Privacy Policy for the content and functions

Non-binding English translation. This is a convenience translation of the German original „Datenschutzerklärung" (privacy policy). The legally binding version is the German original; in the event of any discrepancy, the German version shall prevail.

of https://app.laizynote.eu/
(hereinafter the "Services")

As of: May 2026

Introduction

Privacy policies are often hard to read. We understand that. And we want to do it differently. With our privacy policy, we want to give users an easily understandable explanation of the manner in which we process personal data. To this end, we structure our privacy policy clearly for users and show users, for each topic area, whether and how we process the personal data of users.

In this privacy policy, we explain to users whether and how we process personal data. In doing so, we set out for users all processing operations carried out by us, by third-party services engaged or integrated by us, or by other third parties on our behalf, within the scope of using our app, our social media profiles and the functions respectively available in this context, as well as within the scope of performing our contractual relationship (hereinafter collectively also the "Services").

Table of contents

Our privacy policy is structured as follows

1. General

The protection of personal data and privacy is extremely important to us. We therefore wish to offer users comprehensive transparency regarding the processing of personal data (GDPR) and regarding the storage of information on the user's end device (TDDDG). For only if the processing of personal data and information is comprehensible to users as data subjects are they sufficiently informed about the extent, the purposes and the benefit of the processing.

This privacy policy applies to all processing of personal data carried out by us, as well as to the storage of information on end devices. "User" therefore applies both within the scope of providing services in our Services and within external online presences, such as our social media profiles.

The controller within the meaning of the General Data Protection Regulation (GDPR), the Federal Data Protection Act (BDSG) and other data protection provisions is
Joshua Maurer
c/o CS Business Center GmbH
Mittelweg 144
20148 Hamburg
E-mail: support@laizynote.eu
Tel.: +49 40 59361117
Hereinafter referred to as the "controller" or "we".

2. General information on data processing

First of all, we would like to give users some introductory information on what the protection of personal data means, what personal data is, how we process it and what security measures we apply in this respect.

LaizyNote is a business productivity suite for freelancers, self-employed persons and small teams. The web app combines notes, tasks, time tracking, contact management (CRM), projects, calendar, documents and an AI assistant ("Daisy") in a unified platform – including the possibility of inviting one's own customers as guests into dedicated workspaces and working together there. The Service is aimed exclusively at entrepreneurs within the meaning of § 14 BGB and is provided as SaaS via https://app.laizynote.eu.

At this point, we point out that each user is independently responsible for ensuring, with regard to the processing of personal data of itself, its employees, the further users, customers, guests, members, etc. created by it, that compliance with data protection provisions is maintained.

2.1 Processing of personal data

Personal data (hereinafter also "data") means individual details about the personal or factual circumstances of an identified or identifiable natural person.

Individual details about personal or factual circumstances are, for example (i.e. not exhaustively), the following data, whereby it is clarified that not all of this data must also be processed by our Services:

- **personnel data – name, age, marital status, date of birth**
- **communication data – address, telephone number, e-mail address**
- **account data – account number, credit card number**
- **geodata – IP address & location data**
- **health data – state of health, illnesses**

The “processing” of personal data includes, for example, the following measures:

- collection – the collection of data via contact forms, by e-mail or through processes and services used by us
- transmission – the transmission of data to our service providers, integrated services or other third parties
- storage – the storage of data in our databases or on our servers
- alteration – the alteration of data due to changes of name, place of residence or of details in our Services
- erasure – the erasure of data when we no longer have authorisation to process it

2.2 Legal bases for the processing of personal data

We process personal data only within the legally permissible limits. The law already obliges us to do so. In particular the GDPR. We are obliged thereunder to always be able to base data processing operations on a legal basis. These legal bases are laid down in Art. 6(1) GDPR. In the following, we name all legal bases on which we base the processing of personal data.

- Consent – Art. 6(1)(a) GDPR: Data is processed where users have actively consented to this processing, e.g. by an “opt-in”, after we have provided sufficient prior information about its extent and purposes. Should users withdraw their consent or not have granted it, we do not (no longer) process the data of our users for purposes for which we require consent.
- For performance of a contract – Art. 6(1)(b): Data is processed where it is necessary for the performance of a contract between us or for carrying out pre-contractual measures. Once the processing is no longer necessary for the performance of the contract, we no longer process the personal data of users.
- Compliance with a legal obligation – Art. 6(1)(c) GDPR: Data is processed where this processing is necessary for compliance with a legal obligation to which we are subject as controller.
- Legitimate interest – Art. 6(1)(f) GDPR: Data is processed where this is necessary to safeguard a legitimate interest on our side and the interests or fundamental rights and freedoms of users concerning the protection of data do not override it.

Personal data is processed by us only for clearly specified purposes (Art. 5(1)(b) GDPR). As soon as the purpose of the processing ceases to apply, the personal data of users is erased or protected by technical and organisational measures (e.g. by pseudonymisation).

The same applies upon the expiry of a prescribed storage period, subject to cases in which further storage is necessary for the conclusion or performance of a contract. In addition, a statutory obligation to store data for longer or to pass it on to third parties (in particular to law enforcement authorities) may arise. In other cases, the storage period and the type of data collected, as well as the type of data processing, depend on which functions the user uses in the individual case. We are happy to provide users with information on this in the individual case, pursuant to Art. 15 GDPR.

2.3 The following data categories are processed by us

Data categories include, in particular, the following data:

- master data (e.g. names, addresses, dates of birth),
- contact data (e.g. e-mail addresses, telephone numbers, messenger services),
- content data (e.g. text inputs, photographs, videos, contents of documents/files),
- contract data (e.g. subject matter of contract, terms, customer category),
- payment data (e.g. bank details, payment history, use of other payment service providers),
- usage data (e.g. history in our Services, use of certain content, access times),
- connection data (e.g. device information, IP addresses, URL referrer).

2.4 The following security measures are taken by us

In accordance with the statutory requirements and taking into account the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihoods of occurrence and the severity of the threat to rights and freedoms, we take appropriate technical and organisational measures to ensure a level of protection appropriate to the risk.

The measures include, in particular, ensuring that the data of our users is stored and processed confidentially, with integrity and available at all times. Furthermore, controls of access to data, as well as of access, input, disclosure, securing of availability and its separation from data of other natural persons, are among the security measures we implement. In addition, we have established procedures that ensure the exercise of data subject rights (see Section 3), the erasure of data and reactions in the event of a threat to the data of our users. Furthermore, we take the protection of personal data into account already during the development of our software, as well as through procedures that correspond to the principle of data protection by design and by privacy-friendly default settings.

2.5 How we transmit or disclose personal data to third parties

Within the scope of our processing of personal data, it occurs that this data is transmitted or disclosed to other bodies, companies, legally independent organisational units or persons. These third parties may include, for example, payment institutions in the context of payment transactions, service providers entrusted with IT tasks, or providers of services and content that we have integrated into our Services. Should we transmit or disclose the personal data of users to third parties, we observe the statutory requirements and, in particular, conclude corresponding contracts or agreements that serve the protection of data with the recipients of data.

2.6 How a third-country transfer takes place

Should it be set out in this privacy policy that we transmit the personal data of users to a third country, i.e. a country outside the EU or outside the EEA, the following applies. A third-country transfer takes place only in compliance with the statutory requirements. We assure users that we have a contractual or statutory authorisation to transmit and process data in the relevant third country. In addition, we have the data of our users processed only by service providers in third countries that, in our view, have a recognised level of data protection. This means that, for example, a corresponding adequacy decision exists between the EU and the country to which we transmit the personal data of users. An "adequacy decision" is a decision adopted by the European Commission pursuant to Art. 45 GDPR, by which it is established that a third country (i.e. a country not bound by the GDPR) or an international organisation offers an adequate level of protection for personal data. Alternatively, e.g. where there is no adequacy decision, a third-country transfer takes place only where, for example, contractual obligations exist between us and the service provider in the third country by means of so-called standard contractual clauses of the EU Commission, and further technical security precautions have been taken that ensure a level of protection appropriately equivalent to that in the EU, or the service provider in the third country can demonstrate data protection certifications and the data of our users is processed only in accordance with internal data protection rules (Art. 44 to 49 GDPR. Information page of the EU Commission: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_de).

Within the framework of the so-called "Data Privacy Framework" ("DPF"), the EU Commission has recognised the level of data protection for certain companies from the USA as secure within the framework of the adequacy decision of 10 July 2023. A list of the certified companies and further information on the DPF can be found by users on the website of the US Department of Commerce at https://www.dataprivacyframework.gov/ (in English). Within this privacy policy, we inform users which of the services used by us are certified under the Data Privacy Framework.

Please note: Certification under the EU-US Data Privacy Framework (DPF) is company-specific and may change at any time. We regularly review whether the US service providers used by us are certified under the DPF at the time of the respective data processing. The respectively current list of certified companies is available at: https://www.dataprivacyframework.gov/list.

Insofar as a service provider used by us is not (or no longer) certified under the DPF, a transmission of personal data takes place exclusively on the basis of the standard contractual clauses of the EU Commission as well as supplementary technical and organisational measures.

2.7 Erasure of data

The data processed by us is erased in accordance with the statutory requirements as soon as the consents permitting its processing are withdrawn or other permissions cease to apply (e.g. where the purpose of processing this data has ceased to apply or it is not necessary for the purpose). Insofar as the data is not erased because it is necessary for other and legally permissible purposes, its processing is restricted to these purposes. That is, the data is blocked and not processed for other purposes. This applies, for example, to data that must be retained for commercial or tax law reasons, or whose storage is necessary for the assertion, exercise or defence of legal claims or for the protection of the rights of another natural or legal person.
Within this privacy policy, we provide information, where applicable, on the erasure and retention of data that applies specifically to the respective processing operations.

2.8 Storage of and access to data on the user's end device

Insofar as we do not obtain consent from users, the storage of or access to information on the user's end device takes place pursuant to § 25(2) no. 2 of the Act on Data Protection and the Protection of Privacy in Telecommunications and Digital Services (TDDDG), since the storage of and access to this information is strictly necessary in order to provide the desired functions of our Services. Insofar as we obtain consent for this, the legal basis is § 25(1) TDDDG. Our Services use cookies, tokens or other technologies that may be stored on end devices and without which the provision of our Services would not be possible.
Cookies, tokens or other technologies are, as a rule, text files that are stored on the user's end device and can be read out by us and third parties when our Services are accessed. Many of the aforementioned technologies contain their own ID. Such an ID is a unique identifier of the respectively used technology. It consists of a sequence of characters by which websites and servers can assign the specific internet browser or the specific service or end device used in which cookies, tokens or other technologies were stored. This enables the operators of websites and analytics services to identify users as users and to distinguish them from others.

2.9 Processing on behalf of a controller

Should we make use of external service providers for the processing of data, these are carefully selected and engaged by us. Should the services provided by these service providers constitute processing on behalf of a controller within the meaning of Art. 28 GDPR, the service providers are bound by our instructions and are regularly monitored. Our data processing agreements correspond to the strict requirements of Art. 28 GDPR and the requirements of the German data protection authorities.

3. Rights of data subjects

If the personal data of our users is processed, they are data subjects within the meaning of the GDPR and users have the following rights vis-à-vis the controller:

3.1 Right of access

Users can request confirmation from the controller as to whether personal data concerning users is processed by us.

If such processing exists, users can request information from the controller on the following:

- the purposes for which the personal data is processed;
- the categories of personal data that are processed;

- the recipients or categories of recipients to whom the personal data concerning users has been or will be disclosed;
- the envisaged period for which the personal data concerning users will be stored or, if specific information on this is not possible, criteria for determining the storage period;
- the existence of a right to rectification or erasure of the personal data concerning users, a right to restriction of processing by the controller or a right to object to this processing;
- the existence of a right to lodge a complaint with a supervisory authority;
- all available information on the origin of the data, where the personal data is not collected from the data subject;
- the existence of automated decision-making, including profiling, pursuant to Art. 22(1) and (4) GDPR and – at least in these cases – meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Users have the right to request information as to whether the personal data concerning users is transmitted to a third country or to an international organisation. In this context, users can request to be informed of the appropriate safeguards pursuant to Art. 46 GDPR in connection with the transmission.

3.2 Right to rectification

Users have a right to rectification and/or completion vis-à-vis the controller, insofar as the processed personal data concerning users is inaccurate or incomplete. The controller must carry out the rectification without undue delay.

3.3 Right to restriction of processing

Under the following conditions, users can request the restriction of the processing of the personal data concerning users:

- where users contest the accuracy of the personal data concerning users, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and users refuse the erasure of the personal data and instead request the restriction of the use of the personal data;
- the controller no longer needs the personal data for the purposes of the processing, but users need it for the assertion, exercise or defence of legal claims, or
- where users have objected to the processing pursuant to Art. 21(1) GDPR and it is not yet established whether the legitimate grounds of the controller override the grounds of users.
- Where the processing of the personal data concerning users has been restricted, this data may – apart from its storage – only be processed with consent or for the assertion, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of an important public interest of the Union or a member state.

Where the restriction of processing has been restricted in accordance with the above conditions, users are informed by the controller before the restriction is lifted.

3.4 Right to erasure

3.4.1. Users can request that the controller erase the personal data concerning users without undue delay, and the controller is obliged to erase this data without undue delay, where one of the following grounds applies:

- The personal data concerning users is no longer necessary for the purposes for which it was collected or otherwise processed.
- Users withdraw the consent on which the processing was based pursuant to Art. 6(1)(a) or Art. 9(2)(a) GDPR, and there is no other legal basis for the processing.

- Users object to the processing pursuant to Art. 21(1) GDPR and there are no overriding legitimate grounds for the processing, or users object to the processing pursuant to Art. 21(2) GDPR.
- The personal data concerning users has been unlawfully processed.
- The erasure of the personal data concerning users is necessary for compliance with a legal obligation under Union or member-state law to which the controller is subject.
- The personal data concerning users has been collected in relation to the offer of information society services pursuant to Art. 8(1) GDPR.

3.4.2. Where the controller has made the personal data concerning users public and is obliged to erase it pursuant to Art. 17(1) GDPR, it shall, taking account of available technology and the cost of implementation, take reasonable steps, including of a technical nature, to inform controllers which are processing the personal data that users as data subjects have requested the erasure by them of any links to, or copies or replications of, this personal data.

3.4.3. The right to erasure does not exist insofar as the processing is necessary

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or member-state law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health pursuant to Art. 9(2)(h) and (i) and Art. 9(3) GDPR;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes pursuant to Art. 89(1) GDPR, insofar as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing, or
- for the assertion, exercise or defence of legal claims.

3.5 Right to notification

Where users have asserted the right to rectification, erasure or restriction of processing vis-à-vis the controller, the controller is obliged to communicate this rectification or erasure of the data or restriction of processing to all recipients to whom the personal data concerning users has been disclosed, unless this proves impossible or involves a disproportionate effort.

Users have the right vis-à-vis the controller to be informed about these recipients.

3.6 Right to data portability

Users have the right to receive the personal data concerning users that users have provided to the controller in a structured, commonly used and machine-readable format. Furthermore, users have the right to transmit this data to another controller without hindrance from the controller to which the personal data was provided, provided that the processing is based on consent pursuant to Art. 6(1)(a) GDPR or Art. 9(2)(a) GDPR or on a contract pursuant to Art. 6(1)(b) GDPR and the processing is carried out by automated means.
In exercising this right, users also have the right to have the personal data concerning users transmitted directly from one controller to another controller, insofar as this is technically feasible. The freedoms and rights of other persons must not be adversely affected thereby.

The right to data portability does not apply to processing of personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

3.7 Right to object

Users have the right, on grounds relating to their particular situation, to object at any time to the processing of personal data concerning users which is carried out on the basis of Art. 6(1)(e) or (f) GDPR; this also applies to profiling based on these provisions.

The controller no longer processes the personal data concerning users, unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of our users, or the processing serves the assertion, exercise or defence of legal claims.

Where the personal data concerning users is processed for direct marketing purposes, users have the right to object at any time to the processing of the personal data concerning users for the purposes of such marketing; this also applies to profiling insofar as it is related to such direct marketing.

If users object to the processing for direct marketing purposes, the personal data concerning users is no longer processed for these purposes.

In connection with the use of information society services, and notwithstanding Directive 2002/58/EC, users have the possibility to exercise the right to object by automated means using technical specifications.

3.8 Right to withdraw the data protection declaration of consent

Users have the right to withdraw a data protection declaration of consent at any time. The withdrawal of consent does not affect the lawfulness of the processing carried out on the basis of the consent up to the withdrawal. The processing is lawful up to a withdrawal – the withdrawal therefore only takes effect on the processing after receipt of the withdrawal. Users can declare the withdrawal informally by post or e-mail. The processing of personal data then no longer takes place, subject to permission by another legal basis. If this is not the case, the data of our users must be erased without undue delay after the withdrawal pursuant to Art. 17(2) GDPR. The right to withdraw consent, subject to the aforementioned conditions, is ensured.

The withdrawal is to be addressed to:

Joshua Maurer
c/o CS Business Center GmbH
Mittelweg 144
20148 Hamburg
E-mail: support@laizynote.eu
Tel.: +49 40 59361117

3.9 Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, users have the right to lodge a complaint with a supervisory authority, in particular in the member state of their residence, place of work or the place of the alleged infringement, if users consider that the processing of the personal data concerning users infringes the GDPR.

The supervisory authority with which the complaint was lodged informs the complainant of the status and outcome of the complaint, including the possibility of a judicial remedy pursuant to Art. 78 GDPR.

3.10 Automated decisions in individual cases, including profiling

Automated decision-making in individual cases within the meaning of Art. 22 GDPR does not take place. However, in individual areas we use automated procedures to structure or optimise content, communication or processes (e.g. statistical analyses, AI-supported answer suggestions). These procedures produce no legal effect vis-à-vis users and do not similarly significantly affect them.

3.11 Notification obligations of the controller

Should the personal data of users have been disclosed to other recipients (third parties) with a legal basis, we communicate to them every rectification, erasure or restriction of the processing of personal data (Art. 16, Art. 17(1) and Art. 18 GDPR). The notification obligation ceases to apply where it involves a disproportionate effort or is impossible. We further inform users, on request, about the recipients.

4. Information on the cookies and other technologies used

We use cookies or other technologies to provide our Services, to evaluate them and to conduct marketing with the evaluated data. Cookies are, for example, small text files that contain data from visited websites or domains and are stored on a device (computer, tablet or smartphone). When users access a website, the cookie stored on a device sends information to whoever placed the cookie.

4.1 How we use cookies and other technologies

We want users to be able to make an informed decision for or against the use of cookies and other technologies that are not strictly necessary for the technical characteristics of the Services. Therefore, in the event that we use cookies and other technologies requiring consent, we enable users to choose, within corresponding settings, which cookies and other technologies users allow. Here, it always applies that functional cookies and other technologies are mandatory for visiting our Services and are therefore already allowed via our default settings. Statistics and marketing cookies and other technologies are optional. Users can allow them by correspondingly consenting to the setting of these cookies and other technologies in the consent banner. Alternatively, users can reject statistics and marketing cookies and other technologies.

4.2 Storage period of cookies and other technologies

The specific storage period of cookies and comparable technologies depends on the respectively used service and is transparently presented in the consent banner or in the cookie overview available there. Insofar as no specific information is provided, cookies are erased or lose their validity after 24 months at the latest. Where cookies and other technologies were set on the basis of consent, users have the possibility at any time to withdraw a consent given or to object to the processing of data by cookies / technologies (collectively referred to as “opt-out”).

5. Data processing in connection with the use of our Services

The use of our Services with all their functions involves the processing of personal data. We explain to users here exactly how this happens.

5.1 Informational use of our Services

The purely informational accessing of our Services requires the processing of the following personal data and information: device type and device version, operating system used, IP address of the end device with which users access our Services, and the time of accessing our Services. All this information is automatically transmitted by a device, unless users have configured it in such a way that the transmission of the information is suppressed.
This personal data is processed for the purpose of the functionality and optimisation of our Services, as well as to ensure the security of our information technology systems. These purposes are at the same time legitimate interests under Art. 6(1)(f) GDPR; the processing therefore takes place with a legal basis.

5.2 Use through or after registration

5.2.1 Registration

Beyond the purely informational use of our Services, users have the possibility to register for our Services and to use our entire offering. In doing so, we process in particular master data and contact data such as the name, the e-mail address and the password. In addition, we automatically process connection data such as date, device information and IP address.

Some processing steps may also take place at third-party providers. The data processing of the third-party providers takes place on the terms of the respectively applicable privacy policies. In the case of data processing with third-party providers, this may constitute processing on behalf of a controller within the meaning of Art. 28 GDPR. This is subject to strict statutory requirements, which we comply with in the course of our contractual agreements with our processors.

The use during or after completed registration and login, and the associated data processing operations, may differ from purely informational use. The collection of this data associated with a profile takes place for the purpose of verifying the status and the associated fulfilment of our contractual obligations towards users. These are legitimate purposes under Art. 6(1)(b) GDPR. Should consent be necessary for the processing operation, we will obtain it at the relevant point (e.g. via the opt-in possibility within a consent banner upon first use of our Service). For any further questions, we are happy to assist users within the scope of the right of access under Art. 15(1) GDPR.

5.2.2 Setting up and using a user account

Users can create a user account in our Services in order to make use of our Services and their functions. When users do this, the personal data provided by them there is transmitted to us by the end device and stored in our information technology systems. The IP address and the time of a registration are also stored. When users log in to their user account, our Service stores tokens on the end device to enable them to stay logged in – even if they have to reload our Services in the meantime. By creating the user account, users can use the functions of our Services.

The processing operations associated with creating a user account serve the purpose of being able to assign future usage operations and of being able to access the entire offering of our Services. When ordering any products or booking services, the processing of data further serves the performance of the contract and is thus purpose-bound and necessary pursuant to Art. 6(1)(b) GDPR.

The storage of the IP address and time of registration is necessary to ensure the security of our information technology systems. This is at the same time our legitimate interest, which is why the processing is also lawful pursuant to Art. 6(1)(f) GDPR.

The personal data entered by users is stored until the time of erasure of this data within the user account or, at the latest, until the complete erasure of the user account with us. Contrary to this, we process certain personal data of users only insofar as we have a statutory or contractual authorisation for this. This is the case, for example, where we may retain contract or payment data even after erasure of the user account for billing or other reasons necessary for the proper handling of our contractual relationship.

5.2.3 Further details on the user account

After registration and login for our Services, users have the possibility to voluntarily provide further information about themselves and their personal data. This information concerns further master data such as, in particular, the upload of a profile picture, the provision of the date of birth or year of birth, the provision of the place of residence, the provision of personal interests or the assignment of a username deviating from a natural name. We process this data within the scope of completing the user account and, where applicable, for our workspace functions. The use of the named functions is an essential part of our Services; the processing of data therefore serves the performance of the contract and is thus purpose-bound and necessary pursuant to Art. 6(1)(b) GDPR.

5.2.4 Sign-on, single sign-on and social login

In order to be able to use some or all of our Services, users must, where this is necessary for use, first log in. We then create a user profile to which the specific information that users have provided can be assigned. Various possibilities are open to users for logging in. Users can log in with an e-mail address, use the single sign-on or social login procedure or, where offered by us, first use a guest access.

Google Firebase Authentication

To handle the login process, we use Google Firebase Authentication. The recipient of the data is Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland. This data processing is necessary for the initiation of the contract and for the performance of the contract according to the login procedure chosen by users. The legal basis for the data processing is therefore Art. 6(1)(b) GDPR.

Login with the e-mail address and guest access

When users log in with an e-mail address or use our Services via a guest access, an individual ID is first generated for the device and stored together with an IP address and, in the case of an e-mail login, with an e-mail address and a password.

Login with single sign-on or social login

When users use the single sign-on or social login procedure, users can conveniently log in with us using a Google, Facebook or Apple account. In this procedure, an individual ID is first generated for the device and stored together with an IP address. In the next step, the login name and the password are transmitted to the third-party provider chosen by users. As a result, the third-party provider learns that users use our Services and can assign this information to a user profile there. After verification, we receive, together with a login name, a token confirming that users have an account with the relevant third-party provider with the named access data. In addition, the third-party providers transmit further basic information about a user profile there. We have no influence on whether and which information is transmitted to us. Users can obtain more detailed information from the respective third-party providers:

Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland:
https://policies.google.com/privacy?hl=de.
Apple Distribution International Ltd., Hollyhill Industrial Estate, Hollyhill, Cork, Ireland:
https://www.apple.com/de/privacy/.
Meta Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland:
https://www.facebook.com/privacy/policy/.

5.3 Functions of our Services

Depending on a registration, users have available, among other things, the functions listed at https://laizynote.eu/de/legal/leistungsumfang/ in our Services. We provide users with all the functions listed there so that they can make full use of our Services, depending on the booked model, and so that we can achieve the best result for them in the collaboration. We pass on the data entered by users only to authorised third parties and process it to fulfil the contractual relationships entered into with users, in particular to fulfil the usage contract that users have concluded on the use of our Services. The legal basis for processing data therefore results from Art. 6(1)(b) GDPR.

5.4 Workspace function

With our workspace function, we give users the possibility to compose their own content such as documents, appointments and information, or to record time, as well as to view and comment on the compositions of other users and to make contact with other users via this. The data categories processed here are master data, where applicable contact data, and where applicable content data. This data can be shared with the users located in a workspace, depending on the configured permissions concept, and processed further by them. Furthermore, the personal data provided by users is transmitted to us by the end device and stored in our information technology systems. The IP address and time of registration are also stored.

The processing operations associated with the workspace function serve the purpose of being able to exchange information with others about our Services and their possible uses and enable users to access the entire offering of our Services. The use of the workspace function is an essential part of our services; the processing of data therefore serves the performance of the contract and is thus purpose-bound and necessary pursuant to Art. 6(1)(b) GDPR.

The storage of the IP address and time of use of our workspace function is necessary to ensure the security of our information technology systems. This is at the same time our legitimate interest, which is why the processing is also lawful pursuant to Art. 6(1)(f) GDPR.
The personal data entered by users is stored until the time of erasure of the profile with us, and beyond that only for as long as the processing is necessary for any performance of the contract and insofar as it is technically possible. A passing on of data to other third parties is not intended.

5.5 Artificial intelligence "Daisy"

In our Services, we use the AI assistant "Daisy", i.e. artificial intelligence services ("AI services"). With the AI services, we can provide users, within the scope of data processing for the provision of our Services, with an intelligent system that processes all interactions in our Services into which the AI services are integrated in the most efficient and, for users, most useful manner. Exactly which Services these are into which we have integrated AI services becomes clear to users from the use of the Services themselves or from the corresponding marking by us. Some Services that work with the support of AI services are:

- summarising, phrasing or structuring notes and documents
- extracting and suggesting tasks from texts
- searching content from workspaces
- processing and answering text inputs
- translation, phrasing assistance and creative suggestions

The data categories processed here are master data, contact data, content data, where applicable usage data, connection data and where applicable contract data. The recipients of the data are the providers of AI services integrated by us and named below. The AI services used by us process personal data exclusively to provide the functions requested by users. Our legal basis for using AI services results from Art. 6(1)(a) GDPR (consent). Should users not have granted us consent to use AI services (no opt-in or withdrawal of consent), we do not (no longer) use AI services within the scope of providing our Services to users. The AI services selected by us have their seat in the EU. The AI services selected by us may not process input data also for AI training purposes. Such processing is technically prevented or has been objected to by a corresponding setting. A data processing agreement pursuant to Art. 28 GDPR for the protection of personal data has been concluded with the AI services selected by us.

Provider of the AI services used by us

Mistral
Mistral AI (SAS)
15 rue des Halles
75001 Paris
France
https://legal.mistral.ai/terms/privacy-policy

5.6 Integrations with external services

We offer users the option of linking external services with LaizyNote in order to exchange data between the services.

lexware office integration (Plus plan only)

Users can connect LaizyNote with their lexware office account to create draft invoices based on data recorded in LaizyNote. For this purpose, contact data, task titles, task descriptions and revenue per task are transmitted to lexware office. The connection is established via an API

key provided by the user. The API key is stored in encrypted form and is no longer visible after saving.
The data categories processed are master data, contact data and content data. The legal basis is Art. 6(1)(a) GDPR (consent). Consent can be withdrawn at any time by removing the connection in the settings.
The recipient of the data is Haufe Service Center GmbH, Munzinger Straße 9, 79111 Freiburg, Germany.
https://datenschutz.lexware.de/lexware-office/

iCal calendar import (all plans)
Users can import external calendars into LaizyNote via an iCal URL. The imported events are automatically updated at regular intervals. The stored URL is encrypted and is no longer visible after saving.
The data categories processed are content data (calendar entries) and connection data (URL of the external calendar). The legal basis is Art. 6(1)(a) GDPR (consent). Consent can be withdrawn at any time by removing the connection in the settings.
The recipient of the data is the respective provider of the external calendar service whose iCal URL the user has stored.

6. Communication services

6.1 Contact form / contact by e-mail

We process the personal data of users that users provide to us in the context of making contact, for the purpose of answering an enquiry, an e-mail or a callback request. The data categories processed here are master data, contact data, content data, where applicable usage data, connection data and where applicable contract data. In individual cases, we pass on this data to companies affiliated with us, or to third parties who, as agreed, may process this data to handle orders and bookings. The legal basis for the processing depends on the purpose of making contact. By an enquiry in the contact form or by making contact by e-mail, users declare that they wish to receive answers or information on certain topics. For this purpose, users also leave their data. We answer an enquiry as desired and process the data of our users for this. The authorisation to process data therefore is based on Art. 6(1)(b) GDPR, since we process it to answer an enquiry and thus to fulfil the contract thereon.

6.2 Feedback form

We process the personal data of users that users provide to us in the context of giving feedback, for the implementation of the feedback, such as to improve our Services. The data categories processed here are master data, contact data, content data, where applicable usage data, connection data and where applicable contract data. In individual cases, we pass on this data to companies affiliated with us, or to third parties whom we use to improve our Services. The legal basis for the processing depends on the purpose of giving feedback. By giving feedback, users declare that they wish, for example, for an improvement of functions of our Services. We take up this information and process the data of our users for this. The authorisation to process data therefore is based on Art. 6(1)(b) GDPR for the fulfilment of the contract.

6.3 Support request

We process the personal data of users that users provide to us in the context of submitting support requests, for the implementation of the support request, such as to remedy disruptions or errors. The data categories processed here are master data, contact data, content data, where applicable usage data, connection data and where applicable contract data. In individual cases, we pass on this data to companies affiliated with us, or to third parties whom we use to remedy disruptions or errors in our Services. The legal basis for the processing depends on the purpose of the support request. By the support request, users declare that they wish, for example, for a remedy of disruptions or errors. We take up this information and process the data of our users for this. The authorisation to process data therefore is based on Art. 6(1)(b) GDPR for the fulfilment of the contract.

6.4 Reporting of illegal content pursuant to the Digital Services Act

We process data of our users that is provided to us by users in the context of reporting illegal content. The data processed here may fall into all of the data categories named in Section 2.3. We process this data to examine the reported content for its illegality and derive the resulting legal obligations therefrom, such as blocking, erasure, criminal prosecution. The legal basis for processing data transmitted to us in the context of reports of illegal content follows from Art. 6(1)(c) GDPR. On the basis of the provisions of the EU Digital Services Act, we are legally obliged to examine illegal content and to derive corresponding measures therefrom.

6.5 Error logging with Sentry

With the help of Sentry.io, we collect data on every access to the server (server log files). The recipient of the data here is Sentry, 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA. The server log files may include the address and name of the accessed Services and files, the date and time of access, the volumes of data transferred, the message about successful access, the browser type and version, the operating system, the referrer URL (the previously visited page) and, as a rule, IP addresses and the requesting provider. The server log files can be used, on the one hand, for security purposes, e.g. to avoid an overload of the servers (in particular in the case of abusive attacks, so-called DDoS attacks), and, on the other hand, to ensure the utilisation of the servers and their stability. Should Sentry transfer this data to a third country (e.g. the USA), this takes place on the basis of a data processing agreement concluded with Sentry and in accordance with the standard contractual clauses agreed with Sentry and other security measures permitted by the GDPR that ensure the security of the processing of personal data with a level of protection identical to that in the EU, in particular on the basis of the EU-US Data Privacy Framework (DPF). The legal basis for using Sentry results from Art. 6(1)(f) GDPR (legitimate interest). We have an interest in regularly reviewing the security and load of our Services. Since we neither pass on the data processed thereby to third parties nor combine it with other data sources, but process it solely on our systems, the interest in handling personal data with as much integrity as possible is not unduly impaired.

7. Payment processing

To handle payment claims, we offer various payment methods. For this, we integrate the payment service providers described below. We do this for the purpose of the proper and needs-based provision of our services. Data processed in this context is usage data, connection data, master data, payment data, contact data or also contract data, such as account numbers or credit card numbers, passwords, TANs and checksums, as well as the contract-, sum- and recipient-related details. The details are necessary to carry out the transactions. The data entered is processed only by the payment service providers and stored with them. We receive no account- or credit-card-related information, but only information about the confirmation or a negative notification of the payment. Under certain circumstances, the data of our users is transmitted by the payment service providers to credit agencies. This transmission serves the purpose of identity and creditworthiness checks. In this respect, we refer to the GTC and the privacy notices of the payment service providers. The legal basis for using the payment service providers results from Art. 6(1)(b) GDPR. We can only provide the services promised to users with our Services, and thus fulfil our contractual obligations, if we make use of third parties, such as the payment service providers, to handle payment movements. Should a payment service provider transfer data to a third country (e.g. the USA), this takes place only in the individual case, on the basis of a data processing agreement concluded with them and in accordance with the standard contractual clauses agreed with them and other security measures permitted by the GDPR that ensure the security of the processing of personal data with a level of protection identical to that in the EU, in particular on the basis of the EU-US Data Privacy Framework (DPF).

Payment service providers

The payment service providers integrated by us are:

Stripe

If users decide on a payment method of the payment service provider Stripe, the payment processing takes place via the payment service provider Stripe Payments Europe Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland, to which we pass on the information provided in the context of the ordering process together with the information about an order (name, address, account number, bank sort code, possibly credit card number, invoice amount, currency and transaction number) pursuant to Art. 6(1)(b) GDPR. Further information on Stripe's data protection at the URL https://stripe.com/de/privacy#translation. Stripe reserves the right to carry out a creditworthiness check on the basis of mathematical-statistical procedures, in order to safeguard the legitimate interest in establishing the user's ability to pay. Stripe transmits the personal data necessary for a creditworthiness check and received in the context of payment processing, where applicable, to selected credit agencies, which Stripe discloses to users on request. The credit report may contain probability values (so-called score values). Insofar as score values are included in the result of the credit report, these are based on a scientifically recognised mathematical-statistical procedure. Address data, among other things but not exclusively, is included in the calculation of the score values. Stripe uses the result of the creditworthiness check with regard to the statistical probability of payment default for the purpose of deciding on the eligibility to use the chosen payment method.
Users can object to this processing of data at any time by a message to Stripe or the engaged credit agencies. However, Stripe may, where applicable, remain entitled to process the personal data of users insofar as this is necessary for contractual payment processing.

8. Hosting

8.1 Provision of our Services

In order to be able to provide users with our Services, we make use of the services of the hosting providers named below. Our Services are accessed from the servers of these hosting providers. For these purposes, we make use of the infrastructure and platform services, computing capacity, storage space and database services, as well as security services and technical maintenance services, of the hosting providers.
The data processed includes all such data that users enter, or that is collected from users, in the context of use and communication in connection with their visit to our Services (e.g. IP address). Our legal basis for using the hosting providers to provide our Services results from Art. 6(1)(f) GDPR (legitimate interest).

8.2 Receipt and sending of e-mails

The services of the hosters used by us can also include the sending, receipt and storage of e-mails. For these purposes, the addresses of the recipients of e-mails as well as the senders, as well as further information concerning the e-mail dispatch (e.g. the providers involved) and the contents of the respective e-mails, are processed. The aforementioned data is processed, among other things, for the purposes of detecting spam. E-mails are, as a rule, not sent in encrypted form over the internet. As a rule, e-mails are indeed encrypted in transit, but (unless end-to-end encryption takes place) not on the servers from which they are sent and received. We can therefore assume no responsibility for the transmission path of the e-mails between the sender and receipt on our server. Our legal basis for using the hosting providers for the receipt and sending of e-mails results from Art. 6(1)(f) GDPR (legitimate interest).

8.3 Collection of access data and log files

We ourselves (or the hosting providers) collect data on every access to the server (server log files). The server log files may include the address and name of the accessed Services and files, the date and time of access, the volumes of data transferred, the message about successful access, the device type and version, the operating system, the referrer URL (the previously visited page) and, as a rule, IP addresses and the requesting provider.
The server log files can be used, on the one hand, for security purposes, e.g. to avoid an overload of the servers (in particular in the case of abusive attacks, so-called DDoS attacks), and, on the other hand, to ensure the utilisation of the servers and their stability. Our legal basis for using a hosting provider for the collection of access data and log files results from Art. 6(1)(f) GDPR (legitimate interest).

The hosting providers used by us are the following:

"Webgo" for delivery of the web application (frontend), e-mail mailboxes, domain management
Webgo GmbH
Heidenkampsweg 81
20097 Hamburg
Germany

"Google Firebase" for backend (Firestore database, Authentication, Cloud Storage, Cloud Functions, Analytics)
Google Firebase (Google Ireland Ltd.)
Google Ireland Ltd.
Gordon House
Barrow Street
Dublin 4
Ireland

9. Tracking & tools

To ensure a smooth technical process and an optimal user-friendly use of our Services, we use the following services:

For the functioning of our Services, to measure their use and for related marketing purposes, we use various services. These services consist predominantly of such services as the Google Firebase technology provides.

In the following, we show users which services are functionally necessary. The use of the functionally necessary services is covered by the legal basis of Art. 6(1)(b) GDPR (for performance of the contract) or by the legal basis of Art. 6(1)(f) GDPR (on the basis of our legitimate interest).

Functionally necessary services
The following services are necessary for the functioning of our Services.

- Cloud Functions
- Authentication
- App Check
- Cloud Messaging
- In-App Messaging
- Cloud Firestore
- Cloud Storage
- Hosting
- Security Rules
- Remote Config
- Test Lab

Cloud Storage: the recipient of the corresponding data is Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland. Should Google transfer this data to a third country (e.g. the USA), this takes place only in the individual case, on the basis of a data processing agreement concluded with Google and in accordance with the standard contractual clauses agreed with Google and other security measures permitted by the GDPR that ensure the security of the processing of personal data with a level of protection identical to that in the EU, in particular on the basis of the EU-US Data Privacy Framework (DPF).

reCAPTCHA (within Firebase App Check)

Within Firebase App Check, we use Google reCAPTCHA (Enterprise or v3) as an attestation provider. In this context, reCAPTCHA does not serve to secure individual online forms, but verifies in the background that requests to our backend originate from a genuine, unmodified instance of our app (app integrity/attestation). For this, reCAPTCHA processes technical information such as usage and connection data (e.g. IP address, browser and device information) and technical interaction signals in order to detect and ward off automated or abusive access. The recipient of the data is Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland. Should Google transfer this data to a third country (e.g. the USA), this takes place only in the individual case, on the basis of a data processing agreement concluded with Google and in accordance with the standard contractual clauses agreed with Google and other security measures permitted by the GDPR that ensure the security of the processing of personal data with a level of protection identical to that in the EU, in particular on the basis of the EU-US Data Privacy Framework (DPF). Insofar as personal data is processed, this takes place on the basis of our legitimate interest pursuant to Art. 6(1)(f) GDPR in ensuring the security, integrity and functionality of our Services.
More information at: https://policies.google.com/privacy?hl=de GDPR info:
https://business.safety.google/compliance/#!%23gdpr

Cloudflare Turnstile

In our Services, we use the service "Cloudflare Turnstile" to protect our login area from abusive automated use ("bots"). The provider, and thus the recipient of data, is Cloudflare Germany GmbH, Rosenheimer Straße 143C, 81671 Munich, Germany. Cloudflare Turnstile serves to verify whether an input is made by a human or by an automated program. For this, Cloudflare Turnstile processes connection data and usage data, such as in particular various technical information (so-called "signals"), such as IP address, browser information (user agent), and other technical characteristics of the system used. This data is used to detect and block suspicious or automated access. The processing takes place exclusively for the purpose of ensuring the integrity and security of our Services and of defending against attacks on our IT systems. Should Cloudflare transfer this data to a third country (e.g. the USA), this takes place only in the individual case, on the basis of a data processing agreement concluded with Cloudflare and in accordance with the standard contractual clauses agreed with Cloudflare and other security measures permitted by the GDPR that ensure the security of the processing of personal data with a level of protection identical to that in the EU, in particular on the basis of the EU-US Data Privacy Framework (DPF). Insofar as personal data is processed, this takes place on the basis of our legitimate interest pursuant to Art. 6(1)(f) GDPR in ensuring the security and functionality of our Services. Further information on data protection at Cloudflare at: https://www.cloudflare.com/de-de/turnstile-privacy-policy/.

10. Transactional mailings

For administrative operations, to confirm actions and within the scope of our non-promotional customer communication, we send transactional notifications (hereinafter "transactional mailings") to users. Our transactional mailings contain important administrative information on our Services. For the management of our transactional mailings, as well as for the creation and sending of transactional mailings, we use the transactional mail services listed below. In the context of users accessing the transactional mailings, technical information, such as information on the browser and the system, as well as the IP address and the time of access, may be collected. This information is used for the technical tracing of the interaction with our transactional mailings on the basis of the technical data or the target groups and their reading behaviour. The legal basis for using transactional mailings lies in Art. 6(1)(b) GDPR, since with the information in the transactional mailings we fulfil our contractual obligations towards users. Should we, in doing so, make use of the services of third-party providers for this, the legal basis for this lies in Art. 6(1)(f) GDPR. We have a legitimate interest in standardising the sending of transactional mailings and controlling it collectively. In doing so, the interest of users in the most economical processing possible of their data is not unduly impaired. Should providers transfer data to a third country (e.g. the USA), this takes place only in the individual case, on the basis of a data processing agreement concluded with them and in accordance with the standard contractual

clauses agreed with them and other security measures permitted by the GDPR that ensure the security of the processing of personal data with a level of protection identical to that in the EU, in particular on the basis of the EU-US Data Privacy Framework (DPF).

Provider of the transactional mail services used by us

MailerSend for transactional e-mails
MailerSend, Inc.
228 Park Ave S
PMB 54955
New York
New York 10003-1502
USA
https://www.mailersend.com/legal/privacy-policy

11. Newsletter dispatch

With consent (regularly by subscribing), we send newsletters, e-mails and other electronic notifications (hereinafter "newsletter") to users. Our newsletters generally contain technical, commercial and promotional information on our Services. For the management of our newsletter subscribers, as well as for the creation and sending of newsletters, we use the newsletter services listed below. To sign up for our newsletter, it is generally sufficient for users to provide an e-mail address. Sign-up for our newsletter always takes place in a so-called double opt-in procedure. After signing up for our newsletter, users therefore receive an e-mail in which they are asked to confirm the sign-up by activating a confirmation link. This confirmation is necessary to prevent someone else from signing up with an e-mail address for a newsletter. We log the sign-ups to the newsletter for the purpose of being able to demonstrate the sign-up process in accordance with the legal requirements. For this, we store the sign-up and the confirmation time, as well as the IP address. Changes to the data stored with the dispatch service provider are also logged. Users can unsubscribe from our newsletter at any time. For this, users simply click on the "unsubscribe" button contained in the footer of every newsletter. Should users unsubscribe from our newsletter, an e-mail address may be stored for up to three years on the basis of our legitimate interests before we erase it, so that we can demonstrate a consent formerly given. Insofar as we engage a service provider with the sending of e-mails, this takes place on the basis of our legitimate interests in an efficient and secure dispatch system. Our newsletters may contain a so-called "web beacon". A web beacon is a pixel-sized file that is retrieved from our server (or, when a dispatch service provider is used, from its server) when the newsletter is opened. In the context of this retrieval, technical information, such as information on the browser and a system, as well as the IP address and the time of retrieval, is first collected.
This information is used for the technical improvement of our newsletter on the basis of the technical data or the target groups and their reading behaviour on the basis of their retrieval locations (which can be determined with the help of the IP address) or the access times. This analysis also includes the determination of whether the newsletters are opened, when they are opened and which links are clicked. For technical reasons, this information can indeed be assigned to the individual newsletter recipients. However, it is neither our endeavour nor, where used, that of the dispatch service provider, to observe individual users. Rather, the analyses serve us to recognise the reading habits of our users and to adapt our content to them or to send different content according to the interests of our users.
The analysis of the newsletter and the measurement of success take place, subject to an express consent of the users, on the basis of our legitimate interests for the purposes of using a user-friendly and secure newsletter system, which serves both our business interests and corresponds to the expectations of the users.
The legal basis for sending newsletters, and thus also for using web beacons, is a consent, where users have granted us this by subscribing to the newsletter, and therefore results from Art. 6(1)(a) GDPR. Should users not have granted us consent to send newsletters, we do not (no longer) send newsletters to users. This also automatically eliminates the use of web beacons.

Should we, in doing so, make use of the services of third-party providers for this, the legal basis for this lies in Art. 6(1)(f) GDPR. We have a legitimate interest in standardising the sending of newsletters and controlling it collectively. In doing so, the interest of users in the most economical processing possible of their data is not unduly impaired. Should providers transfer data to a third country (e.g. the USA), this takes place only in the individual case, on the basis of a data processing agreement concluded with them and in accordance with the standard contractual clauses agreed with them and other security measures permitted by the GDPR that ensure the security of the processing of personal data with a level of protection identical to that in the EU, in particular on the basis of the EU-US Data Privacy Framework (DPF).

Provider of the newsletter services used by us

MailerLite
MailerLite UAB
Paupio g. 246
LT-11341 Vilnius
Lithuania.
https://www.mailerlite.com/gdpr-compliance

12. Profiles on social media websites

We maintain profiles on the platforms of the social networks of the internet and, in this context, process personal data in order to communicate with the users active there or to offer information about us. We point out to users that the data of our users may be processed outside the area of the European Union when visiting our profiles. Responsible for this are the operators of the respective social networks. A detailed presentation of the respective forms of processing and the possibilities of objection (e.g. opt-out) can be found by users in the privacy policies of the operators of the respective social networks.
When visiting our social media profiles, usage behaviour may be evaluated and information obtained from this may be communicated to us ("insights"). This evaluation takes place for the purposes of the economic optimisation and needs-based design of our Services. The data categories processed here are, where applicable, master data, where applicable contact data, content data, usage data, connection data. The recipient of the data is the provider of the respective social media platform as joint controller pursuant to Art. 26 GDPR. The legal basis for processing the data in accordance with the requirement named here results from our legitimate interest and thus from Art. 6(1)(f) GDPR. The respective social media platform is responsible for the implementation of data subject rights. We provide information on data subject rights below, when naming the respective social media platform on which we maintain a profile. Users can also assert their rights vis-à-vis us; we will then forward their request promptly to the operator of the social media platform.

Instagram
Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland. Data subject rights: https://privacycenter.instagram.com/policy.

TikTok
TikTok Technology Limited, 10 Earlsfort Terrace, Dublin D02 T380, Ireland. Data subject rights: https://www.tiktok.com/legal/privacy-policy?lang=de-DE.

LinkedIn
LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland. Data subject rights: https://de.linkedin.com/legal/privacy-policy.

YouTube
Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland. Data subject rights: https://www.youtube.com/howyoutubeworks/our-commitments/protecting-user-data/#privacy-guidelines.

13. Plugins in our Services

In our Services, we integrate content such as videos, buttons, social media icons, etc. from social networks and other websites via plugins. The integration always works in such a way that the social networks learn and process an IP address via these plugins. The IP address is necessary for the display of the content of the plugins, as it is needed so that the social networks whose plugins we have integrated can send information to the browser. Some social networks use pixel tags (invisible graphics, also referred to as "web beacons") for statistical or marketing purposes. Through the "pixel tags", information such as the visitor traffic in our Services can be evaluated. Further information can also be stored in cookies on a device and contain, among other things, technical information on a browser and an operating system, on the time of visiting our Services, and other details on the use of our Services, and be combined with information from other sources.

Integration of YouTube videos
We use YouTube for the purpose of integrating videos via the video plugin of YouTube for the personal design of our Services. Through the integration of videos via the video plugin of YouTube, Google can analyse usage behaviour in our Services. The data categories processed here are usage data, connection data. The recipient of the data is Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland. Should Google transfer this data to a third country (e.g. the USA), this takes place only in the individual case, on the basis of a data processing agreement concluded with Google and in accordance with the standard contractual clauses agreed with Google and other security measures permitted by the GDPR that ensure the security of the processing of personal data with a level of protection identical to that in the EU, in particular on the basis of the EU-US Data Privacy Framework (DPF). The legal basis for using YouTube is a consent (e.g. via an opt-in in the consent banner), where users have granted us this in the context of the visit to our Services, and therefore results from Art. 6(1)(a) GDPR. On the basis of a consent, cookies or similar (text) files are stored on the user's end device and personal data is read out thereby. Should users not have granted us consent to use YouTube (no opt-in or withdrawal of consent), we do not (no longer) use YouTube in the context of visits to our Services. Further information on data processing at https://policies.google.com/privacy?hl=de.