Pliant Privacy Policy

Last Updated: 20.05.2026

1. Introduction

Pliant Payments Inc. (“Pliant,” “we,” “us,” or “our”) is committed to protecting your personal information and being transparent about how we use it. Pliant’s Services are designed for use by business customers, and are not intended for personal, family, or household use. However, there may be instances where we process personal information about you in the commercial context. “Personal Information” means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to an identified or identifiable individual. Personal Information does not include information that has been de-identified, anonymized, or aggregated such that it can no longer reasonably be used to identify an individual. This Privacy Policy (the “Policy”) describes how we collect, use, disclose, and safeguard Personal Information when you use our products and services, our website, the Pliant web app, and the Pliant mobile app (collectively, the “Services”).

Capitalized terms that are used but not defined herein have the same meaning as set forth in the Pliant Payments, Inc. Platform Agreement, Payments Agreement, and Payment Card Addendum, and any applicable Pliant terms and policies, as amended from time to time (collectively, the “Pliant Terms”).

In this Privacy Policy, we may refer to “Payment Network and Processing Partners” (which include card networks, payment processors, and other entities that support the routing, processing, and settlement of payment transactions in connection with the Services).

Pliant operates as a platform provider and service provider in connection with financial products and services offered by our Financial Institution Partners. In many cases, we process Personal Information on behalf of our business customers in connection with providing the Services.

In connection with our provision of services in the financial sector, we may collect, use, and process non-public personal information (“NPI”) as defined under applicable state and federal financial privacy laws. We handle such information in accordance with applicable legal requirements and our contractual obligations with Financial Institution Partners, including requirements relating to confidentiality, and permitted use of such information.

We may also process certain information subject to additional legal or contractual requirements, such as where we act pursuant to a Business Associate Agreement or other applicable regulatory framework.

This Policy also describes:

- Our use of artificial intelligence (AI)
- Our obligations under applicable state law and HIPAA (where applicable)
- Your privacy rights

By accessing or using our Services, you acknowledge that you have read, understood, and agree to this Privacy Policy. Your continued use of the Services after any updates to this Privacy Policy constitutes your acceptance of those changes.

This Privacy Policy applies to our U.S. operations and Services. If you are located outside the United States, different terms or privacy policies may apply.

2. Scope and Applicability of this Policy

This Privacy Policy applies to certain information that we collect and process about individuals acting on behalf of our business customers, including employees, contractors, and other authorized users, when you visit, interact with, or use Pliant's website, mobile app, web app, and Services (including integrations, APIs and connections with third-party platforms), as well as when you engage with our social media, emails, newsletters, advertisements, and other locations or platforms, whether online or offline, where you interact with our business (collectively, the "Business").

This Privacy Policy does not apply to third-party websites, applications, or services, even if they are used in connection with our Services, that are not owned or operated by Pliant.

In many cases, Pliant processes Personal Information on behalf of its business customers and acts as a "service provider" or "contractor" (as defined under applicable U.S. privacy laws, including the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA/CPRA")). In such cases, we process Personal Information solely for the purpose of providing the Services in accordance with our agreements with our business customers and applicable law.

3. Personal Information We Collect

The Personal Information we collect depends on your interactions with Pliant, the Services you use as well as your location and applicable law. If you provide us with Personal Information about another individual, you represent that you have the authority to do so and have obtained any necessary consents and provided any required notices.

A. Information Provided to Pliant

When you open and maintain an account with Pliant, we will collect certain information about you, your company, and individuals associated with your company. This information may include:

- **Business Contact Information,** including your name, phone number, email, employer, job title, and address;
- **Identification Verification Information**, including Personal Information of the company's beneficial owners, control persons, and other relevant persons, such as their name, email address, phone number, employer, job title, date of birth, residential address, country of citizenship, photograph, tax identification numbers (such as Social Security numbers, employer identification numbers, or similar identifiers), driver's license, passport or other government-issued identification, and any other Personal Information collected as part of our KYC (Know-Your-Customer) and AML (Anti-Money Laundering) obligations;
- **Communications**, including when you contact sales or support, ask questions, participate in promotions, provide product feedback or otherwise communicate with us;
- **Content**, including any documentation, files, or information you provide, which may include information about you or your business;

- **Audio or Video Recordings,** including recordings and, where applicable, transcripts of customer support calls, training sessions, and meetings, which may be monitored or recorded (where permitted by applicable law and, where required, with prior notice and consent) for purposes such as quality assurance, training, security, compliance, and recordkeeping;
- **Healthcare-Related Data (Limited Cases)**, where, in limited cases (such as when users upload transaction receipts), we may collect healthcare-related information, including provider name, service details, billing or procedure codes, payment amounts, and insurance information. We do not intentionally collect full medical records;
- **Third-Party Information**, including information you choose to provide about co-workers, contractors, vendors, or potential referrals, such as their business contact information, where you have the necessary authority to share such information; and
- **Account Information**, including usernames, payment and bank account information, and authentication and security credentials.

B. Information We Collect Automatically

We automatically collect certain information when you interact with our Services, including when you visit our website, use our applications, or access your account. We use common technologies such as cookies, pixels, web beacons, log files, and similar tracking technologies to collect this information.

The information we collect automatically may include:

- **Usage and Interaction Information**, including details about how you access and use our Services, such as pages viewed, features used, links clicked, referring and exit pages, date and time of access, page response times, errors, and other interaction data (e.g., scrolling, clicks, and mouse movements);
- **Device and Technical Information**, including your IP address, device identifiers, browser type and version, operating system, time zone settings, mobile carrier, application version, authentication and security-related information, access dates and times, system activity, and diagnostic or crash data;
- **Log and Performance Data**, including logs of activity within the Services, API calls, system performance data, error reports, and other operational data used to maintain, secure, and improve the Services;
- **Approximate Location Information**, which may be inferred from your IP address to determine your general geographic location; and
- **Cookie and Tracking Information**, including identifiers and information collected through cookies and similar technologies used to operate and secure our Services, analyze usage, and support marketing and promotional activities.

We and our service providers may use these technologies for purposes such as authentication, security, fraud prevention, analytics, and improving functionality and user experience.

For more information about the cookies and similar technologies we use, including how to manage your preferences, please see the Cookies and Tracking Technologies section below as well as our Privacy Settings on the Pliant website.

California Residents
We may allow third parties to collect information through cookies and similar technologies for business purposes such as analytics and marketing, which may be considered "sharing" under California law. California residents may opt out of such sharing as described in our Cookie Notice or by using the "Do Not Sell or Share My Personal Information" link available on our website.

C. Information We Collect from Other Sources

We may collect Personal Information about you from other sources, including Financial Institution Partners, Payment Network and Processing Partners, service providers, integration partners, publicly available sources, and third parties that support our business or the Services. We may combine this information with the Personal Information you provide directly to us.

These sources may include:

- **Financial Institution Partners and Payment Network and Processing Partners**, such as issuing banks, card networks, and payment processors, which provide information to support onboarding, identity verification, transaction processing, risk assessment, and compliance with applicable legal and regulatory requirements;
- **Identity Verification, Fraud, and Compliance Providers**, which help us verify identity, assess risk, prevent fraud, and comply with legal and contractual obligations;
- **Business Partners and Integration Providers**, including vendors, merchants, and third-party service providers that interact with your company or enable integrations and functionality within the Services;
- **Service Providers**, which support our operations, including analytics, security, and infrastructure services;
- **Marketing, Analytics, and Advertising Partners**, which help us understand prospective customers, improve our marketing efforts, and measure campaign effectiveness, in accordance with applicable law; and
- **Publicly Available Sources**, including information from public databases, registries, and other sources used for due diligence, risk management, and business development purposes.

We process information obtained from these sources in accordance with applicable law and any contractual obligations.

D. Do Not Track Signals

Our Services do not currently respond to “Do Not Track” (DNT) signals. We operate as described in this Privacy Policy regardless of whether a DNT signal is received. If our practices change, we will update this Privacy Policy accordingly.

4. How We Use Your Personal Information

We use Personal Information for business and commercial purposes in accordance with this Privacy Policy. The purposes for which we use Personal Information are listed below.

- **Service Delivery**. To provide, operate, and maintain our Services, website, and other aspects of our Business, including to facilitate your company’s application for, and use of, financial products and services provided by our Financial Institution Partners and Payment Network and Processing Partners; to support onboarding, customer validation, identity verification, and account administration; to enable use of Pliant Cards; to verify financial information to establish spending and credit limits (where applicable); to process transactions and enable payments and fund transfers; to prevent or address technical issues and outages; to analyze and monitor usage and activity; and to communicate with you regarding your accounts, transactions, and use of the Services.
- **Communications**. To communicate with you about our Services, including to provide notices, updates, security alerts, and information regarding changes to our policies and Pliant Terms; to respond to support requests and inquiries; and to send transactional, relationship, and, where permitted, marketing communications;
- **Service Improvement**. To provide, maintain, improve, and develop our Services, including by measuring usage, analyzing performance, conducting analytics, and preventing or addressing technical issues and disruptions. We may also use information to improve and expand our products and operations, including by analyzing usage patterns, submitted documentation, and transaction-related information;
- **Legal and Compliance**. To comply with applicable legal, regulatory, and contractual obligations, including those arising from our relationships with Financial Institution Partners and Payment Network and Processing Partners; to respond to and cooperate with law enforcement, government authorities, courts, and regulators; to maintain records necessary to demonstrate compliance; to protect our legal rights and pursue available remedies; and to comply with requirements relating to payment programs, incentives, and rewards offered in connection with our Services;
- **Rewards Programs**. To administer and operate cashback or rewards programs, including calculating eligibility and cashback amounts based on transaction activity, determining applicable rates or thresholds, processing and issuing cashback payments, and preventing fraud or misuse of such programs.
- **Marketing and Promotions**. To send you marketing and promotional communications about our Services, including updates, offers, and events that may be of interest to you; to personalize such

communications based on your interactions with our Services; and to measure and improve the effectiveness of our marketing activities, in accordance with applicable law;

- **Artificial Intelligence**. We may use artificial intelligence and machine learning technologies to support certain aspects of our Services, such as identity verification, fraud detection, risk assessment, customer support, and product improvement. These technologies may process Personal Information as necessary to perform these functions. For more information, please see the "Use of Artificial Intelligence" section below.
- **Internal Operations**. To conduct internal reporting, auditing, and research, including through surveys, focus groups, and other feedback mechanisms;
- **At Your Direction**. To fulfill any other purpose at your direction, including as expressed through your or your company's use of the Services; and
- **Consent-Based Processing**. To use your information for additional purposes where we provide notice to you and, where required, obtain your consent.

5. Cookies and Tracking Technologies

We use cookies, pixels, web beacons, and similar tracking technologies ("Cookies") to collect information automatically when you interact with our Services. Cookies help us operate and secure our Services, improve functionality, analyze usage, and support marketing and advertising activities.

Types of Cookies We Use

We use the following categories of Cookies:

- **Essential Cookies**
  These Cookies are necessary for the operation of our Services. They enable core functionality such as security, authentication, and accessibility. Without these Cookies, the Services cannot function properly.
- **Functional Cookies**
  These Cookies allow us to analyze how users interact with our Services and help us improve performance and usability. They may also enable enhanced features and personalization.
- **Marketing Cookies**
  These Cookies are used to deliver relevant advertising and to measure the effectiveness of our marketing campaigns. They may track your activity across websites and services over time.

Third-Party Cookies and Technologies

We may allow third-party service providers to place Cookies on our Services for analytics, advertising, and other business purposes. These providers may collect information about your interactions with our Services and other websites over time. These third parties may include, for example:

- Analytics and performance providers (such as Google Analytics, Microsoft Clarity, and similar tools)

- Advertising and marketing partners (such as Google Ads, Meta (Facebook), LinkedIn, Microsoft Advertising, and similar platforms)
- Customer engagement and support providers (such as HubSpot, Intercom, and similar tools)
- Testing and optimization providers (such as Visual Website Optimizer (VWO))
- Content and media providers (such as YouTube)
- Infrastructure and hosting providers (such as Vercel)
- Review and feedback platforms (such as Trustpilot)

Some third-party services may provide embedded content (such as videos or reviews). When you interact with this content, the third party may set Cookies or collect information about your interaction in accordance with their own privacy policies.

Your Choices and Controls

You can manage your Cookie preferences at any time through our consent management tool, which allows you to accept or reject non-essential Cookies.

Depending on your location, you may also have the right to opt out of certain types of data processing, including the use of Cookies for targeted advertising.

Most web browsers also allow you to control Cookies through their settings. However, disabling certain Cookies may affect the functionality of the Services.

California Privacy Notice – Cookies

The use of certain Cookies, particularly Marketing Cookies, may be considered “sharing” of personal information under California law for purposes of cross-context behavioral advertising.

California residents can opt out of such sharing by:

- using the “Do Not Sell or Share My Personal Information” link on our website, or
- adjusting their preferences through our Cookie consent tool.

Updates to This Section

We may update our use of Cookies and similar technologies from time to time. Any changes will be reflected in this Privacy Policy and, where required, through updates to our Cookie consent tool.

6. Use of Artificial Intelligence

We use artificial intelligence (“AI”) and machine learning technologies to support and enhance certain aspects of our Services, including identity verification, fraud detection, risk assessment, customer support, and product improvement.

These technologies may process Personal Information as necessary to perform these functions, including by analyzing data, identifying patterns, and generating insights or recommendations.

AI-based systems are used to assist and support our personnel and operate in a supportive capacity only. We do not use AI systems to make solely automated decisions that produce legal or similarly significant effects on individuals. In all cases, including KYC reviews, final determinations are made by our employees, who review relevant information and exercise independent judgment.

We do not use AI systems to profile individuals in a manner that produces legal or similarly significant effects without human involvement.

We implement appropriate safeguards designed to ensure that our use of AI technologies is consistent with applicable law and our internal policies.

Pliant Mind (AI-Supported Features)

As part of our Services, we offer AI-supported functionalities ("Pliant Mind") designed to enhance platform capabilities, improve usability, and support more efficient workflows.

These features allow users to:

- Interact with the platform and submit queries
- Retrieve and analyze relevant information
- Generate summaries, insights, or structured outputs based on available data
- Support internal processes such as reviewing transactions or applying internal rules

Pliant Mind operates solely on data already available within the Pliant Platform, including customer account data, transaction data, and other information accessible to the user. It does not introduce or connect to external data sources and does not expand user permissions.

AI-supported features operate in a supportive capacity only. They do not make independent decisions and are not intended to replace human judgment. Outputs may require review and verification by users, who remain responsible for decisions made based on such outputs.

We do not use customer Personal Information processed through Pliant Mind to train, retrain, or otherwise improve underlying AI models.

AI-Supported Customer Support Tools

We may also use AI-supported tools provided by third-party service providers to assist with customer support, such as responding to general inquiries and providing help center information.

We implement governance measures designed to ensure that AI-supported systems are used in a fair, transparent, and accountable manner. This includes oversight by qualified personnel, periodic review of system outputs, and controls designed to mitigate risks such as bias, inaccuracies, or unintended outcomes.

When you interact with these tools, information you provide (such as message content and related interaction data) may be processed as necessary to provide, maintain, and improve the support functionality. These service providers process such information on our behalf in accordance with contractual obligations and applicable data protection laws.

These tools are designed to assist with general inquiries and do not make decisions that produce legal or similarly significant effects.

We do not use Personal Information from these interactions to train, retrain, or otherwise improve underlying AI models operated by such providers.

7. Sensitive Personal Information

We may collect and process certain information that is considered "sensitive personal information" under applicable law, including:

- financial account and transaction information;
- government-issued identifiers (such as Social Security numbers);
- login credentials and account access information; or
- limited healthcare-related information contained in transaction receipts.

We use sensitive personal information only as necessary to:

- provide and operate our Services;
- process transactions and manage accounts;
- detect and prevent fraud and security incidents; and
- comply with legal and regulatory obligations

We do not use or disclose sensitive personal information for purposes other than those permitted by applicable law, and we do not use such information in a manner that would require offering a right to limit under applicable law.

8. Information We Share

We may share Personal Information with the following categories of recipients, as necessary to provide and support the Services, comply with legal obligations, and operate our business:

- **Affiliates.** We may share Personal Information with our affiliates (i.e., entities that control, are controlled by, or are under common control with Pliant) in accordance with this Privacy Policy.
- **Business Customers.** We may share Personal Information with your company (our business customer) in order to provide the Services on its behalf, including to process transactions, administer accounts, report on usage, respond to inquiries, comply with requests, and meet legal and regulatory obligations. In many cases, we process Personal Information on behalf of your company in accordance with applicable agreements.

  Your company may assign roles and permissions to authorized users, which may allow access to Personal Information relating to your use of the Services. As a result, we may disclose information to other authorized users or individuals acting on behalf of your company, such as members of its finance team, managers, personnel, or service providers. Each business customer is an independent entity, and its processing of Personal Information is subject to its own policies and terms.

- **Financial Institution Partners and Payment Network and Processing Partners.** We may share Personal Information with Financial Institution Partners and Payment Network and Processing Partners in order to provide and support the Services. These partners provide banking and payment services in connection with the Services, while Pliant acts as a platform provider and program manager.

  We disclose Personal Information to support customer identification, identity verification, creditworthiness, risk assessment, fraud prevention, and compliance programs (including KYC and AML obligations), and to enable such partners to determine eligibility for, and provide, financial products and services to your company. This may include sharing business and contact information, identity verification information (including government-issued identifiers), financial and transaction data, and other information collected during onboarding and use of the Services.

  Financial Institution Partners act as independent controllers of Personal Information in connection with the financial products and services they provide. Their processing of Personal Information is subject to their own privacy policies and legal obligations. Pliant acts as a platform provider and service provider in this context and processes Personal Information in accordance with this Privacy Policy and applicable agreements.

- **Service Providers.** We may share Personal Information with third-party service providers that perform services on our behalf, such as cloud infrastructure, hosting, analytics, product development, payment processing, rewards administration, communications, customer and technical support, security monitoring, fraud detection and prevention, and debugging and error repair.

  Depending on the service, we may provide Personal Information on a continuous basis or on an as-needed basis. We contractually restrict our service providers from retaining, using, or disclosing Personal Information for any purpose other than providing services to us and require appropriate security and confidentiality measures. We may permit service providers to use aggregated, de-identified, or anonymized information in accordance with applicable law.

- **Third-Party Services and Integration Partners.** We may share Personal Information with third-party services and integration partners when you or your company choose to use integrations, APIs, or connected services. In such cases, we share information as necessary to enable the integration, process transactions, provide functionality, and support your use of those services. Your use of third-party services is subject to their terms and privacy policies.

- **Credit Reporting and Financial Information Providers.** We may share information with credit reporting agencies and other financial information providers to verify information about your company, assess creditworthiness, support underwriting decisions, and report on account performance, including late or missed payments or other defaults.

  Where applicable, we may provide information to or obtain information from credit reporting agencies and similar providers in accordance with applicable law, including the

Fair Credit Reporting Act ("FCRA"). Such information may be used for purposes such as identity verification, creditworthiness assessment, fraud prevention, and account management, where permitted.

- **Vendors, Payees, and Transaction Counterparties.** We may share Personal Information with vendors, payees, and other third parties involved in transactions conducted through the Services, as necessary to process payments, provide transaction status updates, and support your company's use of the Services.
- **Rewards, Analytics, and Marketing Partners.** We may share Personal Information with rewards and cashback providers, analytics providers, marketing and advertising partners, and referral or joint marketing partners to administer programs, measure and improve our Services, and support marketing activities, in accordance with applicable law.
- **Legal, Compliance, and Security.** We may disclose Personal Information to comply with applicable laws, regulations, payment network rules, and legal processes, including responding to requests from regulators, law enforcement, courts, and public authorities. We may also disclose information to detect, prevent, and investigate fraud, security incidents, or other unlawful activity, and to protect the rights, property, and safety of Pliant, our Services, our business customers, Financial Institution Partners, Payment Network and Processing Partners, or others.
- **Corporate Transactions.** We may disclose Personal Information in connection with, or during negotiations of, any proposed or actual merger, acquisition, financing, reorganization, sale of assets, or other corporate transaction, subject to appropriate confidentiality protections.
- **Card Benefits.** We may also share Personal Information with insurance providers, benefits administrators, and similar third parties in connection with card-related benefits, protections, or insurance programs (such as travel or purchase protection), to administer such programs, process claims, and provide related services.

We do not sell Personal Information as the term "sell" is defined under applicable law. However, we may share Personal Information with third parties for purposes such as analytics, advertising, and marketing, which may be considered "sharing" under applicable law.

9. International Data Transfers

Personal Information we collect may be stored and processed in the United States and in other countries where we or our affiliates and service providers operate or maintain facilities. We maintain primary data centers in the United States.

The Pliant Platform is owned by Pliant GmbH and licensed to Pliant Payments Inc., and as a result, Personal Information may be transferred to and processed by our affiliates, including within the European Economic Area ("EEA"), as necessary to provide and support the Services.

In connection with providing financial services, certain categories of Personal Information, including identity verification information, KYC/AML data, creditworthiness and financial information, and transaction data, may be transferred to and processed by Financial Institution Partners, Payment

Network and Processing Partners, affiliates, and service providers located in the United States, the EEA, and other jurisdictions.

We take steps designed to ensure that Personal Information is processed in accordance with this Privacy Policy and applicable law, including implementing appropriate safeguards for cross-border data transfers where required.

10. Data Retention

We retain Personal Information for as long as necessary to fulfill the purposes described in this Privacy Policy, including to provide the Services, comply with legal, regulatory, and contractual obligations, resolve disputes, and enforce our agreements.

In certain cases, we are required to retain Personal Information for specific minimum periods under applicable law and regulatory requirements. For example, information related to financial transactions, account activity, identity verification, and compliance with anti-money laundering and financial regulations may be retained for a period of five (5) to seven (7) years, or longer where required by applicable law, contractual obligations, or regulatory authorities.

Because retention requirements may vary depending on the type of Personal Information and the Services involved, actual retention periods can differ. For example, certain financial and transaction records may be retained for a minimum period required by applicable financial regulations. We determine appropriate retention periods based on factors such as the amount, nature, and sensitivity of the Personal Information, the potential risk of harm from unauthorized use or disclosure, whether the purposes of processing can be achieved through other means, and applicable legal requirements (such as statutes of limitation).

In some cases, we may retain Personal Information after you are no longer an authorized user or your company's account has been closed, including where required to comply with applicable laws and regulations or obligations arising from our relationships with Financial Institution Partners and Payment Network and Processing Partners (such as anti-money laundering, financial reporting, and recordkeeping requirements). These obligations may limit our ability to delete Personal Information upon request.

When the applicable retention period expires, we will delete or de-identify Personal Information in accordance with our policies and procedures, unless further retention is required or permitted by law.

11. Data Security

We design our systems with security and privacy in mind and implement a range of technical, organizational, and physical safeguards to protect Personal Information. These measures are designed to prevent unauthorized access, use, alteration, and disclosure of Personal Information and include, among other things, encryption, access controls, and secure infrastructure.

We maintain security programs and controls designed to protect Personal Information during transmission and storage and may engage independent third parties to assess and validate aspects of our security practices. We may also require verification of identity before providing access to certain information.

You are responsible for maintaining the confidentiality of your account credentials, limiting access to your devices, and signing out of your account after use.

Despite these measures, no method of transmission over the Internet or method of electronic storage is completely secure. While we strive to protect Personal Information using commercially reasonable safeguards, we cannot guarantee absolute security.

In the event of a security incident affecting Personal Information under our control, we will take appropriate steps to investigate, mitigate, and, where required, notify affected individuals and relevant authorities without undue delay and in accordance with applicable law.

In the event of a data breach involving Personal Information, we will provide notifications in accordance with applicable U.S. federal and state data breach notification laws, including, where required, notification to affected individuals, regulatory authorities, and other relevant parties within the timeframes prescribed by law.

12. Your Privacy Rights

Depending on your location and subject to applicable U.S. law, you may have certain rights regarding your Personal Information, including the right to request access to, correction or deletion of, or restriction of processing of your Personal Information, as well as the right to opt out of certain uses of your Personal Information.

We will respond to verified requests within the timeframes required by applicable law (for example, within forty-five (45) days under the CCPA/CPRA, subject to extension where permitted). We may take reasonable steps to verify your identity before responding to your request, including by requesting additional information necessary to confirm your identity or authority to act on behalf of another individual. Where applicable, you may have the right to appeal our decision regarding your request by contacting us using the details provided below.

Additional information about rights available to residents of certain U.S. states is provided below.

You also have choices regarding the collection and use of your Personal Information. For example, you may choose not to provide certain information; however, doing so may limit your ability to use certain features of the Services.

13. International Users

If you are located in the European Economic Area, United Kingdom, Switzerland, or another jurisdiction with specific data protection laws, additional terms may apply to you. Please refer to the applicable regional privacy notice available on our website for more information about how your personal data is processed.

14. Additional State Specific Disclosures

California Residents

This section provides additional information for California residents about how we collect, use, and disclose Personal Information, and the rights available under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“CCPA/CPRA”).

In the preceding 12 months, we may have collected the following categories of Personal Information: identifiers (such as name and contact information), commercial information, internet or other electronic network activity information, geolocation data, audio, electronic, visual, or similar information (such as customer support interactions), professional or employment-related information, and inferences drawn from such information.

We collect, use, and disclose Personal Information for the business and commercial purposes described in the "How We Use Personal Information" and "Information We Share" sections above.

Subject to certain limitations and exceptions under applicable law, California residents have the following rights:

- Right to Know: to request information about the categories and specific pieces of Personal Information we collect, use, disclose, and share;
- Right to Delete: to request deletion of Personal Information we have collected about you;
- Right to Correct: to request correction of inaccurate Personal Information;
- Right to Opt Out of Sale or Sharing: to opt out of the sale or sharing of Personal Information, including for cross-context behavioral advertising;
- Right to Limit Use of Sensitive Personal Information: to request limitations on the use and disclosure of Sensitive Personal Information; and
- Right to Non-Discrimination: not to receive discriminatory treatment for exercising your rights.

We do not sell Personal Information. We may share Personal Information with third parties for the purposes described in this Privacy Policy, including for analytics and advertising activities, which may be considered "sharing" under California law.

To exercise your rights, please contact us using the information provided in the "Contact Us" section below. We may take steps to verify your identity before responding to your request, as required by law.

You may designate an authorized agent to submit a request on your behalf. To do so, we may require verification of your identity and proof that the authorized agent has permission to act on your behalf, in accordance with applicable law.

Sale and Sharing of Personal Information

We do not sell Personal Information as the term "sell" is defined under the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA/CPRA").

However, we may share Personal Information with third parties for purposes of cross-context behavioral advertising, analytics, and marketing. Such disclosures may be considered "sharing" under the CCPA/CPRA.

The categories of Personal Information that may be shared include identifiers (such as name, email address, IP address, and device identifiers), internet or other electronic network activity information, and inferences derived from such information.

We share Personal Information with categories of third parties such as advertising networks, analytics providers, and marketing partners to support our marketing, analytics, and business operations.

California residents have the right to opt out of the sharing of Personal Information for cross-context behavioral advertising. You can exercise this right by using the “Do Not Sell or Share My Personal Information” link on our website or by contacting us using the information provided in the “Contact Us” section below.

These choices are also described in the “Cookies and Tracking Technologies” section above.

North Dakota Residents

If you are a resident of the State of North Dakota, the following additional disclosures apply to the collection, use, and sharing of your information:

Financial Information. We collect and process certain non-public personal and business-related financial information in connection with your use of the Pliant Platform, including information provided during onboarding, account usage data, and transaction-related information. Such information is used solely for purposes of providing and improving our services, facilitating payment transactions, complying with legal and regulatory obligations, and supporting our relationships with Financial Institution Partners and Payment Network and Processing Partners.

Sharing of Information. We may share your information with our Financial Institution Partners, Payment Network and Processing Partners, and other service providers that perform services on our behalf or support the operation of the Pliant Platform. We may also share information as required by applicable law, regulation, or legal process. We do not disclose your non-public personal information to unaffiliated third parties for their own marketing purposes.

Safeguards and Compliance. We maintain administrative, technical, and physical safeguards designed to protect your information against unauthorized access, use, or disclosure. We require our service providers to implement appropriate data protection measures and to use your information only for authorized purposes. We process and handle information in accordance with applicable data protection and financial privacy laws, including requirements applicable to our Financial Institution Partners and Payment Network and Processing Partners.

We obtain your consent to the collection, use, and sharing of your information as described in this Privacy Policy through your acceptance during onboarding.

15. Children’s Privacy

Our Services are intended for business entities and are not directed to children. We do not knowingly collect Personal Information (as defined under the U.S. Children’s Online Privacy Protection Act (“COPPA”)) from children under the age of 13 or market to such individuals.

We also do not knowingly sell or share (as those terms are defined under applicable law, including the California Privacy Rights Act) the Personal Information of individuals under the age of 16.

If we become aware that Personal Information has been collected from a child under 13 without appropriate authorization, we will take steps to delete such information in accordance with applicable

law. If you are a parent or guardian and believe that a child has provided us with Personal Information, please contact us using the information provided in the “Contact Us” section below.

16. Healthcare and HIPAA-Related Information

In limited cases, users may submit documentation (such as receipts or supporting materials) that contain health-related information. Pliant is not a Covered Entity under the Health Insurance Portability and Accountability Act (“HIPAA”).

To the extent we process Protected Health Information (“PHI”) on behalf of a customer, we do so only pursuant to a valid Business Associate Agreement (“BAA”) and in accordance with applicable legal and contractual requirements. We do not use or disclose such information except as necessary to provide the Services or as otherwise permitted or required by law.

17. Third Party Services

Our Services may contain links to, or integrations with, third-party websites, applications, or services that are not owned or controlled by Pliant. This Privacy Policy does not apply to the privacy practices of such third parties.

If you or your company choose to access or use third-party services in connection with the Services (including through integrations, APIs, or connected platforms), any Personal Information you provide to or that is collected by those third parties will be subject to their respective privacy policies and terms.

We are not responsible for the privacy practices, security, or content of third-party services. We encourage you to review the privacy policies of those third parties before providing any information to them.

18. Changes to this Privacy Policy

We may update or modify this Privacy Policy from time to time to reflect changes in our Services, our business practices, or applicable law. When we do, we will revise the “Last Updated” date at the top of this Privacy Policy.

If we have an existing relationship with you (for example, if you represent a business customer or are an authorized user), we may provide notice of material changes through the Services, your company’s account, or using contact information we have on file. If we do not have an existing relationship with you (for example, if you only visit our website), we will post the updated Privacy Policy on our website.

Any updates to this Privacy Policy will be effective when posted, unless otherwise indicated. We encourage you to review this Privacy Policy periodically to stay informed about how we collect, use, and share Personal Information.

19. Contact Us

If you have any questions or concerns about this Privacy Policy or how we handle Personal Information, please contact us at:

Pliant Payments, Inc.

By Email: privacy@getpliant.com

By Phone: +1 (917) 540-4658

By Mail: Pliant Payments, Inc. 200 Broadway, Office 503 New York, NY Attn: Privacy Office

If you experience any difficulty accessing this Privacy Policy, please contact us using the information above, and we will make reasonable efforts to provide the information in an alternative format.

If you are an employee, contractor, or other authorized user of one of our business customers and have questions about Personal Information processed on behalf of your company ("Customer Data"), please contact your account Administrator or your employer directly. We process such information on behalf of our business customers and may direct your request to the relevant customer, as appropriate.

If you require this Privacy Policy in an alternative or accessible format (for example, due to a disability or accessibility need), please contact us using the information above. We will make reasonable efforts to provide the information in a format that meets your needs, in accordance with applicable law.