32 až 36 GDPR, dokumentáciu súladu a audit. Bezodkladne upozorní na pokyn, ktorý podľa jeho názoru porušuje predpisy o ochrane údajov, a v dotknutom rozsahu ho pozastaví do objasnenia, pokiaľ právo neurčuje inak.

3.3 Klient zodpovedá za právny základ svojho spracúvania, informovanie dotknutých osôb, oprávnenia svojich používateľov a právoplatnosť pokynov. Táto zodpovednosť nezbavuje NASIT vlastných povinností sprostredkovateľa.

3.4 Žiadosť dotknutej osoby týkajúcu sa spracúvania na pokyn NASIT bez zbytočného odkladu postúpi príslušnému Klientovi; obsah žiadosti neposkytne nesprávnej Firme podľa samotnej zhody mena alebo e-mailu. Odpovedá len na oprávnený pokyn alebo z vlastnej zákonnej povinnosti. Pri vlastnom spracúvaní ako prevádzkovateľ vybaví žiadosť samostatne a vysvetlí rozdiel.

Článok 4 Dodávatelia a medzinárodné prenosy

4.1 Klient udeľuje všeobecné písomné povolenie na ďalších sprostredkovateľov uvedených v prílohe B v jej prijatom znení. NASIT vedie dostupný aktuálny register s identitou poskytovateľa a zmluvnej entity, službou, rozsahom údajov, umiestnením a prenosovým režimom. Samostatní prevádzkovatelia sa neoznačujú za ďalších sprostredkovateľov iba preto, že sú príjemcami údajov.

4.2 O zamýšľanom pridaní alebo nahradení ďalšieho sprostredkovateľa NASIT informuje najmenej 30 dní vopred e-mailom alebo iným dohodnutým aktívnym oznámením. Klient môže v tejto lehote vzniesť odôvodnenú námietku ochrany údajov. Strany preveria alternatívu; ak ju nenájdu, Klient môže ukončiť dotknutú časť služby pred zapojením dodávateľa a dostane pomernú cenu neposkytnutého obdobia. Tým nie sú dotknuté jeho práva na export.

4.3 NASIT uloží ďalšiemu sprostredkovateľovi zmluvne rovnocenné povinnosti podľa čl. 28 ods. 4 GDPR a zodpovedá za ich plnenie v zákonnom rozsahu. Overí dostatočné záruky vrátane obmedzení OCR a ďalšieho použitia obsahu. Prístup podpory dodávateľa sa považuje za spracúvanie, aj keď sa primárne úložisko nachádza v EÚ.

4.4 Primárne ukladanie Dokladov je v EÚ. Samo osebe to nevylučuje spracúvanie podporných, identitných alebo platobných údajov mimo EÚ. NASIT vykoná prenos iba pri splnení kapitoly V GDPR: použije uplatniteľné rozhodnutie o primeranosti vrátane overenia jeho rozsahu, alebo vhodné záruky, najmä štandardné doložky, posúdenie prenosu a potrebné doplnkové opatrenia. Nevyhlasuje automaticky každý americký subjekt za pokrytý primeranosťou. Informácie a príslušné záruky sprístupní na žiadosť pri ochrane tajomstiev a údajov iných osôb.

4.5 Odovzdanie Dokladu príjemcovi a jeho poskytovateľovi Peppol je súčasťou oprávneného pokynu. Tieto subjekty nie sú automaticky ďalšími sprostredkovateľmi NASIT; ich rola sa posudzuje podľa vlastného vzťahu. Pri odoslaní mimo EHP sa osobitne určí zodpovednosť a prenosový režim; samotný pokyn Klienta nenahrádza povinné záruky kapitoly V.

Článok 5 Incidenty a audit

5.1 NASIT oznámi Klientovi porušenie ochrany osobných údajov bez zbytočného odkladu po tom, ako sa o ňom dozvie, najneskôr do 48 hodín. Táto lehota je zmluvná vonkajšia hranica, nie oprávnenie čakať 48 hodín. Oznámi aj priebežné informácie bez čakania na úplné vyšetrovanie: povahu, známe kategórie a približné počty, následky, opatrenia a kontaktnú osobu; ďalšie údaje doplní. Klient zostáva zodpovedný za vlastné oznámenia orgánu a osobám, pri ktorých mu NASIT pomáha.

5.2 NASIT poskytne potrebnú súčinnosť pri DPIA, konzultácii, právach osôb a bezpečnostnom posúdení. Primerané náklady nad bežný rozsah možno účtovať iba po vopred oznámenej a prijatej dohode; nesmú podmieňovať bezodkladné oznámenie incidentu ani odstránenie vlastného porušenia NASIT.

5.3 NASIT poskytne relevantnú dokumentáciu a umožní audit Klientovi alebo nezávislému audítorovi viazanému mlčanlivosťou. Bežný audit sa plánuje spravidla 30 dní vopred a raz ročne s primeraným využitím existujúcich dôkazov. Tieto organizačné pravidlá neobmedzujú odôvodnený dodatočný audit pri dôvodnom podozrení na nesúlad, incidente alebo pokyne dozorného orgánu. Audit chráni údaje iných Klientov a nesmie neprimerane ohroziť prevádzku; NASIT poskytne vhodný alternatívny dôkaz, nie plošné odmietnutie kontroly.

Článok 6 Vrátenie výmaz a trvanie

6.1 Po skončení spracúvania Klient zvolí vrátenie údajov a následný výmaz alebo výmaz podľa čl. 28 ods. 3 písm. g) GDPR. Štandardné prevzatie trvá 60 dní po skončení Služby alebo prechodného obdobia podľa VOP; skorší výmaz na overený pokyn je možný, ak mu nebráni právna povinnosť alebo dohodnuté dokončenie vrátenia. Osobitne prijatá dlhšia archivácia sa splní, pokiaľ ju oprávnené strany platne neukončia.

6.2 Po uplynutí príslušného prevzatia alebo vykonaní skoršieho oprávneného pokynu NASIT bez zbytočného odkladu odstráni aktívne kópie vrátane príloh, indexov, odvodených súborov a verzií, na ktoré sa pokyn vzťahuje. Vymazanie zahŕňa aj dotknutých ďalších sprostredkovateľov. Skrytie v aplikácii nie je výmazom. NASIT vedie záznam o vykonaní a na žiadosť poskytne potvrdenie s uvedením prípadných výnimiek.

6.3 Izolované zálohy, snímky, verzie úložísk a obnovovacie či nasadzovacie kópie obsahujúce dotknuté údaje sa odstránia v bežnej kontrolovanej rotácii, najneskôr do 90 dní od dátumu odstránenia aktívnych kópií. Počas tejto doby sa nepoužívajú na bežné spracúvanie, prístup je obmedzený a pri obnove sa opätovne uplatnia evidované pokyny na výmaz. NASIT nesmie túto lehotu obísť premenovaním zálohy na trvalú servisnú kópiu.

6.4 Ak konkrétne údaje vyžaduje uchovať právo, NASIT zdokumentuje kategóriu, dôvod, nevyhnutný rozsah a lehotu, obmedzí ďalšie použitie a informuje Klienta, ak mu to právo nezakazuje. Vlastná evidencia právneho nároku alebo incidentu sa neposudzuje ako automatické oprávnenie zachovať

celý archív Klienta. Údaje vedené NASIT ako samostatným prevádzkovateľom sa posúdia podľa osobitného právneho základu a Zásad; výnimka sa nepredstiera pri údajoch na pokyn.

6.5 DPA trvá, kým trvá príslušné spracúvanie vrátane chránených zostatkových kópií. Zodpovednosť sa riadi VOP a právom bez zásahu do čl. 82 GDPR. Zmena DPA sa oznámi podľa článku 15 VOP a nesmie jednostranne oslabiť povinné záruky alebo rozšíriť pokyny na cudzie účely. Táto verzia 1.2 je účinná od 4. 11. 2026.

Príloha A Technické a organizačné opatrenia

A.1 Prístup. Práva sa prideľujú podľa roly, Firmy a Pracovného priestoru; kontrolujú sa na serveri. Prevádzkové prístupy sú obmedzené a evidované. NASIT Ops používa osobitný prístup cez VPN a druhý faktor TOTP. Táto konkrétna kontrola neznamená, že každé zákaznícke alebo infraštruktúrne prihlásenie má rovnaký druhý faktor. Pri ostatných administrátorských cestách sa uplatní riadené overenie, individuálne oprávnenia a ochrana tajomstiev podľa rizika.

A.2 Prenos a uloženie. Verejná aplikácia a API používajú TLS. Aktivovaný prenos Peppol používa AS4 a príslušné podpisovanie a šifrovanie podľa záväznej špecifikácie. Citlivé integračné tajomstvá a chránené notifikácie FS sú zabezpečené osobitne. Súbory sú v neverejnom úložisku s riadeným prístupom. Táto príloha nevyhlasuje bez ďalšieho, že každá databáza, lokálny disk a každá obnovovacia kópia sú šifrované na úrovni obsahu; NASIT zdokumentuje použitú ochranu jednotlivých vrstiev a podľa rizika zabezpečí potrebné šifrovanie a oddelenú správu kľúčov.

A.3 Oddelenie a evidencia. Údaje sú logicky oddelené podľa Klientov a Firiem. Oprávnenia sa uplatňujú na čítanie, zápis, export aj podporu. Zmeny Dokladov a dôležité prístupové a prevádzkové udalosti majú auditnú evidenciu. Záznamy obsahujú potrebné identifikátory a výsledky; celé Doklady, heslá, tokeny a súkromné kľúče sa nevkladajú do bežných logov.

A.4 Súbory a systémy. Nahrávané podporované súbory prechádzajú kontrolou formátu, limitov a škodlivého obsahu pred uložením. NASIT riadi aktualizácie, zraniteľnosti, konfiguráciu, zmeny a oddelenie testovacieho a produkčného doručovania. Interné conformance prostredie nie je zákazníckou sandboxovou ponukou.

A.5 Zálohy a kontinuita. NASIT vedie pravidelné zálohy, riadený prístup a evidenciu retenčných lehôt, obnovovací postup a overovanie obnoviteľnosti. Samotná existencia databázového dumpu sa nepovažuje za úspešný úplný obnovovací test. Pri dohodnutí konkrétneho RPO alebo RTO ho podloží rozsahom zálohovania, obnovy a meraním. Zálohy zahŕňajú ochranu potrebných väzieb na súbory a dôkazy, nie iba prevádzkovú databázu.

A.6 Osoby a incidenty. Osoby s prístupom sú viazané mlčanlivosťou a primerane poučené. Podporný zásah sa vykonáva v potrebnom rozsahu. NASIT udržiava postup incidentov, eskalácie, obnovy, spracovania žiadostí a likvidácie údajov a preskúma opatrenia najmenej ročne a pri podstatnej zmene. Táto príloha nepredstavuje vyhlásenie o získaní certifikácie ISO 27001.

Príloha B Register služieb a príjemcov

B.1 Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Nemecko: hosting aplikácie a databáz v dátovom centre Norimberg (Nemecko, EÚ) a súvisiaca prevádzková obnova. V rozsahu údajov Dokladov uložených na pokyn ide o ďalšieho sprostredkovateľa NASIT; pri jeho vlastných zákazníckych a účtovných údajoch sa posudzuje samostatná rola dodávateľa. Rozsah zahŕňa databázu, konfiguráciu a riadene vytvorené obnovovacie kópie.

B.2 Microsoft Ireland Operations Limited, Dublin, Írsko (Microsoft Azure): neverejné Blob úložisko súborov a fronty spracovania v regióne Poland Central (Poľsko, EÚ), Azure AI Document Intelligence pre OCR a extrakciu v regióne Germany West Central (Nemecko, EÚ) a Azure Communication Services na odosielanie systémových e-mailov a e-mailov s Dokladmi na pokyn Klienta. Pri obsahu

Dokladov a odosielaní na pokyn ide o ďalšieho sprostredkovateľa; pri vlastných bezpečnostných a obchodných účeloch sa rola posudzuje osobitne. Podporné prístupy podliehajú bodu 4.4.

B.3 Microsoft Ireland Operations Limited (Microsoft Entra External ID) a Google Ireland Limited, Dublin, Írsko (prihlásenie účtom Google): prihlásenie a overenie používateľa, identifikátor účtu, e-mail, meno a relevantné overovacie tvrdenia. Nejde o odovzdanie obsahu faktúr na prihlásenie. Podľa konkrétneho produktu a účelu môžu poskytovatelia konať v zmluvnej alebo samostatnej prevádzkovej role. Podrobnosti vlastného prihlasovacieho spracúvania NASIT sú v Zásadách; tieto služby sa neoznačujú plošne za ďalších sprostredkovateľov obsahu Dokladov.

B.4 PostHog Inc., USA, služba PostHog EU Cloud s uložením údajov v EÚ: produktová analytika a pri príslušnom súhlase záznam relácií. Pre vlastné analytické účely NASIT je dodávateľom spracúvania NASIT, nie automaticky ďalším sprostredkovateľom všetkých zákazníckych faktúr. Do analytiky sa nemá posielať obsah Dokladov; uplatňuje sa maskovanie a obmedzenie zachytávania. Vlastné spracúvanie je opísané v Zásadách vrátane obmedzených udalostí bez analytických cookies a režimu súhlasu.

B.5 Polar, subjekt označený v pokladni a nákupnom doklade: predajca Merchant of Record pre predplatné, daňové, fakturačné a platobné údaje. V týchto vlastných povinnostiach je samostatným prevádzkovateľom, nie ďalším sprostredkovateľom obsahu Dokladov NASIT. NASIT nespracúva úplné číslo platobnej karty. Platobné údaje a podporný prístup môžu podliehať režimu mimo EHP.

B.6 Finančné riaditeľstvo SR, OpenPeppol AISBL, prevádzkovateľ SK-SMP a poskytovatelia príjemcu: príjemcovia údajov v rozsahu registrácie, zákonného oznamovania, sieťových povinností alebo pokynu na doručenie, s rolou určenou príslušným účelom. Nie sú všeobecne ďalšími sprostredkovateľmi NASIT. O zmene ďalších sprostredkovateľov uvedených v bodoch B.1 až B.5 NASIT Klienta vopred informuje podľa bodu 4.2.