Privacy Policy

For Konrad Langenberg Software, compliance with data protection laws is not only a legal obligation, but a necessary element of trust. In the following we want to transparently inform you about the methods, scope and purpose of the processing of your personal data which might be collected from you while visiting this website. We will also inform you about your rights.

Controller

As operator of the website https://vikunja.cloud/, the Konrad Langenberg Software, Willy-Brandt-Allee 31A, 23554 Lübeck, Germany (subsequently referred to as "we" and "us") is the controller pursuant to Art. 4 No. 7 of the General Data Protection Regulation (GDPR). You can contact us at support@vikunja.io with any questions about this privacy policy.

Data protection officer

According to Art. 37 GDPR and § 38 Bundesdatenschutzgesetz (BDSG) we are not obligated to appoint a data protection officer. For any questions regarding the protection of your data and to claim the rights stated hereafter, you can contact us at any time via the contact information mentioned above.

Rights of the data subject

Your rights as a data subject

As a data subject you have the following rights concerning your personal data. You have

- the **right of access** to information on – among others – the purposes of the processing, the categories of personal data concerned, the envisaged period for which the personal data will be stored as well as possible recipients, pursuant to and in accordance with the requirements of Art. 15 GDPR and § 34 BDSG
- the **right to rectification and to erasure** of incorrect or incomplete data pursuant to and in accordance with the requirements of Art. 16 and 17 GDPR and § 35 BDSG.
- the **right to restriction of processing** pursuant to and in accordance with the requirements of Art. 18 GDPR and § 35 (1) 2 BDSG.

- the **right to object**, on grounds relating to your particular situation, to the processing of personal data concerning you which is based on point (e) or (f) of Article 6(1) pursuant to and in accordance with the requirements of Art. 21 (1) GDPR.
- the **right to withdraw** your given consent at any time, which does, however, not affect the lawfulness of processing based on consent before its withdrawal according to Art. 7 (3) GDPR.
- the **right to data portability** in a structured, commonly used and machine-readable format pursuant to and in accordance with the requirements of Art. 20 GDPR
- You have, pursuant to and in accordance with the requirements of Art. 22 GDPR, the **right not to be subject to a decision based solely on automated processing**, including profiling, which entails legal effects concerning you or significantly affects you in a similar way.
- Furthermore pursuant to Art. 77 GDPR you have the **right to lodge a complaint with a supervisory authority** about the processing of your personal data by us, in particular in the member state of your habitual residence, place of work or place of the alleged infringement.

Procedure

When you claim your rights toward us according to the GDPR and the BDSG, we will process the data you thereby submit to fulfill your claims.

Subsequently we will store the data submitted by you and the data submitted by us to you in return for the purpose of documentation until the expiry of the regulatory offense's limitation period (3 years).

The lawfulness of processing and storing the data is based on Art. 6 (1) point (f) GDPR (legitimate interest of data processing). The legitimate interest results from our obligation to fulfill your requests and the need to exonerate ourselves in possible fine proceedings by proving that we have lawfully fulfilled your requests.

You can object to the processing of your personal data based on our legitimate interest at any time under the premises of Art. 21 GDPR. Please use the contact details provided in the imprint. We would like to note that the processing of your personal data is mandatory for the verification of compliance with data protection rights of the data subject according to Art. 21 (1) GDPR, as other methods of verification do not exist or are not equally suitable.

Data protection measures / arrangements

We secure our website and other systems — and thus your data — through technical and organizational measures against loss, destruction, access, change or dissemination through unauthorized persons. In particular your personal data will be transmitted encrypted through the internet. Therefore we operate with the coding system TLS (Transport Layer Security).

Having said this, the transmission of information via internet is never fully safe, which is why we cannot guarantee the safety of the data transmitted by our website to a 100%.

Data processing modalities

Sources and categories of personal data

We process your personal data insofar as it is necessary for the statement, content-related configuration or modification of a contractual relationship between you and us (inventory data). In particular the following can be inventory data: Name, form of address, contact details (postal address, telephone, email address), date of birth , etc.

Furthermore we process your usage data. Usage data is data that is collected when you interact with our web content and our services, in particular your IP address, start and end of your visit on our website and information on the contents you have viewed on our website.

We collect the data mentioned directly from you (e.g., through the visit of our website), or, provided that it is permitted by data protection laws, from third parties or respectively from publicly accessible sources (e.g., commercial or association register, the press, media, internet).

Data transfer to third party countries outside the EU

All information we acquire from or on you will generally be processed on servers located within the European Union. A transmission of your data or a processing of your data in third party countries will occur without your explicit consent solely if this is legally intended or permitted and if an appropriate data protection level is guaranteed in the third party country or if there are contractual obligations in place via the EU’s so-called standard contractual clauses.

With regard to data transfers to the United States, the European Commission has issued an adequacy decision known as the EU-U.S. Data Privacy Framework, which ensures an adequate level of protection for the transfer of personal data by companies participating in the EU-U.S. Data Privacy Framework.

The adequacy decision applies only to companies that have officially self-certified under the Data Privacy Framework. Outside of this framework, the U.S. is considered a so-called “unsafe third

country.” When personal data is transferred to the U.S., there is a risk that U.S. security authorities may access this data under the “Cloud Act.” EU citizens have no effective legal remedies against these measures, either in the U.S. or in the EU.

To the extent that we use services that transfer personal data to the U.S., it is up to the respective service provider to ensure that the company is certified under the EU-U.S. Privacy Framework.

Data disclosure, processing on behalf of the controller

We will never illicitly disclose your personal data to third parties. However, we may disclose your data to third parties, in particular if you have agreed to data disclosure, if the disclosure is necessary to fulfill our legal obligations or if we are obligated or authorized to disclose said data by law or administrative or judicial orders. In particular this may be the case for the purposes of criminal proceedings, averting of dangers or enforcement of intellectual property rights.

We may disclose personal data gathered from you to third parties particularly in the context of contract fulfillment, for example to delivery services or the service used for payment, to the extent that this is necessary for contractual performance. You can find the individual service providers down below under the section "Third party services".

Under certain circumstances we may transmit your data to external service providers which process data on our behalf and in accordance with our instructions (data processor) to simplify and disburden our own data processing. Every data processor will be bound by contract according to Art. 28 GDPR. In particular this means that the data processor has to offer sufficient guarantees that appropriate technical and organizational measures are implemented so that data processing is compliant with the requirements of the GDPR and your rights as a data subject are ensured. Despite commissioning data processors we remain the responsible party for the processing of your personal data according to the GDPR.

Purpose / Objective of the data processing

In general we will use the data solely for the purpose for which the data was gathered. We may subsequently process the data for another, different purpose, provided that this other purpose is not incompatible with the original purpose (Art. 5 (1) point (c) GDPR).

Storage period

Unless specified otherwise, we will store data gathered from you only for as long as it is necessary for each respective purpose and unless there are legal retention obligations preventing deletion, for example from commercial law or tax law.

Individual processing activities / operations

In the following we want to outline as transparently as possible, which of your data we will process under which circumstances, on what basis and for what purpose.

Server log files

Each time our website is accessed, the following general information will be automatically sent to our servers by your browser (so called server log files): Your IP address, product and version information of the browser and operating system used (so called user agent), the webpage from which the access originated (so called referer), date and time of the request and possibly your internet service provider. Furthermore the status and the volume of data will be recorded.

This information is logged by the server, stored in a table, and retained there temporarily (so-called server log files). By analyzing these log files, we can identify and subsequently correct errors on the website, determine the website's traffic volume at specific times and make adjustments or improvements based on that information, as well as ensure the security of the server by tracing the IP addresses from which attacks on our server were launched.

The server log files are deleted on a regular basis (usually after 3 months). Should any of the security-related events mentioned above occur, we reserve the right, within the scope of our legitimate interest, to retain this data for a longer period for the purposes stated above. Once the specified purpose has been fulfilled, the data will be deleted after a reasonable period of time.

The legal basis for the usage of these server log files is Art. 6 (1) point (f) GDPR (legitimate interest of data processing). The legitimate interest arises from the necessity to operate our website, especially to discover and remove website errors, to determine the utilization of the webpage, to make adjustments and improvements and to guarantee the security of the system. You can object to the processing of your personal data based on the legitimate interest at any time under the premises of Art. 21 GDPR. Please use the contact details provided in the imprint. We would like to point out that the processing of your server log files is mandatory in accordance with Art. 21 (1) GDPR, as otherwise the website cannot be operated at all.

Cookies

To improve user-friendliness we use so called "cookies" and the “web Storage” of your browser on our website.

What Cookies are

Simply put, a cookie is a small text file, that stores data about visited websites. Cookies can store a kind of "user profile", including information like your preferred language or other page set-ups, that are required by our website to be able to offer you certain services. This file will be stored on your terminal device and also helps with recognizing you in the event of a new visit to our website.

Under certain circumstances we can gather information on your preferred activities on our webpage through these cookies, and thus align the webpage according to your individual interests and even increase the navigation speed on our website.

How you can avoid Cookies

You can manually delete the cookies in your browser’s security settings at any time.

Optionally you can prevent the storage of cookies by default via the respective settings of your browser. Please do note that in this case you possibly will not be able to use all functions of our website entirely or that errors may occur in the presentation or usage of the website.

Third party Cookies

It is possible that third party service providers, with the help of whom we develop and operate our website, independently store cookies on your terminal device, in particular through so called plugins (see section below "Third-party services"). Should you solely want to accept our own cookies, but not the cookies of these third parties, you can prevent these third party cookies by use of the respective browser setting "Block third-party cookies".

Which Cookies are implemented

In detail our webpage places the following cookies:

Name	Description	Domain	Validity	Third party access
vikunja_cloud_session	This cookie is used to log you in to use the service and recognize you for as long as you are logged in.	vikunja.cloud	2 Hours	No
XSRF-TOKEN	Used to protect the website against Cross-Site Request Forgery (CSRF) attacks by	vikunja.cloud	2 Hours	No

Name	Description	Domain	Validity	Third party access
	verifying that requests originate from the legitimate website.			
remember_web_*	Only set if you choose "Remember me" when logging in. Keeps you logged in across browser sessions so you don't have to log in again. Removed when you log out.	vikunja.cloud	400 Days	No

The legal basis for the use of cookies that are absolutely necessary for the function of the website (e.g. shopping cart cookie, session cookie) is Art. 6 para. 1 p. 1 letter f) GDPR (legitimate interest in data processing) as well as §25 para. 2 No. 2 TTDSG (absolute necessity for the provision of a digital service expressly requested by the user). The legitimate interest results from our need to be able to offer you a functioning website. Cookies are necessary for this because they are an integral part of current Internet technology and without cookies many functions of current websites would not be available. We therefore require cookies to provide you with the website in response to your request.

You can object to the processing of your data based on our legitimate interest at any time under the conditions of Art. 21 GDPR. To do so, please use the contact details provided in the imprint.

However, we would like to point out that the processing of your data in certain cookies is mandatory in the sense of Art. 21 (1) GDPR, as otherwise the website cannot be operated at all and we do not have the technical possibility to prevent the setting of cookies on certain individual end devices. However, you may be able to do this yourself in your browser. For more information on this, please look at the instructions for your browser.

Web Storage

What is Web Storage

Web storage is a technology for web applications that store data in a web browser. Web storage can be seen as a further development of cookies but differs from them in some respects.

In contrast to cookies, which can be accessed by both server and client, the web storage is completely controlled by the client. This means that data is not transferred to the server every time the website is accessed. Access is only possible locally via scripts on the website. Specifically, this

means that third parties cannot access the information stored on the website. Only you and we can access the locally stored data.

Legal basis

The legal basis for the use of web storage, which is absolutely necessary for the function of the website, is Art. 6 para. 1 p. 1 letter f) GDPR (legitimate interest in data processing) and §25 para. 2 No. 2 TTDSG (absolute necessity for the provision of a digital service expressly requested by the user). The legitimate interest results from our need to be able to offer you a functioning website. The Web Storage is necessary for this because it is an integral part of current Internet technology and without it many functions of current websites would not be available. We therefore require the Web Storage in order to provide you with the website in response to your request.

You can object to the processing of your data on the basis of our legitimate interest at any time under the conditions of Art. 21 GDPR. To do so, please use the contact details provided in the imprint.

However, we would like to point out that the processing of your data in web storage may be compulsory within the meaning of Art. 21 (1) GDPR, since otherwise the website cannot be operated at all and we do not have the technical option to prevent the usage on certain end devices. However, you may be able to do this yourself in your browser. For more information, please look at the instructions for your browser.

Registration on Vikunja Cloud

To gain access and use our Vikunja Cloud Services, you must register directly on our website. To register, you must provide your name, your email address and a password.

After submitting your registration, you will receive an activation email containing a confirmation link. Your registration will only be completed once you have confirmed your email address by clicking this link (double opt-in procedure). This serves to verify your email address and prevent unauthorized registrations using third-party email addresses.

We process the personal data you provide for the purpose of creating and managing your user account, verifying your email address and granting you access to the Vikunja Cloud Services.

The following information and content are stored in your user account:

- your name and email address
- all data you create within the Vikunja Cloud application at app.vikunja.cloud, such as tasks, projects and attachments; and

- if you subscribe to the service, your payment information as described in the "Stripe" section below.

The legal basis for the usage of data provided by you during the registration process is Art. 6(1)(b) GDPR, insofar as the processing is necessary to provide the requested community functionality.

Furthermore the legal basis for processing mandatory information is Art. 6 (1) point (f) GDPR (legitimate interest of data processing). Our legitimate interest lies in providing a functioning and secure platform, managing user accounts, ensuring reliable user authentication and enabling the provision and administration of the Vikunja Cloud services.

You can object to the processing of your personal data based on the legitimate interest at any time under the premises of Art. 21 GDPR. Please use the contact details provided in the imprint.

You can delete your user account at any time directly through your account profile. Upon deletion, your user account and the associated personal data will be deleted, unless statutory retention obligations or other legal grounds require continued storage.

If your access to Vikunja Cloud has ended, for example because your subscription ended, we delete your user account together with your Vikunja data six months after the end of your access. We remind you by email 30 days, 14 days and 3 days beforehand. Records we must keep under commercial and tax law, such as invoices, are retained for the statutory periods.

If you cancel your subscription and give a reason, we keep the reason after your user account has been deleted, together with the type and date of the cancellation but without any link to you or your account, to understand why customers leave and to improve the service. Please do not include personal details in the reason.

Usage of our web shop

If you want to order something from our web shop, it is mandatory for the conclusion of the contract and the processing of your order that you provide certain information. These entries that are indispensable for the transaction are marked separately, all other entries can be made voluntarily. We will process the data disclosed by you during the order process solely for purposes of handling your order. If you do not enter the required information, we will not be able to process your order.

To handle the order we will redirect you to our ordering software, which is provided by Stripe Payments Europe, Limited (SPEL), 1 Grand Canal Street Lower, D02 H210 Dublin, Ireland by our commission. Stripe Payments Europe, Limited is a subsidiary of Stripe, Inc., 510 Townsend Street, San Francisco, CA 94103, USA. You can find further information about the data privacy of Stripe at: https://stripe.com/en-de/privacy

Furthermore, in the interest of processing your order, it can be necessary to transmit your data to third parties, for example banks/payment service providers, logistics companies, etc. (You can find further information in our terms and conditions, as described above under "Data disclosure" as well as down below in the section "Third party services").

The legal basis for the usage of your data for processing your order is Art. 6 (1) point (b) GDPR (processing for the performance of a contract). The legal basis for the data disclosed by you voluntarily during the order process is Art. 6 paragraph 1 sentence 1 letter a) (consent of the data subject). You can revoke your consent with effect for the future at any time. Please use the contact details provided in the imprint.

Due to obligations from commercial law and tax law, we are required to retain your address, payment and order information for a period of ten years. However we will restrict the data processing after two years, meaning that your data will be solely used to adhere legal obligations.

To prevent unauthorized access to your personal data, especially financial data, by third parties, the ordering process is encrypted via TLS technology.

Furthermore we may process the data provided by you in order to inform you about interesting products from our portfolio or to provide you with technical information via email.

The legal basis for the usage of your contact details is Art. 6 (1) point (f) GDPR (legitimate interest of data processing). The legitimate interest results from our need to provide you with interesting information regarding our products and our company (direct advertisement).

You can object to the processing of your personal data based on the legitimate interest of direct advertisement at any time under the premises of Art. 21 GDPR. Please use the contact details provided in the imprint.

Hosting services

Our website is hosted on servers of external providers to ensure the efficient and secure provision of the website. Parts of Vikunja Cloud are hosted with Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany, which acts as a data processor for us in accordance with Art. 28 GDPR. Other parts of Vikunja Cloud are hosted at Scaleway, 8 RUE DE LA VILLE L'EVÊQUE 75008 PARIS 8, France, which we use as a data processor in accordance with Art. 28 GDPR.

Each time you visit the website, general information is automatically transmitted from your browser to the server (so-called server log files). For more information, see "Server log files" above.

The legal basis for the use of hosting service and the associated processing of your data is Art. 6 para. 1 p. 1 letter f) GDPR (Legitimate Interest in Data Processing). The legitimate interest arises from our need for a technically flawless presentation of our website without requiring in-depth knowledge of website programming and maintenance of IT systems. You can object to the processing of your data on the basis of our legitimate interest at any time under the conditions of Art. 21 GDPR. To do so, please use the contact details provided in the imprint. However, we would like to point out that the processing of your data in this context may be mandatory within the meaning of Art. 21 para. 1 GDPR, as otherwise the website cannot be operated at all without disproportionate effort.

Third party services

For simplification of our data processing and to extend the functionality of our website we use third party services and resources, for example plugins, external content, software or other external service providers (services). In doing so the possibility exists that personal data will be transmitted to the service provider. If required, to protect your data, we have contractually obligated the service provider according to Art. 28 GDPR to solely process the data according to our instructions. We would like to explicitly point out that we are regularly only responsible for the data acquisition and transmission by the service according to the GDPR, but not for a possible subsequential processing by the respective service provider.

In detail we use the following services:

Cloudflare

We use services of Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA ("Cloudflare") for the domain name system (DNS) of our domains, as a content delivery network (CDN) and to protect forms against automated abuse (captcha). Cloudflare acts as a data processor for us in accordance with Art. 28 GDPR.

When our domain names are resolved, Cloudflare's name servers process the requested domain name and the IP address of the requesting DNS resolver. Where content is delivered via Cloudflare's CDN or a form is protected by Cloudflare's captcha, Cloudflare additionally processes your IP address, the requested address, the date and time of the request and technical information about your browser and device, in order to deliver the content securely and to distinguish human visitors from automated requests.

It cannot be ruled out that Cloudflare processes data in the United States. Cloudflare, Inc. is certified under the EU-U.S. Data Privacy Framework (see "Data transfer to third party countries outside the

EU" above).

The legal basis is Art. 6 (1) point (f) GDPR (legitimate interest of data processing). Our legitimate interest lies in the reliable, fast and secure provision of our website and in protecting it against attacks and automated abuse. You can object to the processing of your personal data based on the legitimate interest at any time under the premises of Art. 21 GDPR. Please use the contact details provided in the imprint.

For more information, please refer to Cloudflare's privacy policy: https://www.cloudflare.com/privacypolicy/

Service providers connected with the processing of your order

We may transmit the personal data gathered from you within the scope of conclusion of the contract to third parties, for example to the transport company commissioned with the delivery, or to the service used for payment, insofar as it is necessary for the fulfillment of the contract.

The legal basis for the transmission of the data necessary for the conclusion of the order is Art. 6 (1) point (b) GDPR (processing for the performance of a contract). The provision and transmission is necessary, as your order cannot be processed otherwise.

The legal basis for the data transmission chosen by you voluntarily within the order process (for example for the delivery status via email) is Art. 6 (1) point (a) GDPR (consent of the data subject). You can revoke your consent with effect for the future at any time. Please use the contact details provided in the imprint.

In particular we use the following service providers:

Stripe

We use the Stripe service provided by Stripe Payments Europe, Limited (SPEL), 1 Grand Canal Street Lower, D02 H210 Dublin, Ireland, to process payments. Stripe Payments Europe, Limited is a subsidiary of Stripe, Inc., 510 Townsend Street, San Francisco, CA 94103, USA.

In case you want to purchase a subscription for Vikunja Cloud and proceed with the payment, you will be redirected to a website operated by Stripe. The payment process is carried out directly through Stripe. The personal and payment data you enter during the payment process, such as your name, billing information, email address and payment details (e.g. credit card or bank account information), are collected and processed by Stripe for the purpose of processing and verifying the payment.

Stripe may also process technical information required to securely process the payment, such as your IP address, browser and device information, as well as information about the transaction, including the date, time, amount and status of the payment.

We do not receive or store your complete payment details, such as your full credit card number or bank account details. We only receive the information necessary to manage your subscription and assign the payment to your Vikunja Cloud user account, such as the payment status and transaction-related information.

It cannot be ruled out that Stripe may also transfer your data to the United States and process it there. Stripe, Inc. complies with the requirements of the “EU-U.S. Data Privacy Framework.” The Privacy Framework Agreement governs the protection of personal data transferred from a member state of the European Union to the United States. It ensures that the transferred data is subject to a level of data protection in the United States comparable to that of the European Union. You can view the list of certified companies here: https://www.dataprivacyframework.gov/s/participant-search.

For details about the data collected and information on how Stripe processes the collected data, please refer to Stripe's Privacy Policy: https://stripe.com/en-de/privacy

Lexware Office

For the management of our accounting, we use the Lexware Office service provided by Haufe-Lexware GmbH & Co. KG, Munzinger Straße 9, 79111 Freiburg, Germany, as a data processor in accordance with Art. 28 GDPR.

The use of Lexware Office enables us to centralize and organize accounting-related data, process invoices and other financial documents, reconcile payments and maintain accurate and traceable accounting records. The use of a specialized accounting solution also supports the proper fulfilment of our accounting and documentation obligations and reduces the risk of errors arising from manual processing.

In particular, the following categories of personal data may be processed: master data (e.g. name, address and contact details), bank and payment information, invoice and receipt data, as well as usage-related and technical logs where required for the operation and security of the service.

Lexware Office uses approved subprocessors for additional functions. Where personal data is transferred to recipients outside the EU/EEA, appropriate safeguards in accordance with Art. 44 et seq. GDPR, in particular standard contractual clauses where applicable, are used.

Personal data is stored for as long as necessary for the respective accounting purposes and in accordance with applicable statutory retention obligations, in particular those arising from § 147 AO

and § 257 HGB.

The legal basis for the processing of personal data is Art. 6(1)(f) GDPR (legitimate interest). Our legitimate interest lies in managing our accounting processes efficiently, reliably and in a structured manner. You can object to the processing of your data on the basis of our legitimate interest at any time under the conditions of Art. 21 GDPR. To do so, please use the contact details provided in the imprint.

Billit

To create and send invoices, in particular electronic invoices (e-invoices), we use the Billit platform provided by Billit NV, Oktrooiplein 1/302, 9000 Ghent, Belgium, as a data processor in accordance with Art. 28 GDPR.

Billit receives the data of your payments from our payment service provider Stripe, creates the corresponding invoices and credit notes from it and sends them to you. Where you are a business customer, the invoice may be sent as an e-invoice in a structured format, either by email or via the Peppol network to the access point of your e-invoicing provider.

In particular, the following categories of personal data may be processed: master data (e.g. name, company name, billing address, email address and VAT identification number), invoice and payment data (e.g. invoice number, invoiced items, amounts, taxes and payment status), as well as technical logs where required for the operation and security of the service.

Billit processes the data within the European Economic Area and uses approved subprocessors for additional functions; an up-to-date list is available at https://www.billit.eu/en-int/subprocessors/. Where personal data is transferred to recipients outside the EU/EEA, this only happens with appropriate safeguards in accordance with Art. 44 et seq. GDPR. To the extent Billit processes data for its own purposes, for example to prevent fraud or to secure and improve its platform, it does so as a controller in accordance with its own privacy policy: https://www.billit.eu/en-int/legal-info/privacy-policy-website/

Invoices and the data contained in them are stored in accordance with applicable statutory retention obligations, in particular those arising from § 147 AO and § 257 HGB.

The legal basis for the processing is Art. 6(1)(c) GDPR (legal obligation), as we are required by tax law to issue invoices (§ 14 UStG), and Art. 6(1)(b) GDPR (performance of a contract).

Effective: November 9, 2026

Source: Süddeutsche Datenschutzgesellschaft mbH