

Договор за обработка на лични данни (DPA)

съгласно чл. 28 от ОПЗД – Auftragsverarbeitungsvertrag

1. Страни и обхват

Настоящият Договор за обработка на лични данни ("Договора") е част от споразумението между клиента ("Администратор") и TECHARENABG EOOD ("Обработващ", "ние", "InboxDoc") и урежда обработката на лични данни от Обработващия от името на Администратора във връзка с услугата за обработка на фактури InboxDoc.

2. Предмет и срок

Предмет на настоящия Договор е обработката на лични данни, извършвана от Обработващия от името на Администратора с цел предоставяне на услугата InboxDoc: сканиране на свързаните имейл акаунти на Администратора за съобщения с прикачени фактури, извличане на структурирани данни от фактури и предоставянето им в таблото на Администратора.

Настоящият Договор е в сила, докато Обработващият обработва лични данни от името на Администратора, и се прекратява автоматично при прекратяване на основното споразумение за услугата и след изтриване или връщане на всички лични данни съгласно т. 12.

3. Характер и цел на обработката

Обработващият обработва лични данни изключително с цел: свързване с посочените от Администратора имейл акаунти (Gmail, Outlook или IMAP) чрез предоставения от Администратора достъп; идентифициране на имейл съобщения, които съдържат или вероятно съдържат прикачени фактури или кредитни известия; извличане на структурирани данни от фактури от тези прикачени файлове (детерминистично от структуриран XML на електронна фактура, когато е наличен, или чрез извличане с помощта на изкуствен интелект от PDF файла в останалите случаи); както и съхранение, визуализиране и експортиране на извлечените структурирани данни чрез таблото на Администратора.

4. Категории лични данни

- Данни за акаунта на потребителите на Администратора (име, имейл адрес)
- Метаданни на сканирани имейли (подател, тема, дата)
- Данни, извлечени от фактури/кредитни известия (име на доставчик, номер на фактура, дати, суми, валута) - може инцидентно да съдържат лични данни, когато фактурата посочва физическо лице като доставчик или клиент
- OAuth токени за достъп/опресняване, или криптирана парола за приложение за IMAP, използвани единствено за поддържане на имейл връзката
- Приблизителна държава, извлечена еднократно от IP адреса при регистрация; самият IP адрес не се съхранява

5. Категории субекти на данни

Собствените потребители на акаунта на Администратора (напр. служители с достъп до таблото), както и трети лица, посочени във фактури, обработвани чрез услугата (напр. лица за контакт при доставчици, еднолични търговци, издаващи фактури на Администратора).

6. Права и задължения на Администратора

Администраторът остава единствено отговорен за законосъобразността на личните данни, които предоставя за обработка (включително свързаните имейл акаунти), и за отговорите на искания на субекти на данни, освен доколкото Обработващият е длъжен да съдейства съгласно т. 10. Администраторът носи отговорност за даването на документираните инструкции на Обработващия; настоящият Договор, заедно с обичайното използване на документираните функции на услугата от Администратора, представлява такава инструкция.

7. Задължения на Обработващия

- Обработващият обработва лични данни само въз основа на документираните инструкции от Администратора, включително относно международни трансфери на данни, освен ако не е длъжен да постъпи по друг начин съгласно правото на ЕС или на държава членка.
- Обработващият гарантира, че лицата, оправомощени да обработват лични данни, са поели задължение за поверителност.
- Обработващият не съхранява изходни файлове (прикачени PDF файлове или XML файлове на електронни фактури) - съхраняват се единствено извлечените от тях структурирани данни.
- Обработващият прилага техническите и организационните мерки, описани в т. 8.
- Обработващият не ангажира друг обработващ (подизпълнител) без предварително общо разрешение от Администратора, което Администраторът дава с настоящото за подизпълнителите, изброени в т. 9; Обработващият информира Администратора за всякакви планирани промени относно добавянето или замяната на подизпълнители, като дава на Администратора възможност да възрази.

8. Технически и организационни мерки (ТОМ)

- Криптиране на OAuth токени и IMAP пароли за приложения в покой; HTTPS/TLS за цялото предаване на данни
- Row-Level Security в базата данни, така че всеки клиент има достъп единствено до собствените си данни
- Без съхранение на изходни PDF/XML файлове - съхраняват се само извлечените структурирани данни (вижте Политиката за поверителност)
- Достъп до Gmail/Outlook единствено чрез OAuth права с минимално необходимите разрешения; пароли за Gmail/Outlook никога не се изискват или съхраняват (IMAP паролите за приложения се криптират и никога не се съхраняват в явен текст)
- Налична двуфакторна автентикация (MFA) за достъп до акаунта
- Контрол на достъпа: вътрешният достъп до производствени данни е ограничен до лица, които се нуждаят от него за поддръжка/експлоатация
- Където е възможно, се използва детерминистично извличане без изкуствен интелект (структуриран XML на електронна фактура); извличането с изкуствен интелект се използва само като резервен метод и единствено върху самия документ, никога върху данни за достъп

9. Подизпълнители

Администраторът разрешава на Обработващия да ангажира следните подизпълнители:

- Supabase — хостинг на база данни, удостоверяване — ЕС (Ирландия, eu-west-1)
- Vercel Inc. — хостинг на приложението / serverless функции — ЕС (Дъблин, dub1; фиксирано)
- Cloudflare, Inc. — мрежов прокси/DNS
- Anthropic, PBC — извличане на данни от фактури с помощта на изкуствен интелект (само като резервен метод; не се използва за електронни фактури, обработвани чрез структуриран XML) — САЩ; гаранция за трансфер: стандартни договорни клаузи (чл. 46 от ОРЗД)
- Lemon Squeezy, Inc. (компания на Stripe) — обработка на плащания в качеството на "merchant of record"
- Google LLC — достъп до Gmail API (с изричното съгласие на Администратора); Google Analytics (GA4), само след съгласие за бисквитки — САЩ
- Microsoft Corporation — достъп до Outlook/Microsoft Graph API (с изричното съгласие на Администратора)

10. Съдействие при искания на субекти на данни

Предвид характера на обработката, Обработващият съдейства на Администратора, доколкото това е разумно възможно, за изпълнение на задължението му да отговаря на искания от субекти на данни, упражняващи правата си съгласно Глава III от ОРЗД. Когато субект на данни се обърне директно към Обработващия, той препраща искането към Администратора без неоправдано забавяне, освен ако не е инструктиран друго.

11. Уведомяване при нарушение на сигурността на личните данни

Обработващият уведомява Администратора без неоправдано забавяне, след като узнае за нарушение на сигурността на личните данни, засягащо данните на Администратора, и оказва разумно съдействие във връзка със собствените задължения на Администратора за уведомяване съгласно чл. 33/34 от ОРЗД.

12. Изтриване или връщане на данните след прекратяване

След прекратяване на основното споразумение за услугата Обработващият, по избор на Администратора, изтрива или връща всички лични данни, обработвани от името на Администратора, и изтрива съществуващите копия, освен ако правото на ЕС или на държава членка изисква продължаващо съхранение. Изтриването на акаунт, инициирано от Администратора чрез функцията за самообслужване "Изтриване на акаунт", незабавно и необратимо изтрива извлечените данни за фактури, отменя OAuth токените при съответния доставчик и изтрива данните за профила и известията, както е описано в Политиката за поверителност.

13. Право на контрол

Обработващият предоставя на Администратора цялата информация, необходима за доказване на спазването на задълженията по настоящия Договор и чл. 28 от ОРЗД, и допуска и съдейства при проверки, включително инспекции, извършвани от Администратора или одитор, упълномощен от него, при спазване на разумно предварително уведомление и поверителност.

14. Отговорност

Отговорността между страните във връзка с настоящия Договор се урежда от разпоредбите за отговорност на основните Общи условия.

15. Приложимо право

Настоящият Договор се урежда от правото на България и Общия регламент относно защитата на данните (ЕС) 2016/679.

TODO(legal-review): Настоящият документ е изготвен като проект въз основа на описаната ни техническа реализация; той все още не е прегледан от адвокат, специализиран в областта на защитата на данните, и не следва да се използва, подписва или изпраща на клиенти като обвързващ правен документ преди такъв преглед.