

Táto zmluva upravuje, ako spracúvame osobné údaje, ktoré do služby HACCP Denník vložíte vy alebo vaši zamestnanci. Uzatvára sa podľa článku 28 ods. 3 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 (ďalej len **GDPR**) a zákona č. 18/2018 Z. z. o ochrane osobných údajov.

Tvorí neoddeliteľnú súčasť Všeobecných obchodných podmienok. Uzatvárate ju spolu s nimi, teda vytvorením účtu — vrátane bezplatného skúšobného obdobia. Nepodpisuje sa. Ak potrebujete podpísané vyhotovenie do svojej zložky GDPR, na požiadanie ho vystavíme.

Článok 1 — Zmluvné strany

Prevádzkovateľ ste vy — podnikateľ, ktorý si službu objednal a ktorý určuje, ktoré osobné údaje sa do nej vložia a prečo. Vaše identifikačné údaje sú tie, ktoré ste uviedli pri registrácii a ktoré máte v účte.

Sprostredkovateľ sme my:

- [DOPLNIŤ: obchodné meno]
- Sídlo: [DOPLNIŤ: sídlo]
- IČO: [DOPLNIŤ: IČO], DIČ: [DOPLNIŤ: DIČ], IČ DPH: [DOPLNIŤ: IČ DPH]
- Zapísaný: [DOPLNIŤ: zápis v registri]
- Kontakt pre otázky ochrany údajov: [DOPLNIŤ: kontaktná e-mailová adresa]

Prevádzkujeme službu HACCP Denník na adrese haccp.bizpilot.sk.

Článok 2 — Prečo ste prevádzkovateľom vy a nie my

Toto rozdelenie nie je formalita. Rozhoduje o tom, kto za čo zodpovedá.

Vy ste zamestnávateľ. Vy rozhodujete, ktorí vaši ľudia budú do denníka zapisovať, pod akým menom, akú budú mať rolu a čo napíšu do popisu odchýlky. Vy máte zákonnú povinnosť viesť HACCP evidenciu a vy zodpovedáte za to, že ste svojich zamestnancov o spracúvaní ich údajov informovali.

My poskytujeme nástroj. Údaje spracúvame len preto, aby služba fungovala, a len tak, ako nám to ukladá táto zmluva. Nerozhodujeme o tom, čo sa do denníka zapíše.

Vo vzťahu k vašim vlastným údajom ako zákazníka — fakturačné údaje, prihlasovací e-mail majiteľa, komunikácia s podporou — sme prevádzkovateľom my. Tento vzťah upravujú Zásady spracovania osobných údajov, nie táto zmluva.

Článok 3 — Predmet, povaha, účel a trvanie spracúvania

Predmet. Spracúvanie osobných údajov, ktoré vy alebo vaši používatelia vložíte do služby, prípadne ktoré vzniknú jej používaním (napríklad čas zápisu, IP adresa pri prihlásení).

Povaha spracúvania. Zhromažďovanie, zaznamenávanie, usporadúvanie, uchovávanie, nahliadanie, vyhľadávanie, generovanie PDF zostáv, zálohovanie a obmedzenie spracúvania (prepnutie účtu do režimu len na čítanie). Spracúvanie je automatizované. Naši ľudia sa k údajom dostanú len vtedy, keď je to nevyhnutné na podporu, opravu chyby alebo údržbu.

Účel. Výhradne poskytovanie služby, teda:

1. vedenie HACCP evidencie — teploty, sanitácia, odchýlky, nápravné opatrenia, alergény,
2. preukázanie, kto a kedy záznam vykonal,
3. generovanie PDF zostáv pre kontrolu RÚVZ a RVPS,
4. prevádzka používateľských účtov, PIN prihlásení a spárovaných tabletov,
5. zabezpečenie služby — obmedzenie počtu pokusov o prihlásenie, auditný denník, riešenie incidentov,

6. spracovanie HACCP dokumentu, ktorý sami nahráte do modulu AI import.

Na nič iné. Údaje nepoužívame na vlastné účely, na marketing, na tréningovanie modelov strojového učenia ani ich nikomu nepredávame.

Trvanie. Po celý čas trvania zmluvy o poskytovaní služby vrátane skúšobného obdobia. Trvá aj vtedy, keď je účet prepnutý do režimu len na čítanie — v ňom sa nové záznamy neukladajú, ale evidencia je naďalej prístupná a PDF export funguje. Končí vysporiadaním podľa článku 13.

Článok 4 — Typ osobných údajov a kategórie dotknutých osôb

Kategória dotknutých osôb	Osobné údaje
Majiteľ, štatutár alebo kontaktná osoba prevádzkovateľa	Meno, e-mailová adresa (zároveň prihlasovacie meno), heslo výhradne v podobe kryptografického odtlačku, čas posledného prihlásenia, čas udelenia súhlasov, IP adresa a označenie prehliadača pri prihlásení. Pri fyzickej osobe — podnikateľovi aj obchodné meno a adresa prevzatá z Registra právnických osôb.
Zamestnanci a ďalšie osoby, ktoré zapisujú do denníka	Meno a priezvisko, rola (zamestnanec, vedúci, majiteľ), PIN o dĺžke 4 až 6 číslíc výhradne v podobe kryptografického odtlačku, farba avatara, dátum, do ktorého je prístup platný (brigádnici), čas každého zápisu, meno pripísané ku každému záznamu, IP adresa a označenie zariadenia pri prihlásení. Zamestnanci s vlastným prístupom majú aj e-mailovú adresu.
Osoby uvedené vo voľných textoch	Čokoľvek, čo používateľ napíše do popisu odchýlky, do nápravného opatrenia, do dôvodu storna alebo do dôvodu nesplnenia sanitačnej úlohy. Rozsah týchto údajov určujete výlučne vy. My ho vopred nevieme obmedziť.
Osoby zachytené na fotografii priloženej k odchýlke	Obrazový záznam, ak ho používateľ vyhotoví a priloží. Služba fotografie zamestnancov nevyžaduje ani neponúka — namiesto fotky používa iniciály a farbu.
Osoby uvedené v dokumente nahratom do modulu AI import	Meno, funkcia a podpis členov HACCP tímu, zodpovednej osoby, vedúceho prevádzky, adresa prevádzky — v rozsahu, v akom sú v dokumente, ktorý nahráte. Uložený je nahratý súbor, text z neho získaný a úryvky, na ktoré sa návrh nastavenia odvoláva.

Osobitné kategórie údajov. Služba nie je navrhnutá na spracúvanie údajov podľa článku 9 GDPR — teda ani na údaje o zdraví. Do denníka nepatria zdravotné preukazy, lekárske posudky ani záznamy o chorobách zamestnancov. Ak ich do služby napriek tomu vložíte, robíte to na vlastnú zodpovednosť.

Platobné údaje. Nespracúvame žiadne. Platí sa výhradne na faktúru prevodom. Systém neobsahuje platobnú bránu a neexistuje v ňom miesto, kam by sa dalo zadať číslo karty.

Článok 5 — Spracúvanie výhradne na základe pokynov

- Osobné údaje spracúvame len na základe vašich zdokumentovaných pokynov. Pokynom je táto zmluva, Všeobecné obchodné podmienky, nastavenia, ktoré si v službe zvolíte, a používanie jej funkcií.
- Ďalší pokyn nám môžete dať písomne alebo e-mailom na kontaktnú adresu uvedenú v článku 1. Ak si jeho splnenie vyžiada neprimeraný zásah do služby, dohodneme sa na podmienkach vopred.
- Ak by nás právo Európskej únie alebo Slovenskej republiky nútilo spracúvať údaje inak, oznámime vám to pred spracúvaním — okrem prípadu, keď je takéto oznámenie zakázané z dôvodu verejného záujmu.
- Ak sa domnievame, že váš pokyn porušuje GDPR alebo iný predpis o ochrane údajov, okamžite vás na to upozorníme a do vyriešenia ho nevykonáme.

Článok 6 — Mlčanlivosť

- K vašim údajom majú prístup len osoby, ktoré ho nevyhnutne potrebujú na plnenie svojich úloh — úzky okruh určených ľudí na našej strane.

2. Všetky tieto osoby sú písomne zaviazané mlčanlivosťou a poučené o povinnostiach podľa GDPR. Závazok mlčanlivosti trvá aj po skončení ich pracovného alebo obdobného vzťahu.
3. Prístup do produkčného prostredia je evidovaný.
4. Heslá a PIN kódy sú uložené len ako kryptografické odtlačky. Neexistuje spôsob, ako ich zobrazíť späť — ani pre nás, ani pre vás. Zabudnutý PIN sa nedá vyhľadať, len nastaviť nový.

Článok 7 — Bezpečnosť spracúvania

Prijali sme technické a organizačné opatrenia primerané riziku podľa článku 32 GDPR. Ich úplný zoznam je v **Prílohe č. 2**, ktorá je súčasťou tejto zmluvy a slúži vám ako podklad pre vlastnú dokumentáciu.

Najpodstatnejšie z nich:

- Údaje jednotlivých zákazníkov sú oddelené na úrovni databázy. Príslušnosť k firme sa nikdy neurčuje z požiadavky prehliadača, len z overenej relácie alebo z tokenu spárovaného tabletu.
- Záznamy evidencie sa nedajú prepísať ani zmazať. Oprava sa robí stornom pôvodného riadku a novým záznamom; pôvodný zostáva a v PDF je prečiarknutý.
- Časové pečiatky sú vždy serverové, nikdy z tabletu.
- Heslá a PIN kódy sú hashované algoritmom argon2id.
- Nahraté súbory ležia mimo webového priečinka, pod náhodnými názvami, a vydajú sa len po overení, že patria vašej firme.
- Prenos medzi prehliadačom a serverom je šifrovaný.

Opatrenia priebežne vyhodnocujeme a môžeme ich meniť, ak tým neznížime dosiahnutú úroveň ochrany.

Článok 8 — Ďalší sprostredkovatelia

1. Udeľujete nám **všeobecné písomné povolenie** podľa článku 28 ods. 2 GDPR zapojiť do spracúvania ďalších sprostredkovateľov.
2. Aktuálny zoznam je v **Prílohe č. 1** a je trvalo zverejnený na tejto stránke.
3. Každú zamýšľanú zmenu — pridanie nového sprostredkovateľa alebo nahradenie doterajšieho — vám oznámime **najmenej 30 dní vopred** e-mailom na adresu majiteľa účtu a zverejníme ju v Prílohe č. 1.
4. Proti zmene môžete do 30 dní od oznámenia **namietat**. Ak námietku neodstránime iným riešením, môžete zmluvu vypovedať ku dňu účinnosti zmeny; vrátime vám pomernú časť vopred zaplateného predplatného a evidencia vám zostane dostupná na stiahnutie.
5. Každému ďalšiemu sprostredkovateľovi ukladáme zmluvne rovnaké povinnosti ochrany údajov, aké máme voči vám. Za ich plnenie zodpovedáme, akoby sme spracúvanie vykonávali sami.

Poskytovateľ jazykového modelu — osobitné pravidlá

Poskytovateľ jazykového modelu je zapojený **výhradne pri funkcii AI import** a výhradne na dokumenty, ktoré do nej sami nahráte. Platí:

- Bez použitia tejto funkcie sa poskytovateľovi neodošle nič. Nič nebeží na pozadí.
- Odosielame obsah nahratého dokumentu — text, prípadne obrázok strany pri skenovanom dokumente. Slovenské HACCP plány bežne obsahujú mená členov HACCP tímu, zodpovednej osoby a podpisy. **Tieto údaje neanonymizujeme ani nemaskujeme**. Dokument sa odošle tak, ako ste ho nahrali.
- Neodosielame názov vašej firmy z našej databázy, mená vašich používateľov, e-mailové adresy, IP adresy ani identifikátory relácie. Ani vaše existujúce nastavenie prevádzky — porovnanie s ním prebieha až po odpovedi u nás.
- Funkciu vôbec nemusíte použiť. Na vašu žiadosť ju vo vašom účte natrvalo vypneme; potom sa k poskytovateľovi modelu nedostane žiadny váš údaj.
- Aktívny je vždy len jeden poskytovateľ modelu. Ktorý, je uvedené v Prílohe č. 1.

Článok 9 — Prenos do tretích krajín

1. Vaše údaje sú uložené a spracúvané na serveroch umiestnených v [DOPLNIŤ: krajina umiestnenia serverov].
2. K prenosu mimo Európskeho hospodárskeho priestoru dochádza len v prípadoch výslovne uvedených v Prílohe č. 1, teda pri funkcii AI import a pri načítaní javascriptovej knižnice do prehliadača.
3. Ak funkciu AI import nepoužijete, obsah vašej evidencie neopustí krajinu uvedenú v bode 1.
4. Právnym základom prenosu je [DOPLNIŤ: rozhodnutie o primeranosti alebo štandardné zmluvné doložky podľa čl. 46 GDPR]. Kópiu príslušnej dokumentácie vám na požiadanie poskytneme.
5. Do tretej krajiny neprenášame žiadne údaje nad rámec uvedený v Prílohe č. 1.

Článok 10 — Pomoc pri právach dotknutých osôb

1. Žiadosti dotknutých osôb vybavujete vy. Vaši zamestnanci sa obracajú na vás ako na svojho zamestnávateľa, nie na nás.
2. Ak sa dotknutá osoba obráti priamo na nás, žiadosť **nevybavíme**. Bez zbytočného odkladu ju postúpime vám a osobu na to upozorníme.
3. Poskytneme vám primeranú súčinnosť — technické vyhľadanie údajov konkrétnej osoby, výpis, opravu tam, kde je technicky možná, a informácie o tom, kde sa údaje v službe nachádzajú.
4. **Obmedzenie, ktoré musíte poznať vopred:** záznamy evidencie sa zásadne neprepisujú a nemažú. Je to dôkazná evidencia — prepísaný dôkaz je bezcenný. Opravu vykonáme stornom a novým záznamom, pôvodný riadok zostáva viditeľný. Právo na opravu a na výmaz preto v tejto časti nevieme uplatniť prepísaním údajov. Uchovávanie je v tomto rozsahu potrebné na splnenie vašej zákonnej povinnosti viesť HACCP evidenciu.
5. **Export vlastných údajov máte dostupný kedykoľvek.** PDF zostavy si viete vygenerovať sami, počas celého trvania zmluvy aj vtedy, keď je účet v režime len na čítanie. Vaše dáta nikdy nedržíme ako páku.
6. Strojovo čitateľný export údajov služba zatiaľ neponúka samoobslužne. Na vašu písomnú žiadosť vám pripravíme kópiu vašich údajov v strojovo čitateľnom formáte, spravidla do 30 dní.
7. Súčinnosť v bežnom rozsahu je bezplatná. Pri opakovaných alebo neprimerane rozsiahlych žiadostiach sa dohodneme na náhrade skutočných nákladov vopred.

Článok 11 — Pomoc pri povinnostiach podľa článkov 32 až 36 GDPR

So zreteľom na povahu spracúvania a informácie, ktoré máme k dispozícii, vám poskytneme súčinnosť pri plnení vašich povinností:

1. **Bezpečnosť spracúvania (čl. 32).** Príloha č. 2 je pripravená tak, aby ste ju vedeli priložiť do vlastnej dokumentácie.
2. **Porušenie ochrany údajov (čl. 33 a 34).** Postup je v článku 12.
3. **Posúdenie vplyvu na ochranu údajov (čl. 35).** Na požiadanie vám poskytneme opis spracovateľských operácií, prijatých opatrení, zoznam ďalších sprostredkovateľov a informácie o umiestnení údajov.
4. **Predchádzajúca konzultácia s dozorným orgánom (čl. 36).** Poskytneme podklady, ktoré na konzultáciu potrebujete.
5. Ak sa na nás obráti Úrad na ochranu osobných údajov Slovenskej republiky vo veci týkajúcej sa vašich údajov, bez zbytočného odkladu vás o tom informujeme — okrem prípadu, keď nám to právo zakazuje.

Článok 12 — Ohlasovanie porušenia ochrany osobných údajov

1. Ak zistíme porušenie ochrany osobných údajov, ktoré sa týka údajov spracúvaných pre vás, oznámime vám to bez zbytočného odkladu, **najneskôr do [DOPLNIŤ: hodín] hodín** od chvíle, keď sme sa o ňom dozvedeli.
2. Oznámenie pošleme e-mailom na adresu majiteľa účtu. Ak je vec naliehavá, skúsime vás zastihnúť aj telefonicky na čísle uvedenom v účte.

3. Oznámenie obsahuje:
 - opis povahy porušenia,
 - kategórie a približný počet dotknutých osôb a záznamov,
 - čas, kedy k porušeniu došlo, a čas, kedy sme sa o ňom dozvedeli,
 - meno a kontakt osoby, ktorá vám poskytne ďalšie informácie,
 - opis pravdepodobných následkov,
 - opis prijatých a navrhovaných opatrení vrátane opatrení na zmiernenie následkov.
4. Ak nemáme všetky informácie naraz, pošleme ich postupne, ako ich zistíme. Nečakáme s prvým oznámením na úplný obraz.
5. **Ohlásenie Úradu na ochranu osobných údajov a oznámenie dotknutým osobám robíte vy.** My vám na to dodáme podklady. Za vás nekonáme, ak sa nedohodneme inak.
6. O porušeních vedíme vlastnú evidenciu a na požiadanie vám z nej poskytneme výpis týkajúci sa vašich údajov.
7. Oznámenie podľa tohto článku nie je uznaním zodpovednosti.

Článok 13 — Vymazanie alebo vrátenie údajov po skončení zmluvy

1. Po skončení poskytovania služby si **vyberiete vy**, či vám údaje vrátime, alebo ich vymažeme. Voľbu nám oznámte písomne alebo e-mailom.
2. **Kým sa nerozhodnete, nič nemažeme.** Účet zostane v režime len na čítanie: prihlásite sa, vidíte celú evidenciu a PDF export vám funguje ďalej. Viesť HACCP evidenciu je vaša zákonná povinnosť a my z nej nerobíme páku.
3. **Vrátenie** znamená PDF zostavy za zvolené obdobie, ktoré si viete stiahnuť sami, a na žiadosť aj kópiu údajov v strojovo čitateľnom formáte podľa článku 10 bodu 6.
4. **Výmaz** vykonáme do 30 dní od vašej žiadosti a písomne ho potvrdíme. Týka sa databázových záznamov vrátane auditného denníka aj nahratých súborov na úložisku. Služba dnes nemá samoobslužné tlačidlo na mazanie účtu — výmaz vykonáme na vašu žiadosť zásahom na strane servera.
5. Po vykonaní výmazu sú údaje nenávratne stratené. Zostavy, ktoré si chcete ponechať, si stiahnite pred podaním žiadosti.
6. Výnimkou z výmazu sú:
 - kópie v zálohách, ktoré zanikajú uplynutím zálohovacieho cyklu — [DOPLNIŤ: dĺžka zálohovacieho cyklu]; do ich zániku ostávajú chránené touto zmluvou a nepoužívajú sa na iný účel než obnovu,
 - údaje, ktoré musíme uchovať podľa právneho predpisu, najmä účtovné doklady; tie spracúvame ako prevádzkovateľ podľa Zásad spracovania osobných údajov.
7. Uchovávanie údajov počas trvania zmluvy sa riadi vašou zákonnou povinnosťou viesť HACCP evidenciu a lehotami, ktoré ste si zvolili — [DOPLNIŤ: retenčné lehoty zvolené prevádzkou]. Prevádzkové technické údaje (záznamy o prihláseniach, IP adresy, auditný denník) uchovávame po dobu trvania zmluvy.

Článok 14 — Audit a preukázanie súladu

1. Na vašu písomnú žiadosť vám poskytneme informácie potrebné na preukázanie súladu s článkom 28 GDPR: Prílohu č. 2, aktuálny zoznam ďalších sprostredkovateľov, informácie o umiestnení údajov a odpovede na primeraný bezpečnostný dotazník. Vo väčšine prípadov to postačuje.
2. Ak vám to nestačí, máte právo na audit alebo kontrolu na mieste. Platí pre ne:
 - najviac raz za dvanásť mesiacov, oznámené najmenej 30 dní vopred,
 - v pracovných dňoch a v pracovnom čase, tak aby nenarušili prevádzku služby,
 - audítor musí byť viazaný mlčanlivosťou a nesmie byť naším konkurentom.
3. Bez obmedzenia počtu a lehoty môžete audit vykonať po porušení ochrany údajov, ktoré sa vás dotklo, alebo ak vám to uloží dozorný orgán.

4. Nesprístupníme vám údaje iných zákazníkov, prístupové kľúče, heslá ani informácie, ktorých zverejnenie by ohrozilo bezpečnosť služby. To nie je výhovorka — je to tá istá ochrana, akú poskytujeme vám voči ostatným.
5. Náklady auditu znášate vy. Ak audit zistí podstatné porušenie tejto zmluvy na našej strane, znášame ich my.
6. Rovnaké pravidlá uplatňujeme voči našim ďalším sprostredkovateľom a výsledky, ktoré sa týkajú vašich údajov, vám na požiadanie sprístupníme.

Článok 15 — Zodpovednosť

1. Každá strana zodpovedá za škodu spôsobenú porušením GDPR podľa článku 82 GDPR.
2. Zodpovedáte za zákonnosť údajov, ktoré do služby vložíte — najmä za právny základ ich spracúvania a za to, že ste dotknuté osoby informovali podľa článkov 13 a 14 GDPR.
3. Zodpovedáme za to, že spracúvame len podľa vašich pokynov a že sme prijali opatrenia podľa článku 7 a Prílohy č. 2.
4. Ak jednej strane vznikne sankcia alebo povinnosť nahradiť škodu, ktorú zavinila druhá strana, majú voči sebe nárok na vyrovnanie v rozsahu svojho podielu na zodpovednosti.
5. Poskytneme si vzájomnú súčinnosť pri konaní pred dozorným orgánom alebo súdom.

Článok 16 — Trvanie, zmeny a účinnosť

1. Zmluva nadobúda účinnosť dňom vytvorenia účtu, teda aj na začiatku bezplatného skúšobného obdobia, a to bez ohľadu na to, či ste už za službu zaplatili.
2. Trvá po celý čas poskytovania služby a jej platnosť sa predlžuje o čas potrebný na vysporiadanie podľa článku 13.
3. Zmeny tejto zmluvy vám oznámime najmenej 30 dní vopred e-mailom na adresu majiteľa účtu a zverejníme ich na tejto stránke. Ak so zmenou nesúhlasíte, môžete zmluvu vypovedať ku dňu jej účinnosti; vrátime vám pomernú časť predplatného.
4. Zmena, ktorá je len spresnením textu, opravou zrejmej chyby alebo priamym dôsledkom zmeny právneho predpisu či rozhodnutia dozorného orgánu, môže nadobudnúť účinnosť aj skôr. Aj takú zmenu vám oznámime.
5. Aktualizácia Prílohy č. 1 sa riadi článkom 8, nie týmto článkom.
6. Ak sú Všeobecné obchodné podmienky a táto zmluva v otázkach ochrany osobných údajov v rozpore, prednosť má táto zmluva.

Článok 17 — Záverečné ustanovenia

1. Zmluva sa riadi právom Slovenskej republiky, najmä GDPR a zákonom č. 18/2018 Z. z. Spory patria príslušným súdom Slovenskej republiky.
2. Uzatvára sa elektronicky a bez podpisu. Na požiadanie vám vystavíme podpísané vyhotovenie v PDF.
3. Aktuálne znenie je vždy dostupné na tejto stránke a na stiahnutie v PDF, aby ste ho vedeli založiť do vlastnej dokumentácie a predložiť pri kontrole.
4. Ak sa niektoré ustanovenie stane neplatným, ostatné zostávajú v platnosti. Neplatné ustanovenie sa nahradí takým, ktoré je mu najbližšie účelom.
5. Prílohy č. 1 a č. 2 sú neoddeliteľnou súčasťou tejto zmluvy.

Príloha č. 1 — Zoznam ďalších sprostredkovateľov

Stav ku dňu uvedenému pri tomto dokumente. Zmeny oznamujeme podľa článku 8.

Ďalší sprostredkovateľ	Čo pre nás robí	Aké údaje spracúva	Kde spracúva
[DOPLNIŤ: obchodné meno poskytovateľa hostingu], [DOPLNIŤ: sídlo poskytovateľa hostingu]	Prevádzka servera, databázy a úložiska nahratých súborov	Všetky údaje uložené v službe	[DOPLNIŤ: krajina umiestnenia serverov]
[DOPLNIŤ: obchodné meno poskytovateľa e-mailovej služby], [DOPLNIŤ: sídlo poskytovateľa e-mailovej služby]	Odosielanie systémových správ — overenie e-mailu, obnova hesla, upozornenia, odoslané zostavy	E-mailová adresa a meno adresáta, obsah správy vrátane priložených PDF zostáv s menami zamestnancov	[DOPLNIŤ: krajina spracúvania]
Google (rozhranie Gemini API)	Prečítanie HACCP dokumentu nahratého do modulu AI import a návrh nastavenia prevádzky. Zapojený len pri tejto funkcii a len na dokumenty, ktoré nahráte.	Obsah nahratého dokumentu — text, prípadne obrázok strany. Môže obsahovať mená, funkcie a podpisy osôb uvedených v dokumente. Nič z našej databázy sa neodosiela.	Mimo EHP — Spojené štáty americké a ďalšie krajiny podľa infraštruktúry poskytovateľa
Anthropic (rozhranie Claude API)	Tá istá funkcia ako vyššie. Použije sa ako náhrada, nie súčasne.	Rovnaký rozsah ako vyššie	Mimo EHP — Spojené štáty americké

Poznámky k zoznamu:

- Poskytovateľ jazykového modelu je v danom čase aktívny **vždy len jeden**. Ak nie je nastavený žiadny, modul AI import je nedostupný a neodosiela sa nič.
- Ak modul AI import nepoužijete alebo si ho dáte vypnúť, poskytovateľ modelu nespracúva žiadne vaše údaje.
- **Štatistický úrad Slovenskej republiky** nie je naším ďalším sprostredkovateľom. Pri registrácii mu odošleme výhradne vaše IČO a z verejného Registra právnických osôb prevzmememe názov, právnu formu a adresu. Úrad je samostatným prevádzkovateľom tohto registra.
- Platobná brána v zozname nie je, pretože žiadnu nepoužívame.

Príloha č. 2 — Technické a organizačné opatrenia

Opis opatrení podľa článku 32 GDPR. Je napísaný tak, aby ste ho vedeli priložiť do vlastnej dokumentácie a predložiť pri kontrole.

1. Riadenie prístupu

- Heslá sú hashované algoritmom **argon2id**. V databáze ani v zálohách neexistuje čitateľné heslo.
- Minimálna dĺžka hesla je 10 znakov, s čiernou listinou bežných hesiel a zákazom hesla odvodeného z e-mailovej adresy.
- PIN kódy zamestnancov (4 až 6 číslic) sú hashované tým istým algoritmom. **Neexistuje cesta, ako PIN zobrazíť späť**. Triviálne PIN kódy sú odmietnuté a PIN musí byť v rámci firmy jedinečný.
- Neúspešné prihlásenia sú obmedzené počtom pokusov za časové okno — osobitne pre IP adresu, účet aj PIN. Opakované chybné zadanie PIN kódu zariadenie zamkne a zapíše sa do auditného denníka.
- Brigádnikovi sa dá nastaviť dátum, po ktorom sa už neprihlási.
- Odhlásenie zo všetkých zariadení je okamžité a vynúti sa po každej zmene hesla.
- Roly: zamestnanec, vedúci, majiteľ. Oprávnenia sa overujú na strane servera, nielen skrytím položky v ponuke.

2. Oddelenie údajov zákazníkov

- Každý dátový riadok nesie identifikátor firmy. Ten sa **nikdy** neurčuje z požiadavky prehliadača, formulára ani parametra v adrese — len z overenej relácie alebo z tokenu spárovaného tabletu.

- Všetky databázové dotazy prechádzajú jednou vrstvou, ktorá príslušnosť k firme dopĺňa automaticky. Je to jediné miesto v celom systéme, kde sa vykonáva SQL.
- Objekt načítaný podľa identifikátora sa overuje proti firme. Cudzí objekt vráti „nenájdene“, nie „nemáte právo“ — aby sa nedalo zistiť, že taký záznam vôbec existuje.
- Dodržanie tohto pravidla kontroluje automatický nástroj pri každom spustení testov. Na každý koncový bod je napísaný test overujúci, že firma A nevidí údaje firmy B.

3. Integrita a nepopierateľnosť záznamov

- Záznamové tabuľky sú **append-only**: zápis sa nedá zmeniť ani odstrániť. Pokus o to systém odmietne.
- Oprava = storno pôvodného riadku s uvedením dôvodu a osoby + nový záznam. Pôvodný riadok zostáva a v PDF je prečiarknutý.
- Časové pečiatky sú vždy serverové. Zápis so starším dátumom udalosti je označený ako spätný zápis a je ohraničený počtom dní nastaveným pre firmu (najviac 7).
- Meno zapisovateľa sa ku každému záznamu ukladá natrvalo, aby zostalo čitateľné aj po odchode zamestnanca.
- Každú noc sa nad záznamami dňa vypočíta kryptografický odtlačok, ktorý sa reťazí s odtlačkom predchádzajúceho dňa. V pätičke PDF je verifikačný kód obdobia. **Nie je to dôkaz voči nám** — kto ovláda server, vie prepočítať aj reťaz. Je to dôkaz voči tichej dodatočnej zmene záznamu.
- Auditný denník zaznamenáva prihlásenia, zmeny nastavení a bezpečnostné udalosti.

4. Ochrana prenosu a relácií

- Prenos medzi prehliadačom a serverom je šifrovaný.
- Prihlasovacia cookie obsahuje **len náhodný identifikátor**, žiadne údaje. Obsah relácie je uložený na serveri.
- Cookie je neprístupná pre skripty, s obmedzením na vlastnú doménu a v produkcii len cez zabezpečené spojenie.
- Ochrana proti podvrhnutiu požiadavky (CSRF) je zapnutá globálne nad celou aplikáciou, nie len na vybraných miestach.

5. Nahraté súbory

- Ukladajú sa **mimo webového priečinka**, pod náhodnými názvami, s obmedzenými prístupovými právami.
- Typ súboru sa overuje podľa jeho skutočného obsahu, nie podľa prípony. K odchýlke sa nedá podstrčiť iný typ súboru, než aký je povolený.
- Platia limity veľkosti a ochrana proti súboru, ktorý sa po rozbalení neúmerne zväčší.
- Súbor sa vydá len cez prihlásený koncový bod, ktorý overí, že patrí vašej firme. Priamy odkaz na súbor neexistuje.

6. Ochrana databázy

- Všetky dotazy sú parametrizované. Názvy tabuliek a stĺpcov sa overujú proti pevnému zoznamu a nikdy nepochádzajú zo vstupu používateľa.
- Prístupové kľúče k externým službám sú uložené len v konfigurácii servera. Cez používateľské rozhranie sa nedajú nastaviť, takže neležia v databáze ani v zálohách.
- Aplikácia sa v produkčnom režime odmietne spustiť bez nastaveného tajného kľúča.

7. Minimalizácia údajov

- Fotografie zamestnancov sa neukladajú vôbec. Namiesto nich sa používajú iniciály a farba.
- Pri neúspešnom prihlásení sa do auditného denníka neukladá zadaná e-mailová adresa.
- V tabuľke obmedzenia pokusov nie je e-mailová adresa čitateľná — je nahradená odtlačkom. Tabuľka teda nie je zoznamom skúšaných adries.
- Nespracúvame platobné karty, geolokáciu, biometriu ani odtlačok zariadenia.

- Nepoužívame analytiku, meracie kódy ani marketingové skripty — v systéme nie je ani jeden.
- Používame dve cookies, obe vlastné a nevyhnutné: prihlásenie a identifikácia spárovaného tabletu. Žiadne analytické ani marketingové cookies.

8. Dostupnosť a obnova

- Zálohovanie: [DOPLNIŤ: frekvencia záloh, spôsob uloženia a doba uchovania].
- Overenie obnovy zo zálohy: [DOPLNIŤ: periodicita testu obnovy].
- Zamknutý alebo nezaplatený účet zostáva v režime len na čítanie. Evidencia a PDF export fungujú ďalej — dostupnosť vašich dôkazov nie je viazaná na platbu.

9. Organizačné opatrenia

- Prístup k produkčnému prostrediu má len úzky okruh určených osôb, písomne zaviazaných mlčanlivosťou.
- Účet správcu systému je vedený mimo bežnej tabuľky používateľov; bez nastavených prístupových údajov je celá správcovská sekcia nedostupná.
- Zmeny databázovej schémy sa vykonávajú len číslovanými migračnými skriptami, nikdy ručným zásahom.
- Testy vrátane kontrol oddelenia údajov zákazníkov sa spúšťajú pri každej zmene.

Papier funguje, ale má dve slabiny. Na vytlačenej tabuľke nikto nevidí, že sa tri dni nezapisovalo — prázdny riadok vyzerá rovnako ako ten, ktorý sa doplní zajtra. A prepísané číslo sa nedá odlíšiť od pôvodného.

HACCP Denník vedie tie isté záznamy digitálne: zápis trvá desať sekúnd na tablete, oprava je vždy nový záznam a pôvodný zostáva prečiarknutý aj s dôvodom. Pre kontrolu vytlačíte hotové PDF na jeden klik.

14 dní zadarmo, bez platobnej karty — haccp.bizpilot.sk