

Privacy Policy of Pliant GmbH

MCP Connector

This Privacy Policy applies to processing of personal data when a customer enables the Pliant Model Context Protocol connector (the “Connector”) for use with an AI-based software solution or other application that supports MCP (the “Connected Service”), and when an individual user connects their individual Pliant Platform account to that service. Connected Services may include, without limitation, Claude AI, Claude Code, ChatGPT, Codex, Cursor AI, Gemini AI, Notion AI, and other current or future MCP-compatible solutions.

The customer enables the Connector for its Pliant Platform account at organisational level. This organisational enablement makes the Connector available to platform users but does not connect their individual accounts or automatically disclose data to a Connected Service. Each user must separately initiate the connection for their own Pliant Platform account.

This Privacy Policy applies primarily to the individuals whose personal data may be processed through the Connector, including employees, cardholders, other authorised platform users and other individuals identified in Pliant Platform records. “You” therefore means the individual platform user connecting and using the Connector.

This Privacy Policy covers processing through the Connector and supplements the privacy policy applicable to the customer’s use of the Pliant Platform, taking into account the relevant contracting entity, product setup and jurisdiction. That privacy policy explains how personal data is otherwise processed in the Pliant Platform, including the applicable purposes, legal bases, categories of personal data, recipients, retention periods and individual rights.

This Policy applies to all Pliant customers and platform users, regardless of their contractual setup. The applicable data protection requirements and individual rights may vary depending on the relevant contracting entity, product setup and jurisdiction.

1. Controller

The controller for the processing of personal data described in this Privacy Policy is:

Pliant GmbH
Prenzlauer Allee 242-247
10405 Berlin, Germany
Email: info@getpliant.com

2. Contact details of a Data Protection Officer

Our data protection officer is available to provide you with information on the issue of data protection under the following contact details:

Katharina A. Weimer, LL.M. (UNSW)
Fieldfisher Tech Rechtsanwaltsgesellschaft mbH
Landsberger Str. 110
80339 Munich, Germany
E-Mail: privacy@getpliant.com
Web: www.fieldfisher.com

3. How the Connector works

An Organisation Owner, Admin or another platform user authorised by the customer first enables the Connector for the customer organisation and may permit one or more Connected Services. Individual users cannot connect their account unless the organisational setting is enabled.

Each individual user then connects their own Pliant Platform account through OAuth 2.0 or another supported secure authentication method. The user's access to information and/or ability to perform actions through the Connector remain limited to that user's existing Pliant Platform role and permissions.

Read requests: When a user asks a Connected Service to retrieve, search, explain, summarise or analyse Pliant Platform information, the Connected Service sends a supported tool request to the Connector. Pliant verifies the user's permissions and returns only information that the user is authorised to access and that is necessary for the request.

Write requests: Where a write tool is available, a user may instruct the Connected Service to create, update, classify or otherwise manage Pliant Platform data. Pliant performs the requested action only if the tool is enabled and the user is authorised to perform that action. Depending on the action and the applicable workflow, an additional confirmation, review and/or approval may be required before execution. The Connector does not bypass Pliant Platform Permissions or approval workflows and does not independently grant the Connected Service authority to act.

In both cases, the Connector:

- responds to requests initiated through a Connected Service and does not continuously synchronise the customer's Pliant Platform account with that service, unless a specific feature expressly provides otherwise;
- applies the requesting user's current role and permissions to each read or write request and cannot access another organisation's data;
- may offer different read and write tools depending on the customer setup, Pliant Platform configuration, Connected Service and/or user role; and
- does not provide or control the underlying AI-based software solution, determine how a Connected Service formulates its outputs, or guarantee that those outputs are complete or accurate.

4. Purposes and legal bases

Pliant processes Connector data to authenticate users, receive, validate and fulfill supported read and write requests, provide and administer the integration, maintain security and audit records, troubleshoot errors, prevent misuse and, where necessary, comply with legal obligations. Processing of the underlying Pliant Platform data continues for the purposes and on the legal bases described in the privacy policy applicable to the customer's use of the Pliant Platform.

Connector processing and processing necessary to provide the requested service is pursuant to Pliant's legitimate interests in providing a secure and user-controlled integration.

5. Personal data processed through the Connector

Depending on the request, enabled tools, customer configuration and user permissions, the Connector may process data including personal data, from the customer's Pliant Platform account. The data may relate to employees, cardholders, authorised platform users and other individuals identified in transactions, expenses, receipts, invoices, documents and/or related records.

The categories of personal data being processed may include:

- identity, access, preference and connection data, such as names, business contact details, user and organisation identifiers, roles, permissions, authentication and connection records, language or locale preferences, and notification settings;
- organisation, account and financial overview data, such as organisation settings, account entries, balances, limits, cashback, emissions information, billing reports, direct-debit information and payout history;
- member and team data, such as users, cardholders, teams, assignments, roles, permissions and related administration records;
- card and card-account data, such as masked card references, card type and status, card accounts, card templates, limits, available amounts, card histories, card requests and card-limit change requests;
- transaction, merchant, expense and document data, such as transaction details, coding and review status, descriptions, categories, allocations, custom fields, receipts, invoices, statements and private or automated reimbursements;
- accounting, classification and reporting data, such as suppliers, projects, subcategories, VAT rates, accounting exports, accounting integrations and settings, accounting dimensions and organisation- or transaction-level custom fields;
- approval, beneficiary and payment-related records, such as approval requests and policies, beneficiary and beneficiary payment details, internal or external transfer records, payout payment records and related statuses; and
- technical, security and audit data, such as IP addresses, timestamps, tool and connection events, request status, errors and limited diagnostic information.

The inclusion of a category, object or record above does not mean that every Connected Service or user can access or modify it. Nor does it mean that the Connector can initiate, approve or execute the underlying process. The available read or write operation always depends on the tools enabled for the customer and the requesting user's existing permissions.

Transaction descriptions, merchant information, receipts, invoices and other supporting documents may contain personal data or confidential information. Where the Pliant Platform is used in connection with insurance products, documents submitted for claims or reimbursements may also contain health-related data, including information about medical treatment, medical supplies, healthcare providers or identifiers appearing in those documents.

The Connector may read, transmit or otherwise process this information through a Connected Service only where relevant functionality is enabled, the user is authorised to access it and the processing is necessary for the request. Health related data concerning individual users is processed on the basis of explicit consent. Further information is provided in the privacy policy applicable to the customer's use of the Pliant Platform.

6. Data not made available through the Connector

The Connector is not designed or permitted to provide a Connected Service with:

- sensitive payment or authentication credentials, such as full card numbers, CVC or CVV values, PINs, chip or magnetic stripe authentication data, passwords, one-time passwords or 3-D Secure credentials;
- identity verification source documents, biometric templates, detailed KYC or AML investigation files, or source reports used for creditworthiness assessments; or
- the user's complete Connected Service account history, memory, unrelated conversations or files merely because the Connector is enabled.

Pliant receives only the requests, tool parameters, data and technical information that the Connected Service sends to the Connector to fulfill a supported read or write request.

7. Permitted use cases

Within the user's existing Pliant Platform role and permissions, and depending on the tools enabled for the customer, the Connector may support read and write use cases, including:

- searching, retrieving, filtering, explaining, summarising and analysing organisation, account, member, team, card, transaction, expense, document, accounting, approval and payment-related information;
- preparing spend, trend, reconciliation, accounting and management-reporting analyses or structured outputs, and identifying missing information, unusual patterns or items requiring review;

- coding, enriching or updating transactions, including descriptions, accounting fields, dimensions, custom fields and review status;
- creating or managing members and teams, including assignments and other administration available to the requesting user;
- reading or managing receipts, reimbursements, exports, accounting settings, approval requests, notification settings and other supported workflows;
- reading, creating or updating supported card, card-account or card-control information where the relevant tools are available; and
- retrieving or reviewing beneficiary, transfer, payout and account-entry information, and performing any related action only where a specific tool is enabled and the user has the necessary permission and completes any required confirmation or approval.

Some capabilities are currently available and others may be added, changed or removed over time. Availability depends on the customer's Pliant Platform setup, the Connector functionality supported by the relevant Connected Service and the user's existing role and permissions. A write tool cannot allow a user to do more than that user is authorised to do directly in the Pliant Platform. Pliant will provide appropriate prior information and, where required, obtain the relevant customer or user authorisation before enabling materially different functionality.

Outputs generated by a Connected Service may be incomplete or inaccurate. Users must review material outputs and proposed actions before relying on them.

8. Disclosure to AI-based software solutions and other service providers

When a user invokes the Connector, customer data, including personal data, is transmitted to the customer's environment with the relevant Connected Service. It is then received and processed by the provider of that service under the customer's own account, subscription and contractual arrangements. Depending on the service, the applicable provider or contracting entity may vary according to the customer's location and setup.

Pliant does not provide or administer the customer's Connected Service subscription and does not determine that provider's retention periods, model-improvement, international data transfer or other account settings. Processing by the Connected Service is governed by the customer's applicable terms and privacy documentation with the relevant provider.

9. Data retention

Underlying customer data, including personal data read from or written to the Pliant Platform, is stored and retained in accordance with the rules and provisions outlined in the privacy policy applicable to the customer's use of the Pliant Platform. The Connector does not create a separate permanent copy of information returned to, or received from, the respective Connected Service, except where an authorised write request creates or changes a record in the Pliant Platform.

Connection credentials and status records are retained while needed to maintain, expire or revoke the connection. Security and audit logs may record identifiers, timestamps, the tool invoked, request status, confirmation or approval events, errors and limited diagnostic information. Content is logged only where necessary for security or troubleshooting and retained under Pliant's applicable retention schedule and legal obligations.

Pliant cannot delete information retained in the customer's Connected Service account. The customer, user or relevant administrator must manage conversations, tool results and retention through that service in accordance with applicable contractual arrangement.

10. Disconnection and Individual Rights

An Organisation Owner, Admin or another platform user authorised by the customer may disable the Connector or a particular Connected Service for the organisation. Each user may separately disconnect their own account through the applicable settings. Access also ends if the user is deactivated or loses the required Pliant Platform permissions. Disconnection prevents future access but does not automatically delete information already retained in the Connected Service or reverse actions previously completed through an authorised write request.

Depending on applicable law, individuals may have rights of access, correction, deletion, restriction, portability and objection, and may have the right to withdraw consent or complain to a competent supervisory authority. The privacy policy applicable to the customer's use of the Pliant Platform provides further information about individual rights and how they may be exercised.

Requests concerning Pliant's Connector processing may be sent to privacy@getpliant.com. Requests concerning information retained by a Connected Service should be addressed through the customer's administrator for that service or directly to the relevant service provider, as applicable.