Divvly Privacy Policy

Last updated: January 25, 2026

> **This Privacy Policy** describes how we collect, use, and protect the personal data of users of the Divvly application and website at **www.divvly.app**.

1. Data Controller

ProWebDev

ul. Jarzębinowa 69

52-200 Karwiany, Poland

NIP: 639-194-31-91

Contact: support@divvly.app

1.1. About Divvly

Divvly enables users to:

- Split expenses among group members
- Track financial settlements
- Manage shared expenses
- Scan receipts with automatic data recognition (OCR)
- Get intelligent AI-powered expense categorization

- Convert currencies in real-time
- Use free and paid subscription tiers

---

2. What Data We Collect

2.1. Account Data

- Email address
- Username
- Password (stored encrypted using bcrypt)
- Profile picture (optional)
- Currency and language preferences

2.2. Social Login Data

When signing in with Google, Facebook, or Apple, we receive:

- Unique provider account identifier
- Email address
- Name (if shared)
- Profile picture (if shared)

2.3. Automatically Collected Data

- IP address
- Device identifiers
- Browser type and version
- Operating system
- Date and time of access
- Pages visited
- Referral source

2.4. Payment Data

- Transaction history
- Subscription information
- Stripe customer identifier

> **Important:** Payment card data (card number, expiration date, CVV) is **never stored** on our servers. Payments are processed directly by Stripe, a PCI DSS Level 1 certified payment provider.

2.5. Application Usage Data

- Expense and group information
- Category names and transaction descriptions
- Scanned receipts (processed via OCR and AI)
- Imported CSV files

2.6. Push Notification Data

- Device tokens (for sending notifications)
- Device platform (Web, iOS, Android)
- Notification preferences

3. Legal Basis for Processing

We process your personal data based on the following legal grounds under GDPR:

Purpose	Legal Basis (GDPR Article 6)
Providing services (account, app functionality)	Performance of a contract (Art. 6(1)(b))

Payment processing	Performance of a contract (Art. 6(1)(b))
Marketing and newsletters (with consent)	Consent (Art. 6(1)(a))
Analytics and service improvement	Legitimate interest (Art. 6(1)(f))
Security and fraud prevention	Legitimate interest (Art. 6(1)(f))
Tax and accounting compliance	Legal obligation (Art. 6(1)(c))

---

4. How We Use Your Data

1. **Service delivery** – Enable expense splitting, group management, and settlements
2. **Account management** – Registration, login, settings
3. **Payment processing** – Handle transactions and subscriptions via Stripe
4. **Receipt scanning** – Automatically extract data from receipts using OCR
5. **Expense categorization** – AI-powered category suggestions
6. **Currency conversion** – Fetch real-time exchange rates
7. **Communication** – Respond to inquiries, system notifications
8. **Push notifications** – Alert about new expenses, settlements, invitations
9. **Analytics** – Improve service quality and user experience
10. **Security** – Protect against unauthorized access and abuse
11. **Legal obligations** – Tax documentation and compliance

---

5. Cookies and Tracking

5.1. Cookie Consent Management – Cookiebot

We use **Cookiebot** (deployed via Google Tag Manager) to manage cookie consents. Upon your first visit, you will see a banner allowing you to:

- Accept all cookies
- Reject optional cookies
- Configure detailed preferences

You can change your preferences at any time via the "Cookie settings" link in the website footer.

5.2. Cookie Categories

Category	Description	Legal Basis
Necessary	Required for website operation (session, authentication, security)	Legitimate interest
Functional	Remember user preferences (language, currency)	Legitimate interest
Analytics	Google Tag Manager – visitor statistics and behavior analysis	Consent

5.3. Google Tag Manager

We use Google Tag Manager to manage tracking tags (including Cookiebot) and website analytics. GTM collects:

- Number of visits and users
- Time spent on site
- Entry and exit pages
- Traffic sources
- User interactions and events

5.4. Google reCAPTCHA v3

We use Google reCAPTCHA v3 to protect forms from automated attacks (spam, bots). reCAPTCHA may collect device data and interaction patterns to verify human users.

5.5. Session and Authentication

We use cookies to maintain user sessions (JWT). Sessions expire after 2 days of inactivity.

---

6. Third-Party Services

6.1. Social Login Providers (OAuth)

Provider	Data Shared	Privacy Policy
Google	ID, email, name, photo	policies.google.com/privacy
Facebook	ID, email, name	facebook.com/privacy/policy
Apple	ID, email, name (optional)	apple.com/privacy

6.2. Payment Processing – Stripe

Payments are processed by **Stripe, Inc.** Stripe processes:

- Payment card data
- Billing address
- Transaction history

Stripe is **PCI DSS Level 1** compliant. Privacy policy: stripe.com/privacy

6.3. Amazon Web Services (AWS)

We use the following AWS services:

Service	Purpose	Data Processed

AWS Hosting (EC2/ECS)	Backend application hosting	All application data
AWS S3	File storage (CSV imports)	User-uploaded files
AWS SES	Email delivery (notifications, confirmations)	Email addresses, message content
AWS Textract	OCR – receipt text recognition	Receipt images
AWS Bedrock (Claude AI)	Receipt analysis and category suggestions	Receipt data, expense descriptions

AWS servers are located in the **eu-central-1 (Frankfurt)** region. AWS holds ISO 27001, SOC 1/2/3 certifications and GDPR compliance.

6.4. Frontend Hosting – AWS Amplify

The website is hosted on **AWS Amplify**. Amplify is part of the Amazon Web Services ecosystem and processes technical data (IP addresses, request headers) for content delivery. Data is processed in the EU (Frankfurt) region.

6.5. Exchange Rates – FXRatesAPI

We use **FXRatesAPI** for currency conversion. This service only receives currency pair information – no personal user data is transmitted.

---

7. International Data Transfers

Some of our service providers are located outside the European Economic Area (EEA):

Provider	Location	Safeguards

Amazon Web Services	EU (Frankfurt)	Data processed within EEA
Google LLC	USA	Standard Contractual Clauses (SCC), Data Privacy Framework
Stripe, Inc.	USA	Standard Contractual Clauses (SCC), PCI DSS
Meta Platforms	USA	Standard Contractual Clauses (SCC)
Apple Inc.	USA	Standard Contractual Clauses (SCC)

8. Data Retention

Data Type	Retention Period
Account data	Until account deletion + 30 days backup
Expense and group data	Until account deletion
Transaction and accounting data	5 years (tax regulations)
Subscription data	Duration of subscription + 5 years
Server logs	90 days
Analytics data	26 months (Google default)
Receipt images (OCR)	Processed and deleted immediately after extraction
CSV import files	30 days after import completion

9. Your Rights

Under GDPR, you have the following rights:

- **Right of access** (Art. 15) – Request information about your data and obtain a copy
- **Right to rectification** (Art. 16) – Correct inaccurate or incomplete data
- **Right to erasure** (Art. 17) – Request deletion of your data ("right to be forgotten")
- **Right to restriction** (Art. 18) – Limit how we process your data
- **Right to data portability** (Art. 20) – Receive your data in a machine-readable format (JSON, CSV)
- **Right to object** (Art. 21) – Object to processing based on legitimate interest
- **Right to withdraw consent** – Withdraw consent at any time for consent-based processing
- **Right to lodge a complaint** – File a complaint with a supervisory authority

> **To exercise your rights, contact us at:** support@divvly.app
>
> We will respond within **30 days**. Complex requests may be extended by an additional 60 days.

9.1. Supervisory Authority

You may lodge a complaint with:

President of the Personal Data Protection Office (UODO)

ul. Stawki 2

00-193 Warsaw, Poland

Website: uodo.gov.pl

10. Artificial Intelligence and Automated Processing

10.1. OCR and Receipt Recognition

We use OCR technology (AWS Textract) to automatically extract data from receipt photos:

- Vendor name
- Purchase date
- Total amount and tax
- Line items

10.2. AI Category Suggestions

Our AI system (AWS Bedrock with Claude model) analyzes expense descriptions and suggests appropriate categories. The final category choice is always up to the user.

10.3. Automated Decision Making

We do not make decisions based solely on automated processing that would have legal effects or similarly significantly affect users.

11. Data Security

We implement appropriate technical and organizational security measures:

11.1. Technical Measures

- TLS/SSL encryption for all connections
- Data encryption at rest (AES-256)
- Regular backups
- Firewalls and intrusion detection
- Password hashing (bcrypt)

- Short-lived JWT tokens

11.2. Organizational Measures

- Access limited to authorized personnel only
- Security incident response procedures
- Regular security audits
- Data processing agreements with third parties

12. Required vs. Optional Data

12.1. Required Data

Some data is necessary to use our services:

- **Account creation** – Email and password (or social login via Google/Facebook/Apple)
- **Payments** – Data required by Stripe for transactions

12.2. Optional Data

Other data (name, profile picture, preferences) is provided voluntarily.

13. Children's Privacy

Our services are not directed to children under 16 years of age. We do not knowingly collect personal data from children. If we become aware that we have collected personal data from a child under 16, we will take steps to delete such information.

14. Changes to This Policy

We may update this Privacy Policy. We will notify you of significant changes via:

- In-app notification
- Email (for major changes)
- Updated "Last modified" date

15. Contact

For privacy-related inquiries:

Administrator Danych Osobowych
ProWebDev
ul. Jarzębinowa 69, 52-200 Karwiany, Polska

E-mail: support@divvly.app
Subject: "Data Protection" or "GDPR"

Document version: 1.0 | Published: January 25, 2026