

Datenschutzhinweise der Pliant GmbH (Pliant Mobile-App)

Wir, die Pliant GmbH, stellen Ihnen neben unserer Internet-Webseite und der Pliant Web-App auch eine Pliant Mobile-App zur Verfügung, die Sie sich auf Ihr mobiles Endgerät herunterladen können (im Folgenden „**Pliant Mobile-App**“). Im Folgenden informieren wir über die Erhebung personenbezogener Daten bei Nutzung unserer Pliant Mobile-App. Bitte beachten Sie die gesonderten Datenschutzerklärungen für die Webseite sowie unsere Pliant Web-App.

1. Verantwortlicher

Verantwortlicher für die Verarbeitung von personenbezogenen Daten, die bei der Nutzung der Pliant Mobile-App erfasst werden, ist:

Pliant GmbH
Prenzlauer Allee 242-247
10405 Berlin
Deutschland
E-Mail: info@getpliant.com

2. Kontaktdaten des Datenschutzbeauftragten

Unser Datenschutzbeauftragter steht Ihnen gerne für Auskünfte oder Anregungen zum Thema Datenschutz zur Verfügung:

datenschutz nord GmbH
Kurfürstendamm 212
10719 Berlin
E-Mail: office@datenschutz-nord.de
Web: www.datenschutz-nord-gruppe.de

3. Nutzungsdaten zu statistischen Zwecken

Bei der Nutzung der Pliant Mobile-App erheben wir auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO die nachfolgend beschriebenen personenbezogenen Daten, um Ihnen die Funktionen unserer Pliant Mobile-App anzubieten und die Stabilität und Sicherheit der Pliant Mobile-App zu gewährleisten. Diese von uns verfolgten Zwecke stellen zugleich das berechtigte Interesse im Sinne von Art. 6 Abs. 1 lit. f DSGVO dar. Der Datensatz besteht aus:

Privacy Policy of Pliant GmbH (Pliant mobile app)

We, Pliant GmbH, provide you, in addition to our internet website and the Pliant web app, also with a Pliant mobile app, which you can download to your mobile device (hereinafter "**Pliant mobile app**"). In the following, we provide information about the collection of personal data when using our Pliant mobile app. Please refer to the separate privacy policies for the website and our Pliant web app.

1. Controller

Controller for the processing of personal data collected when using our Pliant mobile app is:

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

2. Contact data of the data protection officer

Our data protection officer will be happy to provide you with information on data protection:

datenschutz nord GmbH
Kurfürstendamm 212
10719 Berlin, Germany
email: office@datenschutz-nord.de
web: www.datenschutz-nord-gruppe.de

3. Usage data for statistical purposes

When using our Pliant mobile app, we collect the personal data described below on the basis of Art. 6 (1) lit. f GDPR to provide you with the features of our Pliant mobile app as well as to ensure the stability and security of the Pliant mobile app. These purposes pursued by us represent at the same time the legitimate interest within the meaning of Art. 6 (1) lit. f GDPR. The data set consists of:

- dem Datum und der Uhrzeit der Abfrage,
- Zeitzonendifferenz zur Greenwich Mean Time (GMT)
- der übertragenen Datenmenge,
- dem Zugriffsstatus (Datei übertragen, Datei nicht gefunden),
- dem verwendeten Betriebssystem,
- das Gerätemodell
- der IP-Adresse des anfragenden Gerätes, die so verkürzt wird, dass ein Personenbezug nicht mehr herstellbar ist.

Die genannten Protokolldaten werden nur anonymisiert ausgewertet.

4. Funktionen und Zwecke der Pliant Mobile-App

Mithilfe der Pliant Mobile-App können Kartennutzer mit einer Firmenkreditkarte sicher auf zahlungsrelevante Karteninformationen, wie etwa die Kartennummer und den Sicherheitscode, direkt innerhalb der App zugreifen. Die Pliant Mobile-App erleichtert darüber hinaus das Ausgabenmanagement, indem sie es Nutzern ermöglicht, Transaktionen zu überwachen, digitale Belege hochzuladen und im Falle eines Verlusts oder Diebstahls der Karte eine Ersatzkarte zu bestellen. Die Verarbeitung von personenbezogenen Daten erfolgt auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO.

- Download

Beim Herunterladen der Pliant Mobile-App werden die dafür notwendigen Informationen an den App Store übertragen, also insbesondere Name, E-Mail-Adresse und Kundennummer Ihres Accounts, Zeitpunkt des Downloads, Zahlungsinformationen und die individuelle Gerätekenziffer. Auf diese Datenerhebung haben wir jedoch keinen Einfluss und sind nicht dafür verantwortlich. Wir verarbeiten diese bereitgestellten Daten, soweit dies für das Herunterladen der Pliant Mobile-App auf Ihr Endgerät notwendig ist. Sie werden darüber hinaus nicht weiter gespeichert.

- Anmeldung in der Pliant Mobile-App

Zum Login werden folgende Daten des Kartennutzers verarbeitet: E-Mail-Adresse, Passwort und Mobile-Tan (Zwei-Faktor-Authentifizierung) oder alternativ eine biometrische Identifizierung über das mobile Endgerät (z.B. Fingerabdruck, FaceID). Die angegebenen Daten verarbeiten wir zur Anmeldung und weiteren Bedienung/Nutzung der Pliant Mobile-App.

- the date and time of the request,
- time zone difference from Greenwich Mean Time (GMT)
- the amount of data transferred,
- the access status (file transferred, file not found),
- the operating system used,
- the device model,
- the IP address of the requesting device, which is shortened so that a personal reference can no longer be established.

The aforementioned log data is only evaluated anonymously.

4. Functionalities and purposes of the Pliant mobile app

With the help of the Pliant mobile app, card users with a company credit card can securely access essential payment details, such as the card number and security code, directly within the app. Furthermore, the Pliant mobile app streamlines expense management, allowing users to monitor transactions, upload digital receipts and order a replacement card if theirs is lost or stolen. The processing of personal data is based on Art. 6 para. 1 lit. b GDPR.

- Download

When downloading the Pliant mobile app, the necessary information is transferred to the app store, i.e. in particular name, email address and customer number of your account, time of download, payment information and the individual device identification number. However, we have no influence on this data collection and are not responsible for it. We process this provided data as far as this is necessary for downloading the Pliant mobile app to your end device. They are not stored further beyond that.

- Login to the Pliant mobile app

The following card user data is processed for login: Email address, password and mobile tan (two-factor authentication) or alternatively biometric identification via the mobile device (e.g. fingerprint, FaceID). We process the specified data for registration and further operation/use of the Pliant mobile app.

- Push-Nachrichten

Push-Nachrichten in der Pliant Mobile-App werden genutzt, um Karteninhaber über neue Kartentransaktionen, die Genehmigung neuer Karten oder den Ablauf bestehender Karten zu informieren. Außerdem nutzen wir Push-TANs benutzen, um Nutzer über die Zwei-Faktor-Authentifizierung für die Pliant Web-App zu authentifizieren.

5. Pliant Mobile App-Berechtigung

Damit alle Funktionalitäten und Dienste der Pliant Mobile-App funktionstüchtig sind, muss die Pliant Mobile-App auf verschiedene Funktionen und Daten des Geräts zugreifen können. Dazu ist es technisch notwendig, dass der Pliant Mobile-App bestimmte Zugriffsberechtigungen gewährt werden. Wollen Sie bestimmte Zugriffsberechtigungen nicht erteilen, sind einige Funktionalitäten und Dienste der Pliant Mobile-App nicht nutzbar. Die Pliant Mobile-App benötigt folgende Berechtigungen:

- Kamera und Speicher (Aufnahme von Fotos/Zugriff auf Fotos auf dem Gerät sowie Dateien)

Sie können der Pliant Mobile-App erlauben, Fotos aufzunehmen bzw. auf den Speicher Ihres Smartphones (Bildergalerie und Dateisystem) zuzugreifen. Die Pliant Mobile-App benötigt Zugriff auf die auf dem Gerät gespeicherten Dateien (Bildergalerie und Dateisystem), damit Sie Rechnungen sowohl im Bild- als auch im PDF-Format hochladen können. Für die Authentifizierung brauchen wir Zugriff auf die Schnittstelle zur biometrischen Identifizierung (z.B. Face ID).

6. Nutzung der Firmenkreditkarte in einem Mobile Wallet

Unsere Kunden haben zudem die Möglichkeit, die Firmenkreditkarte zu einem sog. Mobile Wallet hinzuzufügen; weitere Informationen hierzu finden Sie in den Mobile Wallet AGB.

Der betreffende Anbieter des Mobile Wallet ist eigenständig Verantwortlicher dafür, wie er die von Ihnen zur Verfügung gestellten persönlichen Daten (z.B. kartenbezogene Informationen, Gerätestandort, Informationen über Geräteeinstellungen) im Rahmen der Nutzung des Mobile Wallet verwendet und verwaltet. Bitte beachten Sie die entsprechenden Datenschutzhinweise des jeweiligen Mobile Wallet - Anbieters.

- Push notifications

Push notifications in the Pliant mobile app are used to notify cardholders about new card transactions, approval of new cards, or expiration of existing cards. We also use push-TANs to authenticate users via two-factor authentication for the Pliant web app.

5. Pliant mobile app authorizations

In order for all functionalities and services of the Pliant mobile app to work, the Pliant mobile app must be able to access various functions and data of the device. For this it is technically necessary that the Pliant mobile app is granted certain access permissions. If you do not want to grant certain access permissions, some functionalities and services of the Pliant mobile app are not usable. The Pliant mobile app requires the following authorizations:

- Camera and memory (taking photos/accessing photos on the device as well as files)

You can allow the Pliant mobile app to take photos or access your smartphone's memory (image gallery and file system). The Pliant mobile app needs access to the files stored on the device (image gallery and file system) so that you can upload invoices in both image and PDF format. For authentication, we need access to the interface for biometric identification (e.g. Face ID).

6. Use of the corporate credit card in a Mobile Wallet

Our customers also have the option of adding the corporate credit card to a so-called Mobile Wallet; further information on this can be found in the Mobile Wallet T&Cs.

The relevant Mobile Wallet provider is separately responsible for how it uses and manages any personal information you provide to it (e.g. card-related information, device location, information about device settings) in the context of using the Mobile Wallet. Please observe the corresponding privacy policy of the respective Mobile Wallet provider.

7. Verarbeitung besonderer Kategorien personenbezogener Daten (Gesundheitsdaten)

Sofern wir Plattformdienste im Zusammenhang mit Versicherungsprodukten erbringen, können Nutzer die Pliant-Mobile-App verwenden, um Zahlungsnachweise oder sonstige Unterlagen einzureichen und damit unter einer Versicherungspolice gedeckte Ereignisse zu dokumentieren und abzuwickeln. Hierzu können insbesondere medizinische Behandlungen, medizinische Hilfsmittel oder sonstige versicherte Ereignisse gehören, die Rückschlüsse auf gesundheitsbezogene Informationen zulassen können. In diesem Zusammenhang können Nutzer über die Pliant-Plattform Belege, Rechnungen oder sonstige unterstützende Dokumente im Zusammenhang mit Forderungen oder Erstattungen einreichen. Diese Dokumente können gesundheitsbezogene Daten enthalten.

Im Zusammenhang mit der Nutzung der Pliant Mobile-App und der Einreichung von Unterlagen können besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO verarbeitet werden. Hierzu zählen insbesondere Angaben zu medizinischen Behandlungen oder Hilfsmitteln, Informationen zu Leistungsträgern im Gesundheitswesen sowie personenbezogene Identifikationsmerkmale, die in den eingereichten Dokumenten enthalten sind (z. B. der Name des Karteninhabers oder dessen Identifikationsnummer).

Pliant verarbeitet gesundheitsbezogene personenbezogene Daten ausschließlich zu dem Zweck, die Plattformdienste bereitzustellen, Erstattungen zu ermöglichen und die Bearbeitung von Leistungsanträgen im Versicherungsbereich zu unterstützen. Die Verarbeitung gesundheitsbezogener Daten erfolgt auf Grundlage der ausdrücklichen Einwilligung der betroffenen Person gemäß Art. 9 Abs. 2 a) DSGVO. Diese wird erteilt, wenn der Nutzer im Rahmen des Leistungsantrags eine Karte beantragt oder erhält und/oder Belege, Rechnungen oder sonstige Unterlagen aktiv über die Pliant-Mobile-App zu Zwecken der Erstattung oder Leistungsbearbeitung einreicht. Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden, z. B. durch eine E-Mail an privacy@getpliant.com. Der Widerruf der Einwilligung berührt nicht die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung.

In Bezug auf die unmittelbaren Kunden von Pliant (z. B. Versicherungsunternehmen) erfolgt die Verarbeitung der zur Ermöglichung von Erstattungen und zur Abwicklung von Zahlung hinsichtlich versicherter Ereignisse erforderlichen

7. Processing of special category of personal data (health data)

Where we provide platform services in the context of insurance products, users may use the Pliant mobile app to submit proof of payment or other supporting documentation to document and settle events covered under an insurance policy. Such events may include, without limitation, medical treatment, medical supplies or other insured events that may reveal health-related information. In this context, users may submit receipts, invoices or other supporting documents to the Pliant platform in connection with claims or reimbursements. Such documents may contain information relating to health.

In connection with the use of the Pliant mobile app and the submission of such documentation, the categories of personal data that may be processed may include special categories of personal data within the meaning of Article 9 GDPR. This may include, in particular, information relating to medical services or supplies, healthcare provider details, as well as personal identifiers appearing on the submitted documents (such as the card user's name or identification number).

Pliant processes health-related personal data solely for the purposes of providing the platform services, facilitating reimbursements and supporting claims handling in the insurance context. The processing of health-related personal data concerning users is based on the explicit consent of the data subject in accordance with Article 9(2)(a) GDPR. Consent is obtained when the user either applies for or is provided with the card in the insurance context, and/or actively submits receipts, invoices or other supporting documents via the Pliant mobile app for reimbursement or claims handling purposes. Consent may be withdrawn at any time with future effect, e.g. by writing an email to privacy@getpliant.com. The withdrawal of consent does not affect the lawfulness of processing carried out on the basis of consent prior to its withdrawal.

In relation to Pliant's direct customers (such as insurance companies), the processing of information necessary to facilitate reimbursements and settle payments for insured events is carried out for the performance of the contract

Informationen zur Erfüllung des Vertrags zwischen Pliant und dem jeweiligen Kunden gemäß Art. 6 Abs. 1 b) DSGVO.

8. Intercom

Wir verwenden in unserer Mobile-App Intercom, eine Messenger- und Kommunikationsplattform, mit der wir verschiedene Aspekte der Kundenkommunikation und unseres Online-Marketings abdecken, u.a. Chat-Funktion, In-App Mitteilungen, Erinnerungen, Umfragen. Intercom ist ein Softwareunternehmen aus den USA mit einer Niederlassung in Irland.

Rechtsgrundlage der Datenverarbeitung ist, abhängig vom jeweiligen Verwendungszweck, Art. 6 Abs. 1 lit. a DSGVO (Einwilligung), Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) oder Art. 6 Abs. 1 lit. f DSGVO (berechtigzte Interessen, die Kontaktaufnahme mit unseren Kunden zu erleichtern).

Die personenbezogenen Daten werden so lange aufbewahrt, wie sie zur Erfüllung des Verarbeitungszwecks erforderlich sind. Die Daten werden gelöscht, sobald sie für die Zweckerreichung nicht mehr erforderlich sind.

Im Rahmen der Verarbeitung via Intercom können Daten in die USA übermittelt werden. Die Sicherheit der Übermittlung wird über sog. Standardvertragsklauseln abgesichert, welche gewährleisten, dass die Verarbeitung der personenbezogenen Daten einem Sicherheitsniveau unterliegen, das dem der DSGVO entspricht. Zudem nimmt die US - Gesellschaft Intercom, Inc. am EU-U.S. Data Privacy Framework teil; für am EU-U.S. Data Privacy Framework teilnehmende Unternehmen hat die EU - Kommission einen sog. Angemessenheitsbeschluss gefasst, durch den festgelegt wird, dass ein Drittland oder eine internationale Organisation ein angemessenes Schutzniveau für personenbezogene Daten bietet.

9. Google Firebase (Analytics)

Zur Verbesserung unseres Pliant Mobile App-Angebotes nutzen wir Google Firebase von Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA („Firebase“) insbesondere die Services Crashlytics, Pliant App Distribution, Google Analytics und Cloud Messaging. Zweck der Verwendung von Firebase ist, die Nutzung unserer Pliant Mobile-App zu analysieren. Google nutzt dazu Cookies sowie die Werbe-ID Ihres Endgerätes. Mithilfe von Firebase werden Informationen über die Benutzung der Pliant Mobile-App erfasst, an Google übertragen und in

between Pliant and the respective customer in accordance with Article 6(1)(b) GDPR.

8. Intercom

We use Intercom in our mobile app, a messenger and communication platform that we use to cover various aspects of customer communication and our online marketing, including chat function, in-app messages, reminders, surveys. Intercom is a software company based in the US with a branch in Ireland.

Legal basis for data processing is, depending on the respective purpose of use, Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. b GDPR (performance of contract) or Art. 6 para. 1 lit. f GDPR (legitimate interests to facilitate contact with our customers).

The personal data are kept for as long as they are necessary to fulfill the purpose of the processing. The data will be deleted as soon as they are no longer required to achieve the purpose.

In the context of processing via Intercom, data may be transmitted to the USA. The security of the transmission is achieved by so-called standard contractual clauses, which ensure that the processing of personal data is subject to a security level that corresponds to that of the GDPR. In addition, the U.S. entity Intercom, Inc. participates in the EU-U.S. Data Privacy Framework; for companies participating in the EU-U.S. Data Privacy Framework, the EU Commission has issued a so-called adequacy decision, which determines that a third country or an international organization offers an adequate level of protection for personal data.

9. Google firebase (Analytics)

To improve our Pliant mobile app offering, we use Google Firebase from Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA ("Firebase") in particular the services Crashlytics, Pliant App Distribution, Google Analytics and Cloud Messaging. The purpose of using Firebase is to analyze the use of our Pliant mobile app. Google uses cookies and the advertising ID of your end device for this purpose. With the help of Firebase, information about the use of the Pliant mobile app is collected, transmitted to Google and stored within their

deren Infrastruktur gespeichert. In unserem Auftrag wertet Google die Daten zur Art und Weise der Ihrer Nutzung unserer Pliant Mobile-App aus. Die so gesammelten Daten werden nicht mit Ihren sonstigen Profildaten zusammengeführt, sondern gehen in eine anonyme Statistik ein. Über die gewonnenen Statistiken können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten.

Rechtsgrundlage der Datenverarbeitung ist Ihre Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO. Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden, z.B. indem Sie in den Geräteeinstellungen die Nutzung der Werbe-ID beschränken oder den Schieberegler unter Profileinstellungen und Präferenzen für Firebase aktivieren bzw. deaktivieren. Weitere Informationen finden Sie [hier](#) sowie in den [Datenschutzinformationen](#) von Firebase.

10. Speicherdauer

Wir löschen die verarbeiteten personenbezogenen Daten, wenn sie für die vorgenannten Verarbeitungszwecke nicht mehr erforderlich sind und gesetzliche Aufbewahrungspflichten einer Löschung nicht entgegenstehen.

11. Weitergabe an Dritte

Ihre Daten geben wir nur an Dritte weiter, wenn Sie sich hiermit einverstanden erklärt haben oder wir hierzu aufgrund einer Rechtsgrundlage berechtigt oder verpflichtet sind.

Folgende Kategorien von Empfängern erhalten Ihre Daten:

- Kartenherausgeber zur Durchführung gesetzlicher Anforderungen
- Mit uns verbundene Unternehmen bzw. unsere Partnerbank zur Einrichtung und Führung eines Abrechnungskontos bzw. zur Zurverfügungstellung der Kreditlinie und hiermit erforderlichen Erfüllung gesetzlicher Anforderungen
- Kartenbüro zur Ausstellung der Karte
- Unternehmen zur Verarbeitung von Kartenzahlungen und Daten von Karteninhabern
- Anbieter von Karten-Zusatzleistungen (wie z.B. Versicherungsdienstleister, Anbieter von Flughafen-Lounges).

12. Partner-Integration

Wenn Sie Kreditkarten-Funktionen über die Anwendung eines Pliant-Partners nutzen (Partner-Integration), übermitteln

infrastruktur. On our behalf, Google evaluates the data on the way you use our Pliant mobile app. The data collected in this way is not merged with your other profile information, but goes into anonymous statistics. The statistics obtained allow us to improve our offer and make it more interesting for you as a user.

The legal basis for the data processing is your consent according to Art. 6 (1) lit. a DSGVO. Consent can be revoked at any time with effect for the future, e.g. by restricting the use of the advertising ID in the device settings or by activating or deactivating the slider under Profile Settings and Preferences for Firebase. You can find more information [here](#) and in the [privacy information](#) of Firebase.

10. Storage duration

We delete processed personal data when they are no longer required for the aforementioned processing purposes and no statutory retention obligations prevent deletion.

11. Transfer to third parties

We will only pass on your data to third parties if you have agreed to this or if we are entitled or obliged to do so on by virtue of a legal basis.

The following categories of recipients receive your data:

- Card issuer for the implementation of legal requirements
- Our affiliated companies respectively our partner bank for setting up and maintaining a settlement account respectively providing a credit line and thereby fulfilling legal requirements
- Card office for issuing the card
- Companies for processing card payments and cardholder data
- Service providers to support the sales team (shared growth)

12. Partner integration

If you use credit card functions via the application of a Pliant partner (partner integration), we transmit credit card and

wir Kreditkarten- und Transaktionsdaten, die zur Nutzung der vom Partner über seine Anwendung zur Verfügung gestellten Kreditkarten-Funktionen erforderlich sind (z.B. Name des Kartennutzers, Kartennummer, Betrag, Datum, Uhrzeit, Händlername), an den jeweiligen Partner. Wir und der jeweilige Partner verarbeiten die Daten insoweit als sog. gemeinsam Verantwortliche i.S.v. Art. 26 DSGVO und haben diesbezüglich Vereinbarungen festgelegt, wer von uns welchen datenschutzrechtlichen Verpflichtungen nachkommt; den wesentlichen Inhalt stellen wir Ihnen auf Anfrage zur Verfügung. Weitere Informationen zu den über die Partner-Anwendung verarbeiteten Daten können Sie den Datenschutzhinweisen des Partners entnehmen. Bei Fragen zur Wahrung der Betroffenenrechte können Sie sich sowohl an uns (u.a. per E-Mail an support@getpliant.com) als auch an den jeweiligen Partner wenden.

13. Auftragsverarbeiter

Wir geben Ihre Daten im Rahmen einer Auftragsverarbeitung gem. Art. 28 DSGVO an Dienstleister weiter, die uns beim Betrieb unserer Mobile-App und der damit zusammenhängenden Prozesse unterstützen. Unsere Dienstleister sind uns gegenüber streng weisungsgebunden und entsprechend vertraglich verpflichtet.

Dies sind Dienstleister der folgenden Kategorien:

- Hosting-Dienstleister / Cloud-Dienstleister für den Betrieb unserer Server und der Pliant Mobile-App
- Entwicklungsdienstleister für Programmierung, Entwicklung, Wartung und Support von Software-Anwendungen
- SMS-Versand-Dienstleister für den Versand von Bestätigungscodes (2-Faktor-Authentifizierung)
- Dienstleister für Push-Benachrichtigungen
- Software-Dienstleister zur Abdeckung verschiedener Aspekte unseres Marketings sowie zur Kundenkommunikation und -verwaltung (z.B. CRM-System, Office-Lösungen, Telefonie, Vertragsverwaltung)
- E-Mail-Versand-Dienstleister für den Versand von Newslettern
- Dienstleister zur Sicherstellung der IT-Sicherheit
- Dienstleister im Rahmen des LogIn-Prozesses
- Dienstleister für die automatisierte Dokumentenverarbeitung
- Dienstleister zur Zahlungsabwicklung
- Analysedienstleister für die Auswertung von Daten und Analyse der Benutzung der Pliant Mobile-App.

credit card transaction data required to use the credit card functions provided by the partner via its application (e.g. name of the card user, card number, amount, date, time, merchant name) to the respective partner. In this respect, we and the respective partner process the data as so-called joint controllers within the meaning of Art. 26 GDPR and have concluded agreements as to which of us fulfills which data protection obligations; we will provide you with the essential content upon request. Further information on the data processed via the partner application can be found in the partner's data protection notices. If you have any questions regarding the assertion of data subject rights, you can contact us (by email to support@getpliant.com, among others) as well as the respective partner.

13. Data processors

We pass on your data to service providers who support us in the operation of our mobile app and the associated processes within the framework of data processing on behalf pursuant to Art. 28 GDPR. Our service providers are strictly bound to us by instructions and are contractually obligated accordingly.

These are service providers of the following categories:

- Hosting service providers / cloud service providers for the operation of our servers and of the Pliant mobile app
- Development service providers for programming, development, maintenance and support of software applications
- SMS dispatch service providers for sending confirmation codes (2-factor authentication)
- Service providers for push notifications
- Software service providers to cover various aspects of our marketing as well as for customer communication and management (e.g. CRM system, office solutions, VoIP, contract management)
- Email service providers for the transmission of newsletters
- Service providers for ensuring IT security
- Service providers in the context of the log-in process
- Service providers for automated document processing solutions
- Payment processing providers

- Analytics service provider for the evaluation of data and analysis of the use of the Pliant mobile app.

Soweit diese Dienstleister Zugriff auf Ihre Daten haben, geschieht das nur in unserem Auftrag und nach unseren Weisungen. Die Dienstleister wurden sorgfältig ausgewählt und sind zudem zur Einhaltung der geltenden Datenschutzbestimmungen verpflichtet worden. Sie erhalten nur in dem Umfang und für den benötigten Zeitraum Zugang zu Ihren Daten, der für die Erbringung der Leistungen erforderlich ist.

Die Server einiger von Pliant eingesetzten Dienstleister befinden sich in den USA und anderen Ländern außerhalb der Europäischen Union (EU) / des Europäischen Wirtschaftsraums (EWR). Nach Möglichkeit möchten wir dies vermeiden und nutzen nur Server mit Standort innerhalb der EU/im EWR. Unternehmen in Ländern außerhalb der EU/des EWR unterliegen einem Datenschutzgesetz, das allgemein personenbezogene Daten nicht in demselben Maße schützt, wie es in den Mitgliedstaaten der Europäischen Union der Fall ist. Es gibt aktuell keinen Beschluss der EU-Kommission, dass Drittländer allgemein ein angemessenes Schutzniveau bieten. Soweit Ihre Daten in einem Land verarbeitet werden, welches nicht über ein anerkannt hohes Datenschutzniveau wie die Europäische Union/der Europäische Wirtschaftsraum verfügt, stellt Pliant über vertragliche Regelungen oder andere anerkannte Instrumente sicher, dass das Datenschutzniveau weitestgehend gesichert wird.

14. Einsatz von KI-Systemen

Wir setzen zur Optimierung unserer internen Arbeitsabläufe und zur Verbesserung unserer Dienstleistungen KI-basierte Softwarelösungen ein. Diese Technologien unterstützen unsere Mitarbeitenden bei manuellen und repetitiven Tätigkeiten, beispielsweise bei der Erstellung von internen Zusammenfassungen, der internen Dokumentation oder bei der Vorformulierung von Texten und E-Mails.

Diese Tools wirken ausschließlich unterstützend und treffen keine eigenen Entscheidungen. Es erfolgen keine automatisierten Entscheidungen im Sinne von Art. 22 DSGVO. Die von KI generierten Ergebnisse werden durch unsere Mitarbeitenden geprüft, überarbeitet und finalisiert. Wir setzen keine Hochrisiko-KI-Systeme im Sinne der KI-VO ein. Die KI-Systeme, die für diese Zwecke eingesetzt werden, nutzen personenbezogene Daten nicht zur Schulung oder Weiterentwicklung der zugrunde liegenden KI-Modelle.

Insofar as these service providers have access to your data, this is only done on our behalf and in accordance with our instructions. The service providers have been carefully selected and are also obliged to comply with the applicable data protection regulations. They will only have access to your data to the extent and for the period required to provide the services.

The servers of some service providers used by Pliant are located in the USA and other countries outside the European Union (EU) / European Economic Area (EEA). Where possible, we would like to avoid this and only use servers located within the EU/EEA. Companies in countries outside the EU/EEA are subject to data protection laws that do not generally protect personal data to the same extent as they do in the member states of the European Union. There is currently no decision by the EU Commission that third countries generally provide an adequate level of protection. Insofar as your data is processed in a country that does not have a recognized high level of data protection such as the European Union/European Economic Area, Pliant ensures that the level of data protection is secured to the greatest possible extent by means of contractual regulations or other recognized instruments.

14. Use of AI systems

As part of our internal processes, we use AI-based software solutions to optimize our internal workflows and to improve our services. These technologies support our employees in manual and repetitive tasks, including but not limited to preparation of internal summaries, internal documentation, or pre-drafting of texts and emails.

These tools operate exclusively in a supportive capacity and do not make independent decisions. No automated decision-making within the meaning of Art. 22 GDPR takes place. Results generated by AI are reviewed, revised, and finalized by our employees. We do not use high-risk AI systems within the meaning of the AI Act. The AI systems used do not use personal data to train or further develop the underlying AI models.

Die Verarbeitung personenbezogener Daten in diesem Zusammenhang erfolgt auf Grundlage unseres berechtigten Interesses (Art. 6 Abs. 1 f) DSGVO) an einer effizienten Gestaltung unserer internen Prozesse und der Sicherstellung unserer Servicequalität. Sie haben das Recht, dieser Verarbeitung jederzeit aus Gründen, die sich aus Ihrer besonderen Situation ergeben, zu widersprechen. Wenn Sie von Ihrem Widerspruchsrecht Gebrauch machen, werden wir Ihre personenbezogenen Daten für diese Zwecke nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.

15. KI-gestützter Chatbot

Zusätzlich zu den in Abschnitt 8 beschriebenen Intercom-Funktionalitäten nutzen wir auch bestimmte KI-gestützte Automatisierungsfunktionen von Intercom, einschließlich des Chatbots „Fin AI“ von Intercom. Der Chatbot dient der Beantwortung allgemeiner Anfragen. Die Antworten werden überwiegend auf Grundlage von den Nutzern zur Verfügung gestellten bzw. zugänglichen Wissensquellen generiert, wie zum Beispiel Inhalten aus unserem Pliant Help Centre sowie sonstigen öffentlich verfügbaren Support- und Produktinformationen.

Bei der Nutzung des Chatbots können Inhalte der Konversation sowie zugehörige Metadaten in dem Umfang verarbeitet werden, der zur Bereitstellung, Absicherung und Qualitätssicherung der Support-Funktion erforderlich ist. Intercom verarbeitet diese Daten als Auftragsverarbeiter gemäß Art. 28 DSGVO auf Grundlage unseres Auftragsverarbeitungsvertrags. Zur Generierung der Antworten werden keine personenbezogenen Daten verwendet; ebenso werden keine personenbezogene Daten aus Chatbot-Interaktionen zur Schulung, Verbesserung oder Weiterentwicklung der zugrunde liegenden KI-Modelle von Fin AI oder anderer von Intercom betriebener Foundation-Modelle genutzt.

Darüber hinaus entwickeln und betreiben wir einen eigenen KI-gestützten Chatbot „Pliant Mind“, der in die Pliant Mobile-App integriert ist. Pliant Mind unterstützt Nutzer, indem er Anfragen auf Grundlage von den Nutzern zugänglichen Wissensquellen beantwortet, wie etwa Inhalten aus unserem Pliant Help Centre sowie sonstigen öffentlich verfügbaren Support- und Produktinformationen. Personenbezogene Daten werden nicht zur Schulung,

The processing of personal data in this context is based on our legitimate interest (Art. 6 (1)(f) GDPR) in efficiently designing our internal processes and ensuring the quality of our services. You have the right to object to the processing at any time on grounds relating to your particular situation. If you exercise your right to object, we will no longer process your personal data for these purposes unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms, or the processing is necessary for the establishment, exercise or defence of legal claims.

15. AI-supported chatbot

In addition to the Intercom functionalities described in Section 8, we also use certain AI-supported automation features of Intercom, including the Intercom’s chatbot “Fin AI”. The chatbot is intended to respond to general inquiries. Its responses are primarily generated based on knowledge sources made available to users, such as content from our Pliant Help Centre and other publicly available support and product information.

When using the chatbot, conversation content and related metadata may be processed to the extent necessary to provide, secure and ensure the quality of the support functionality. Intercom processes such data as our processor pursuant to Art. 28 GDPR under our data processing agreement. No personal data is used to generate responses, nor is any personal data from chatbot interactions used for the purpose of training, improving or further developing the underlying AI models of Fin AI or other foundation models operated by Intercom.

In addition, we are developing and operating our own AI-supported chatbot “Pliant Mind” integrated into the Pliant mobile app. Pliant Mind supports users by answering inquiries based on knowledge sources made available to users, such as content from our Pliant Help Centre and other publicly available support and product information. No personal data is used for the training, improvement or further development of Pliant Mind. Any processing for development purposes would be carried out on a case-by-case basis,

Verbesserung oder Weiterentwicklung von Pliant Mind verwendet. Eine Verarbeitung personenbezogener Daten zu Entwicklungszwecken würde nur im Einzelfall erfolgen und setzt stets Ihre vorherige ausdrückliche und informierte Einwilligung voraus.

Die Verarbeitung personenbezogener Daten in diesem Zusammenhang erfolgt auf Grundlage unseres berechtigten Interesses gemäß Art. 6 Abs. 1 f) DSGVO an der effizienten Gestaltung unserer internen Prozesse und der Sicherstellung der Qualität unserer Dienstleistungen. Sie haben das Recht, dieser Verarbeitung jederzeit aus Gründen, die sich aus Ihrer besonderen Situation ergeben, zu widersprechen. Wenn Sie von Ihrem Widerspruchsrecht Gebrauch machen, werden wir Ihre personenbezogenen Daten für diese Zwecke nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.

16. Pflicht zur Bereitstellung der Daten

Die Bereitstellung Ihrer Daten ist gesetzlich nicht vorgeschrieben und erfolgt freiwillig. Für die Nutzung der Pliant Mobile App-Services ist die Anmeldung mit den Benutzerdaten sowie die Bereitstellung des Zugriffs auf Bildergalerie und Dateisystem aber erforderlich, damit wir die Funktionen der Pliant Mobile-App zweckgemäß (siehe oben) umsetzen zu können. Ohne diese Daten können wir unser Pliant Mobile App-Angebot nicht erbringen.

17. Ihre Rechte als betroffene Person

Bei der Verarbeitung Ihrer personenbezogenen Daten gewährt die DSGVO Ihnen als betroffene Person bestimmte Rechte:

Auskunftsrecht (Art. 15 DSGVO)

Sie haben das Recht, eine Bestätigung darüber zu verlangen, ob Sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so haben Sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf die in Art. 15 DSGVO im Einzelnen aufgeführten Informationen.

Recht auf Berichtigung (Art. 16 DSGVO)

strictly contingent upon your prior explicit and informed consent.

The processing of personal data in this context is based on our legitimate interest (Art. 6(1)(f) GDPR) in efficiently designing our internal processes and ensuring the quality of our services. You have the right to object to the processing at any time on grounds relating to your particular situation. If you exercise your right to object, we will no longer process your personal data for these purposes unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms, or the processing is necessary for the establishment, exercise or defence of legal claims.

16. Obligation to provide the data

The provision of your data is not required by law and is voluntary. However, for the use of the Pliant mobile app services, the login with the user data as well as the provision of access to the image gallery and file system is required so that we can implement the functions of the Pliant mobile app according to purpose (see above). Without this data we cannot provide our Pliant mobile app services.

17. Your Rights as a Data Subject

When processing your personal data, the GDPR grants you certain rights as a data subject:

Right of access (Article 15 GDPR)

You have the right to request confirmation as to whether personal data concerning you are being processed; if this is the case, you have the right to be informed about these personal data and to receive the information listed in detail in Article 15 GDPR.

Right of rectification (Art. 16 GDPR)

Sie haben das Recht, unverzüglich die Berichtigung Sie betreffender unrichtiger personenbezogener Daten und ggf. die Vervollständigung unvollständiger Daten zu verlangen.

Recht auf Löschung (Art. 17 DSGVO)

Sie haben das Recht, zu verlangen, dass Sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 DSGVO im Einzelnen aufgeführten Gründe zutrifft.

Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Sie haben das Recht, die Einschränkung der Verarbeitung zu verlangen, wenn eine der in Art. 18 DSGVO aufgeführten Voraussetzungen gegeben ist, z. B. wenn Sie Widerspruch gegen die Verarbeitung eingelegt haben, für die Dauer der Prüfung durch den Verantwortlichen.

Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

In bestimmten Fällen, die in Art. 20 DSGVO im Einzelnen aufgeführt sind, haben Sie das Recht, die Sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten bzw. die Übermittlung dieser Daten an einen Dritten zu verlangen.

Widerspruchsrecht (Art. 21 DSGVO)

Werden Daten auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO (Datenverarbeitung zur Wahrung berechtigter Interessen) oder auf Grundlage von Art. 6 Abs. 1 lit. e DSGVO (Datenverarbeitung zur Wahrung öffentlichen Interesse oder in Ausübung öffentlicher Gewalt) erhoben, steht Ihnen das Recht zu, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Widerspruch einzulegen. Wir verarbeiten die personenbezogenen Daten dann nicht mehr, es sei denn, es liegen nachweisbar zwingende schutzwürdige Gründe für die Verarbeitung vor, die gegenüber Ihren Interessen, Rechten und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Beschwerderecht bei einer Aufsichtsbehörde (Art. 77 DSGVO)

Sie haben gemäß Art. 77 DSGVO das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden Daten gegen datenschutzrechtliche Bestimmungen verstößt. Das Beschwerderecht kann insbesondere bei einer Aufsichtsbehörde in dem Mitgliedstaat Ihres gewöhnlichen Aufenthaltsorts, Ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes geltend gemacht werden.

You have the right to request the correction of any inaccurate personal data relating to you and, where applicable, the completion of any incomplete data without delay.

Right to erasure (Art. 17 GDPR)

You have the right to request that personal data concerning you be deleted without delay, provided that one of the reasons listed in detail in Art. 17 GDPR applies.

Right to the restriction of processing (Art. 18 GDPR)

You have the right to request the restriction of processing if one of the conditions listed in Art. 18 GDPR applies, for example, if you have objected to the processing, for the duration of the review by the controller.

Right to data portability (Art. 20 GDPR)

In certain cases, which are listed in detail in Art. 20 GDPR, you have the right to receive the personal data concerning you in a structured, common and machine-readable format, or to request the transfer of this data to a third party.

Right of objection (Art. 21 GDPR)

If data are collected on the basis of Art. 6(1)(f) GDPR (data processing for the protection of legitimate interests), or on the basis of Article 6(1)(e) GDPR (data processing for the protection of public interests, or for the exercise of official authority), you have the right to object to the processing at any time on grounds relating to your particular situation. We will then no longer process the personal data unless there are proven compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing serves the assertion, exercise or defense of legal claims.

Right of appeal to a supervisory authority (Art. 77 GDPR)

In accordance with Art. 77 GDPR, you have the right to lodge a complaint with a supervisory authority if you are of the opinion that the processing of data concerning you violates data protection regulations. The right of appeal may in particular be exercised before a supervisory authority in the Member State of your habitual residence, place of work, or place of the alleged infringement.

