

Smlouva o zpracování osobních údajů

Verze 1.0 ze dne 19. 10. 2026 · vygenerováno 29. 10. 2026

Správce:, IČO, sídlo
(dále jen „správce“)

Zpracovatel: Ivo Žáček, IČO, místo podnikání
....., provozovatel služby Kvitano (kvitano.cz) (dále jen „zpracovatel“)

Článek 1 - Předmět smlouvy

1.1 Zpracovatel poskytuje správci cloudovou službu Kvitano pro příjem, vytěžení, kontrolu, export a archivaci účetních dokladů (dále jen „služba“). Při poskytování služby zpracovává zpracovatel osobní údaje jménem správce.

1.2 Strany se dohodly, že se zpracování řídí standardními smluvními doložkami mezi správcem a zpracovatelem přijatými prováděcím rozhodnutím Komise (EU) 2021/915 ze dne 4. června 2021 podle čl. 28 odst. 7 nařízení (EU) 2016/679 (dále jen „doložky“). Doložky jsou uvedeny v článku 3 této smlouvy včetně příloh I až IV a strany je nemění.

1.3 Článek 2 obsahuje doplňující ujednání podle doložky 2 písm. b). Tato ujednání nejsou s doložkami v přímém ani nepřímém rozporu a neomezují základní práva ani svobody subjektů údajů. V případě rozporu mají přednost doložky (doložka 4).

Článek 2 - Doplňující ujednání

2.1 **Pokyny.** Pokynem správce podle doložky 7.1 je tato smlouva a dále každé použití funkcí služby správcem nebo osobami, kterým správce ve službě udělil přístup (nahrání dokladu, oprava údajů, ověření, export, nastavení klienta, smazání). Služba tyto úkony zaznamenává, čímž jsou pokyny písemně doloženy.

2.2 **Ohlášení porušení zabezpečení.** Zpracovatel oznámí správci porušení zabezpečení osobních údajů podle doložky 9.2 bez zbytečného odkladu, **nejpozději do 48 hodin** poté, co se o něm dozvěděl, a to e-mailem na adresu vlastníka účtu správce ve službě.

2.3 **Dílčí zpracovatelé.** Aktuální seznam dílčích zpracovatelů je uveden v příloze IV a zveřejněn na kvitano.cz/legal/data-residency. Zpracovatel oznámí zamýšlenou změnu e-mailem vlastníkovému účtu správce nejméně 30 dnů předem (doložka 7.7 písm. a)). Vznese-li správce proti změně odůvodněnou námitku a strany se nedohodnou, může správce smlouvu o poskytování služby vypovědět bez sankce ke dni zapojení nového dílčího zpracovatele.

2.4 **Audity.** Zpracovatel prokazuje soulad podle doložky 7.6 přednostně poskytnutím dokumentace (popis opatření, seznam dílčích zpracovatelů, jejich smlouvy o zpracování v rozsahu doložky 7.7 písm. c), auditní záznamy týkající se dat správce). Audit v prostorách zpracovatele správce ohlásí nejméně 30 dnů předem, nejvýše jednou za kalendářní rok, ledaže existují známky nesouladu nebo audit vyžaduje dozorový úřad. Náklady auditu nese správce, nebylo-li auditem zjištěno porušení doložek.

2.5 **Ukončení a výmaz.** Po skončení smlouvy o poskytování služby má správce 30 dní na export dat (soubory pro účetní program, CSV/XLSX a originály dokladů). Poté zpracovatel data správce podle doložky 10 písm. d) vymaže, nejpozději do 60 dnů od skončení smlouvy, a výmaz správci potvrdí. Data v šifrovaných zálohách nelze mazat jednotlivě: zůstávají v nich do uplynutí doby uchování záloh (týdenní zálohy 12 týdnů, měsíční archiv až 10 let), nejsou dále zpracovávána ani zpřístupňována a při případné obnově ze zálohy budou znovu vymazána.

2.6 **Nahodilé citlivé údaje (doložka 7.5).** Služba není určena ke zpracování citlivých údajů. Mohou se však objevit nahodile na dokladech (např. paragon z lékárny nebo faktura za zdravotní službu). Zpracovatel takové údaje nevyhledává, nevyhodnocuje ani nepoužívá k jinému účelu než

ke zpracování dokladu, přístup k nim mají jen osoby oprávněné správcem a platí pro ně opatření uvedená v příloze III.

2.7 Umělá inteligence. Vytěžení dokladů provádí model umělé inteligence dílčího zpracovatele (příloha IV) v režimu, kdy poskytovatel nepoužívá data k tréninku modelů. Pravidla a naučené návrhy pro zařazení položek se vedou odděleně pro každého klienta správce a nepoužívají se pro jiné zákazníky zpracovatele ani pro vlastní účely zpracovatele.

2.8 Kontakt zpracovatele pro záležitosti ochrany osobních údajů: info@kvitano.cz. Zpracovatel nejmenoval pověřence pro ochranu osobních údajů, protože mu tato povinnost podle čl. 37 nařízení (EU) 2016/679 nevzniká.

2.9 Trvání a rozhodné právo. Smlouva se uzavírá na dobu, po kterou zpracovatel pro správce zpracovává osobní údaje, a nabývá účinnosti dnem podpisu oběma stranami. Řídí se právem České republiky.

Článek 3 - Standardní smluvní doložky

Prováděcí rozhodnutí Komise (EU) 2021/915, příloha. Strany zvolily MOŽNOST 1 (nařízení (EU) 2016/679) všude, kde doložky nabízejí volbu, a v doložce 7.7 MOŽNOST 2 (obecné písemné povolení).

ODDÍL I

Doložka 1 - Účel a oblast působnosti

- a) Účelem těchto standardních smluvních doložek (dále jen „doložky“) je zajistit soulad s ustanoveními čl. 28 odst. 3 a 4 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).
- b) Správci a zpracovatelé uvedení v příloze I schválili tyto doložky, aby zajistili soulad s čl. 28 odst. 3 a 4 nařízení (EU) 2016/679 a/nebo čl. 29 odst. 3 a 4 nařízení (EU) 2018/1725.
- c) Tyto doložky se uplatňují na zpracování osobních údajů, jak je upřesněno v příloze II.
- d) Přílohy I až IV jsou nedílnou součástí těchto doložek.
- e) Těmito doložkami nejsou dotčeny povinnosti, které správce musí plnit na základě nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.
- f) Tyto doložky samy o sobě nezajišťují soulad s povinnostmi týkajícími se mezinárodního předávání podle kapitoly V nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

Doložka 2 - Neměnnost doložek

- a) Smluvní strany se zavazují, že doložky nebudou měnit, s výjimkou doplňování nebo aktualizace informací v přílohách.
- b) To stranám nebrání v možnosti zahrnout tyto standardní smluvní doložky stanovené v tomto rozhodnutí do širší smlouvy nebo k nim doplnit další doložky nebo další záruky, pokud tyto nejsou se standardními smluvními doložkami v přímém nebo nepřímém rozporu nebo pokud neomezují základní práva nebo svobody subjektů údajů.

Doložka 3 - Výklad

- a) V případech, kdy tyto doložky používají pojmy definované v nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725, mají tyto pojmy stejný význam jako v uvedeném nařízení.
- b) Tyto doložky jsou chápány a vykládány v souladu s ustanoveními nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725.
- c) Tyto doložky nesmí být vykládány způsobem, který by byl v rozporu s právy a povinnostmi stanovenými v nařízení (EU) 2016/679 / nařízení (EU) 2018/1725, nebo který by omezoval základní práva nebo svobody subjektů údajů.

Doložka 4 - Hierarchie

V případě rozporu mezi těmito doložkami a ustanoveními souvisejících dohod existujících mezi stranami v době, kdy jsou tyto doložky sjednány, nebo dohod uzavřených později mají přednost tyto doložky.

Doložka 5 - Nepovinná - Doložka o přistoupení

Strany tuto nepovinnou doložku nepoužívají.

ODDÍL II - POVINNOSTI STRAN

Doložka 6 - Popis zpracování

Podrobnosti týkající se operací zpracování, zejména kategorie osobních údajů a účely zpracování, pro něž jsou osobní údaje zpracovávány jménem správce, jsou uvedeny v příloze II.

Doložka 7 - Povinnosti stran

7.1 Pokyny

a) Zpracovatel zpracovává osobní údaje pouze na základě písemně doložených pokynů správce, pokud mu takové zpracování neukládá právo Unie nebo členského státu, které se na správce vztahuje. V tomto případě zpracovatel správce informuje o uvedeném právním požadavku před zpracováním, pokud to právní předpisy nezakazují z důvodů důležitého veřejného zájmu. Po celou dobu zpracování osobních údajů může správce rovněž vydávat další pokyny. Tyto pokyny musí být vždy písemně doloženy.

b) Zpracovatel neprodleně informuje správce v případě, že dle jeho názoru pokyny správce porušují nařízení (EU) 2016/679 / nařízení (EU) 2018/1725 nebo příslušná ustanovení Unie nebo členského státu o ochraně údajů.

7.2 Omezení účelu

Zpracovatel zpracovává osobní údaje pouze pro konkrétní účel nebo účely zpracování, jak je stanoveno v příloze II, pokud od správce neobdrží další pokyny.

7.3 Doba trvání zpracování osobních údajů

Zpracování zpracovatelem probíhá pouze po dobu stanovenou v příloze II.

7.4 Zabezpečení zpracování

a) Za účelem zajištění bezpečnosti osobních údajů musí zpracovatel zavést přinejmenším technická a organizační opatření uvedená v příloze III. Součástí těchto opatření musí být ochrana údajů před narušením bezpečnosti, které by vedlo k jejich náhodnému nebo protiprávnímu zničení, ztrátě, změně, neoprávněnému zpřístupnění nebo přístupu k nim (porušení zabezpečení osobních údajů). Při posuzování vhodné úrovně zabezpečení vezmou strany v úvahu aktuální stav techniky, náklady na provedení, povahu, rozsah, kontext a účely zpracování a rizika pro subjekty údajů.

b) Zpracovatel poskytne svým zaměstnancům přístup ke zpracovávaným osobním údajům pouze v rozsahu nezbytně nutném pro provádění, správu a kontrolu smlouvy. Zpracovatel zajistí, aby se osoby oprávněné zpracovávat obdržené osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

7.5 Citlivé údaje

Pokud zpracování zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu nebo o sexuálním životě či sexuální orientaci dané osoby nebo údaje týkající se odsouzení v trestních věcech a trestných činů (dále jen „citlivé údaje“), uplatní zpracovatel zvláštní omezení nebo další záruky.

7.6 Dokumentace a soulad

a) Strany musí být schopny prokázat dodržování těchto doložek.

b) Zpracovatel neprodleně a odpovídajícím způsobem vyřídí dotazy správce, které se týkají zpracovávání podle těchto doložek.

c) Zpracovatel poskytne správci veškeré informace potřebné k prokázání souladu s povinnostmi stanovenými v těchto doložkách, které vyplývají přímo z nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725. Zpracovatel též na žádost správce umožní audity činností zpracování, na něž se tyto doložky vztahují, a k těmto auditům přispěje, a to v přiměřených intervalech nebo pokud existují známky nesouladu. Při rozhodování o přezkumu nebo auditu může správce zohlednit

příslušná osvědčení držená zpracovatelem.

d) Správce se může rozhodnout, zda audit provede sám, nebo jím pověří nezávislého auditora. Audity mohou rovněž zahrnovat kontroly v objektech a prostorách zařízení zpracovatele a případně jsou předem včas ohlášeny.

e) Strany na požádání zpřístupní informace uvedené v této doložce, včetně výsledků případných auditů, příslušnému dozоровému úřadu, respektive příslušným dozоровým úřadům.

7.7 Využívání dílčích zpracovatelů údajů

a) **OBEČNÉ PÍSEMNÉ POVOLENÍ:** Zpracovatel má obecné povolení správce k zapojení dílčích zpracovatelů ze schváleného seznamu. Zpracovatel výslovně písemně informuje správce o všech zamýšlených změnách uvedeného seznamu přijetím nebo nahrazením dílčích zpracovatelů nejméně 30 dnů předem, čímž poskytne správci dostatek času na to, aby mohl vznést námitku proti takovým změnám před zapojením dotčeného dílčího zpracovatele / dotčených dílčích zpracovatelů. Zpracovatel poskytne správci informace nezbytné k tomu, aby správce mohl uplatnit své právo vznést námitku.

b) Pokud zpracovatel zapojí dílčího zpracovatele do provádění konkrétních činností zpracování (jménem správce), učiní tak prostřednictvím smlouvy, která ukládá dílčímu zpracovateli v podstatě stejné povinnosti v oblasti ochrany údajů, jaké jsou v souladu s těmito doložkami uloženy zpracovateli údajů. Zpracovatel zajistí, aby dílčí zpracovatel plnil povinnosti, které se na zpracovatele vztahují podle těchto doložek a nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

c) Zpracovatel poskytne správci na jeho žádost opis dohody s dílčím zpracovatelem a veškeré následné změny dohody. V rozsahu nutném k ochraně obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů, může zpracovatel před poskytnutím opisu text dohody upravit.

d) Zpracovatel nese vůči správci plnou odpovědnost za to, aby dílčí zpracovatel plnil povinnosti vyplývající z jeho smlouvy se zpracovatelem. Zpracovatel správce uvědomí, pokud dílčí zpracovatel neplní své povinnosti vyplývající z uvedené smlouvy.

e) Zpracovatel s dílčím zpracovatelem schválí doložku ve prospěch třetí strany, podle níž v případě, že zpracovatel fakticky zmizí, z právního hlediska zanikne, nebo se ocitne v platební neschopnosti, má správce právo ukončit smlouvu s dílčím zpracovatelem a pověřit dílčího zpracovatele, aby osobní údaje vymazal nebo vrátil.

7.8 Mezinárodní předávání údajů

a) Jakékoli předání údajů zpracovatelem do třetí země nebo mezinárodní organizaci se provádí pouze na základě písemně doložených pokynů správce nebo za účelem splnění konkrétního požadavku podle právních předpisů Unie nebo členského státu, které se na zpracovatele vztahují, a to v souladu s kapitolou V nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725.

b) Správce souhlasí s tím, že pokud zpracovatel v souladu s doložkou 7.7 zapojí dílčího zpracovatele do provádění konkrétních činností zpracování (jménem správce) a uvedené činnosti zahrnují předání osobních údajů ve smyslu kapitoly V nařízení (EU) 2016/679, mohou zpracovatel a dílčí zpracovatel zajistit soulad s ustanoveními kapitoly V nařízení (EU) 2016/679 použitím standardních smluvních doložek přijatých Komisí v souladu s čl. 46 odst. 2 nařízení (EU) 2016/679, pokud jsou splněny standardní podmínky pro použití těchto smluvních doložek.

Doložka 8 - Pomoc poskytovaná správci

a) Zpracovatel neprodleně informuje správce o každé žádosti, kterou obdržel od subjektu údajů. Na tuto žádost neodpovídá sám, pokud k tomu není správcem zmocněn.

b) Zpracovatel pomáhá správci při plnění jeho povinností reagovat na žádosti subjektů údajů o výkon jejich práv s přihlédnutím k povaze zpracování. Při plnění svých povinností podle ustanovení

písmen a) a b) postupuje zpracovatel v souladu s pokyny správce.

c) Kromě toho, že má zpracovatel povinnost pomáhat správci podle doložky 8 písm. b), zpracovatel správci dále pomáhá při zajišťování plnění následujících povinností, a to s přihlédnutím k povaze zpracování údajů a informacím, které má zpracovatel k dispozici:

- 1) povinnost provést posouzení dopadu zamýšlených operací zpracování na ochranu osobních údajů (dále jen „posouzení vlivu na ochranu údajů“), pokud je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob;
 - 2) povinnost konzultovat před zpracováním příslušný dozorový úřad, respektive příslušné dozorové úřady, pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika;
 - 3) povinnost zajistit, aby byly osobní údaje přesné a aktuální, a to tím, že zpracovatel správce neprodleně informuje, pokud se dozví, že osobní údaje, které zpracovává, jsou nepřesné nebo zastaralé;
 - 4) povinnosti podle článku 32 nařízení (EU) 2016/679.
- d) V příloze III strany stanoví vhodná technická a organizační opatření, jimiž je zpracovatel povinen správci pomáhat při uplatňování této doložky, jakož i oblast působnosti a rozsah požadované pomoci.

Doložka 9 – Ohlašování případů porušení zabezpečení osobních údajů

V případě porušení zabezpečení osobních údajů zpracovatel spolupracuje se správcem a pomáhá mu při plnění jeho povinností podle článků 33 a 34 nařízení (EU) 2016/679 nebo případně podle článků 34 a 35 nařízení (EU) 2018/1725, přičemž zohlední povahu zpracování a informace, které má zpracovatel k dispozici.

9.1 Porušení zabezpečení údajů zpracovávaných správcem

V případě porušení zabezpečení osobních údajů zpracovávaných správcem zpracovatel napomáhá správci:

- a) při ohlašování případů porušení zabezpečení osobních údajů příslušnému dozorovému úřadu, respektive příslušným dozorovým úřadům, a to bez zbytečného odkladu poté, co se o něm správce dozvěděl, je-li to relevantní / (pokud je nepravděpodobné, že by porušení zabezpečení osobních údajů vedlo k ohrožení práv a svobod fyzických osob);
- b) při získávání následujících informací, které musí být podle čl. 33 odst. 3 nařízení (EU) 2016/679 uvedeny v oznámení správce, a to musí přinejmenším zahrnovat:
 - 1) povahu daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
 - 2) pravděpodobné důsledky porušení zabezpečení osobních údajů;
 - 3) opatření přijatá nebo navržená k přijetí v souvislosti s porušením zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Pokud není možné poskytnout všechny tyto informace najednou, musí původní oznámení obsahovat informace, které jsou v dané době k dispozici, a další informace jsou poté poskytnuty bez zbytečného odkladu, jakmile jsou dostupné.

c) při plnění povinnosti v souladu s článkem 34 nařízení (EU) 2016/679 oznámit bez zbytečného odkladu subjektu údajů porušení zabezpečení osobních údajů, pokud je pravděpodobné, že dané porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

9.2 Porušení zabezpečení údajů zpracovávaných zpracovatelem

V případě porušení zabezpečení osobních údajů zpracovávaných zpracovatelem o tom zpracovatel informuje správce bez zbytečného odkladu poté, co se o tomto porušení dozvěděl. Takové oznámení obsahuje alespoň:

- a) popis povahy daného případu porušení (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a záznamů údajů);
- b) údaje o kontaktním místě, kde lze získat více informací o daném porušení zabezpečení osobních údajů;
- c) pravděpodobné důsledky a opatření přijatá nebo navržená k přijetí v souvislosti s porušením zabezpečení, a to včetně opatření ke zmírnění možných nepříznivých dopadů.

Pokud není možné poskytnout všechny tyto informace najednou, musí původní oznámení obsahovat informace, které jsou v dané době k dispozici, a další informace jsou poté poskytnuty bez zbytečného odkladu, jakmile jsou dostupné.

Strany stanoví v příloze III všechny další informace, které má zpracovatel poskytnout, když správci poskytuje pomoc při plnění povinností správce podle článků 33 a 34 nařízení (EU) 2016/679.

ODDÍL III - ZÁVĚREČNÁ USTANOVENÍ

Doložka 10 - Porušení doložek a ukončení smlouvy

a) Aniž jsou dotčena jakákoli ustanovení nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725, pokud zpracovatel poruší své povinnosti podle těchto doložek, může mu správce nařídit, aby pozastavil zpracovávání osobních údajů, dokud zpracovatel nebude plnit povinnosti podle těchto doložek, nebo dokud nebude smlouva vypovězena. Zpracovatel neprodleně informuje správce v případě, že z jakéhokoli důvodu není schopen plnit ustanovení těchto doložek.

b) Správce je oprávněn vypovědět smlouvu v rozsahu, v němž se týká zpracování osobních údajů v souladu s těmito doložkami, pokud:

1) správce pozastavil podle písmene a) zpracovávání osobních údajů zpracovatelem a plnění povinností podle těchto doložek není obnoveno v přiměřené lhůtě a v každém případě do jednoho měsíce od pozastavení;

2) zpracovatel závažně nebo trvale porušuje tyto doložky nebo povinnosti, které pro něj vyplývají z nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725;

3) zpracovatel neplní závazné rozhodnutí příslušného soudu nebo příslušného dozorového úřadu, respektive příslušných dozorových úřadů týkající se jeho povinností vyplývajících z těchto doložek nebo z nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

c) Zpracovatel je oprávněn vypovědět smlouvu v rozsahu, v němž se týká zpracování osobních údajů podle těchto doložek, pokud poté, co informoval správce o tom, že pokyny správce porušují platné právní požadavky podle doložky 7.1 písm. b), správce na splnění těchto pokynů trvá.

d) Po ukončení smlouvy zpracovatel podle volby správce vymaže veškeré osobní údaje zpracovávané jménem správce a potvrdí správci, že tak učinil, nebo vrátí veškeré osobní údaje správci a vymaže stávající kopie, pokud právo Unie nebo členského státu nepožaduje uchovávání osobních údajů. Dokud nejsou osobní údaje vymazány nebo vráceny, zpracovatel nadále zajišťuje dodržování souladu s těmito doložkami.

Příloha I - Seznam stran

Správce

Jméno/název:

IČO:

Adresa:

Jméno, funkce a kontaktní údaje kontaktní osoby:

Podpis a datum:

Zpracovatel

Jméno/název: Ivo Žáček

IČO:

Adresa:

Jméno, funkce a kontaktní údaje kontaktní osoby: Ivo Žáček, provozovatel služby Kvitano, info@kvitano.cz

Podpis a datum:

Příloha II - Popis zpracování

Kategorie subjektů údajů, jejichž osobní údaje jsou zpracovávány

- uživatelé služby na straně správce – vlastník, účetní a další osoby, kterým správce ve službě udělil přístup, včetně zaměstnanců klientů správce;
- klienti správce, jsou-li fyzickými osobami (zejména osoby samostatně výdělečně činné) – u správce, který vede účetnictví jiným osobám;
- dodavatelé a odběratelé správce nebo jeho klientů uvedení na dokladech, včetně kontaktních osob;
- další osoby uvedené na dokladech (např. přebírající osoba, prodavač, cestující);
- odesílatelé e-mailů, kterými doklady přicházejí na příjmovou adresu ve službě.

Kategorie zpracovávaných osobních údajů

- identifikační údaje: jméno, název, IČO, DIČ, adresa;
- bankovní údaje: číslo účtu, IBAN, BIC, variabilní symbol;
- údaje o transakci: položky dokladu (název, množství, cena, sazba DPH), částky, data, čísla dokladů;
- obrazový záznam dokladu (sken, fotografie, PDF) a originál elektronické faktury;
- obsah e-mailu, kterým doklad přišel: odesílatel, předmět, text, názvy příloh;
- údaje o uživatelích: e-mail, jméno, role, přihlašovací a bezpečnostní údaje (IP adresa u omezení pokusů o přihlášení);
- historie změn údajů dokladu (kdo, kdy, z jaké hodnoty na jakou);
- snímky odpovědí veřejných registrů k dodavateli (registr plátců DPH, ARES).

Zpracovávané citlivé údaje

Citlivé údaje se záměrně nezpracovávají. Mohou se vyskytnout nahodile na dokladech (např. údaj o zdravotní službě). Zpracovatel je nevyhledává ani nevyhodnocuje; platí pro ně řízení přístupu podle oprávnění správce, záznam změn a ostatní opatření z přílohy III (článek 2.6 smlouvy).

Povaha zpracování

Shromáždění (nahrání, příjem e-mailem), uložení, automatizované vytěžení údajů pomocí umělé inteligence, kontroly (výpočty, možné duplicity, bankovní účet dodavatele), úprava údajů na

pokyn uživatele, export do souborů pro účetní nebo skladový program, archivace, zálohování, výmaz.

Účel zpracování jménem správce

Zpracování účetních dokladů správce nebo jeho klientů: příjem, převod do strukturované podoby, kontrola, příprava podkladů pro účetní program (např. POHODA) a skladový systém a archivace dokladů podle § 35a zákona č. 235/2004 Sb. o dani z přidané hodnoty a § 31 zákona č. 563/1991 Sb. o účetnictví.

Doba trvání zpracování

Po dobu poskytování služby správci a dále po dobu podle článku 2.5 smlouvy (30 dnů na export, výmaz do 60 dnů, šifrované zálohy do uplynutí jejich doby uchování).

Zpracování dílčími zpracovateli

Předmět, povaha a doba trvání zpracování jednotlivými dílčími zpracovateli jsou uvedeny v příloze IV. Dílčí zpracovatelé zpracovávají údaje po stejnou dobu jako zpracovatel.

Příloha III - Technická a organizační opatření

Šifrování a pseudonymizace

- přenos dat výhradně přes TLS 1.2 nebo vyšší, HSTS na doméně kvitano.cz;
- šifrování uložených dat (AES-256) u poskytovatelů databáze, úložiště a záloh;
- zálohy navíc šifrovány před odesláním (AGE, X25519); dešifrovací klíč je uložen mimo infrastrukturu služby;
- po zrušení uživatelského účtu se osobní údaje uživatele do 30 dnů vymažou a vazba záznamů na jeho osobu se odstraní (pseudonymizace).

Důvěrnost, oddělení zákazníků a řízení přístupu

- oddělení dat zákazníků na úrovni databáze (Row Level Security);
- oprávnění per uživatel a klient z jediného místa v aplikaci, každá zapisující operace deklaruje potřebné oprávnění a soulad hlídá automatický test;
- hesla nejméně 12 znaků s kontrolou síly hesla a kontrolou proti databázi uniklých hesel (Have I Been Pwned, bez odeslání hesla), omezení počtu pokusů o přihlášení a ověření druhého faktoru;
- dvoufázové ověření (TOTP) se záložními kódy, povinné pro role s právem zápisu, a odhlášení ze všech zařízení;
- přihlašovací cookies nedostupné skriptům (HttpOnly, Secure, SameSite);
- přístup zpracovatele k datům mimo aplikaci (správa, obnova ze zálohy, řešení požadavku) jen v nezbytném rozsahu, s uvedením důvodu v auditním záznamu.

Integrita a záznam událostí

- doklady se ukládají jednou a nelze je přepsat; u každého se ukládá otisk SHA-256 s časem archivace a aplikace umožňuje ověřit neporušenost;
- každá změna údajů dokladu, položky nebo rozkladu DPH se zaznamenává (kdo, kdy, z čeho na co) a záznam přetrvá i smazání dokladu;
- zaznamenávají se exporty do účetního systému (kdo, kdy, které doklady).

Dostupnost a obnova

- týdenní šifrované zálohy celé databáze a úložiště dokladů (uchování 12 týdnů) a měsíční archiv v úložišti se zámkem proti smazání (10 let), oboje v EU;
- automatické ověření záloh, upozornění na selhání i nespustění zálohy, nástroj pro obnovu;
- sledování dostupnosti služby.

Minimalizace a omezení uchování

- veřejným registrům (ARES, registr plátců DPH) se předává jen IČO nebo DIČ dodavatele;
- hlášení chyb neobsahují osobní údaje;
- obrázky z podpisů e-mailů (loga, ikony) se nezpracovávají;
- výmaz po skončení smlouvy podle článku 2.5.

Umělá inteligence

- vytěžení dokladů běží v regionu Google Cloud europe-west4 (Nizozemsko) v režimu bez tréninku modelů na datech zákazníků; region je pevně nastaven v kódu služby;
- ukládání dotazů do mezipaměti (cache) u poskytovatele modelu je pro projekt služby vypnuté;
- pravidla a naučené návrhy zařazení položek se vedou per klient správce a mezi zákazníky se nesdílejí.

Vývoj a provoz

- oddělené produkční a vývojové prostředí, reálná data jen v produkci;
- automatické testy a kontrola známých zranitelností závislostí před nasazením;
- dílčí zpracovatelé vybraní s ohledem na zabezpečení, se smlouvou o zpracování (příloha IV).

Pomoc správci (doložky 8 a 9)

- žádosti subjektů údajů: správce může údaje dokladů sám vyhledat, opravit, exportovat i smazat přímo ve službě; s dalšími požadavky zpracovatel pomůže do 10 pracovních dnů od žádosti;
- porušení zabezpečení: oznámení podle článku 2.2 smlouvy obsahuje údaje podle doložky 9.2 a seznam dotčených klientů správce a dokladů, je-li možné je určit;
- posouzení vlivu: zpracovatel na žádost poskytne popis zpracování, opatření a dílčích zpracovatelů.

Příloha IV – Seznam dílčích zpracovatelů

Správce povolil využití těchto dílčích zpracovatelů (doložka 7.7, obecné povolení). Kde je dílčí zpracovatel americkou společností nebo může data zpřístupnit z USA (provoz, podpora), kryje případné předání jeho smlouva o zpracování na základě rámce EU–USA pro ochranu osobních údajů (Data Privacy Framework) nebo standardních smluvních doložek podle čl. 46 odst. 2 nařízení (EU) 2016/679.

- **Supabase, Inc.** (USA) – databáze, přihlašování uživatelů, úložiště dokladů. Data uložena v AWS eu-central-1 (Frankfurt, Německo). Všechny kategorie údajů. Přenos: standardní smluvní doložky.
- **Railway Corporation** (USA) – běh aplikačního serveru (API). Region EU West (Amsterdam, Nizozemsko). Všechny kategorie údajů při zpracování, trvale neukládá. Přenos: Data Privacy Framework, jinak standardní smluvní doložky.
- **Vercel Inc.** (USA) – webové rozhraní služby a předávání požadavků na API. Region fra1 (Frankfurt, Německo). Údaje při zpracování, trvale neukládá. Přenos: Data Privacy Framework, jinak standardní smluvní doložky.
- **Google Cloud EMEA Limited** (Irsko), poskytovatel Google LLC (USA) – vytěžení dokladů umělou inteligencí (Vertex AI, model Gemini) a záložní rozpoznání textu (Document AI). Region europe-west4 (Nizozemsko), resp. EU endpoint. Obrázek a text dokladu, bez tréninku modelů. Přenos: standardní smluvní doložky ve smlouvě o zpracování Google Cloud.
- **Cloudflare, Inc.** (USA) – DNS, příjem e-mailů na příjmové adresy služby, úložiště šifrovaných záloh (R2, jurisdikce EU). Příchozí e-maily zpracovává na své globální síti při doručení. Přenos: Data Privacy Framework, jinak standardní smluvní doložky.

- **Sendinblue SAS (Brevo)** (Francie) – odesílání e-mailů služby (pozvánky, ověření účtu, upozornění). E-mailová adresa příjemce a obsah upozornění.