



Privacy Policy for the Gentlent Platform (hereinafter „Services“)

As of: August 2025

Introduction

Privacy policies are often difficult to read. We understand that. And we want to do things differently. With our privacy policy, we want to give you an easy-to-understand explanation of how we process your personal data. To this end, we have structured our privacy policy clearly for you and show you for each topic whether and how we process your personal data.

Table of Contents

Our privacy policy is built up the following way:

1. General information - brief introduction to the subject matter of the privacy policy, the controller and the data protection officer
2. General information on data processing - information on what personal data is, on what legal basis we process it or share it with third parties
3. Rights of data subjects - information on your rights to, among other things, information, deletion or objection to our data processing
4. Information on the cookies and other technologies used - information on the use of cookies and other technologies with or with the help of which we process your personal data
5. Data processing in connection with the use of our Services - information on our data processing in our Services themselves, on registration and on individual functionalities
6. Communication Services - information on communication Services and the corresponding processing of your personal data
7. Payment - information on the processing of payments through the integration of payment service providers and the resulting processing of your personal data
8. Provision of our Services - information about our hosting service providers and the Services they use
9. Tracking & tools - information about Services we use to provide you with our Services and to analyze the use of our Services
10. Newsletter - Information on the integration of newsletter Services through which we provide you with regular updates about our Services
11. Fan pages on social media - information about our presence on social media networks and the processing of your personal data that takes place as a result

1. General

The protection of your personal data and your privacy is extremely important to us. Therefore, we would like to offer you

Anschrift / Address

Gentlent GmbH
Am Trippelsberg 92
40589 Düsseldorf
Germany

Kontakt / Contact

E-Mail: support@gentlent.com
Tel.: +49 (0) 211 86843 - 0
Fax: +49 (0) 211 86843 - 999
Web: <https://www.gentlent.com>

Rechtliches / Legal Details

Amtsgericht Düsseldorf
HR-Nr.: HRB 103552
USt.-ID: DE366296666
CEO: Tom Klein, Florian Oliver Elke

Bankkonto / Bank Account

bunq B.V. Niederlassung Deutschland
IBAN: DE56 3701 9000 1010 9445 44
BIC: BUNQDE82



comprehensive transparency regarding the processing of your personal data (GDPR) as well as regarding the storage of information on your end device or regarding the access to information (TDDDG). Because only if the processing of personal data and information is comprehensible for you as a data subject, you are sufficiently informed about the scope, purposes and benefits 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 your end devices. It therefore applies both in the context of providing our services in our Services and within external online presences, such as our social media fan pages.

Controller within the meaning of the General Data Protection Regulation (GDPR), the German Federal Data Protection Act (BDSG) and other data protection regulations is the

Gentlent GmbH
Am Trippelsberg 92
40589 Düsseldorf
Germany

support@gentlent.com
Tel: +49 211 86843 - 0
Fax: +49 211 86843 - 999

Also referred to as „Controller“ or “Us”.

2. General information on data processing

First of all, we would like to give you some introductory information about what the protection of your personal data means, what personal data is, how we process it and what security measures we take in this regard.

2.1. Processing personal data

Personal data (hereinafter also referred to as “data”) is individual information about the personal or factual circumstances of an identified or identifiable natural person.

Individual details about personal or factual circumstances are, for example:

- Personal data - name, age, marital status, date of birth
- Communication data - address, telephone number, e-mail address
- Account data - account and credit card number
- Geodata - IP address & location data
- Health data - health condition, illnesses

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

- Collection - The collection of your data via contact forms, by e-mail or through processes and Services used by us
- Transmission - The transmission of your data to our service providers, integrated Services or other third parties
- Storage - The storage of your data in our databases or on our servers

Anschrift / Address
Gentlent GmbH
Am Trippelsberg 92
40589 Düsseldorf
Germany

Kontakt / Contact
E-Mail: support@gentlent.com
Tel.: +49 (0) 211 86843 - 0
Fax: +49 (0) 211 86843 - 999
Web: <https://www.gentlent.com>

Rechtliches / Legal Details
Amtsgericht Düsseldorf
HR-Nr.: HRB 103552
USt.-ID: DE366296666
CEO: Tom Klein, Florian Oliver Elke

Bankkonto / Bank Account
bunq B.V. Niederlassung Deutschland
IBAN: DE56 3701 9000 1010 9445 44
BIC: BUNQDE82



- Deletion - The deletion of your data when we are no longer authorized to process it

2.2. Legal basis for the processing of your personal data

We only process personal data within the legally permissible limits. We are obliged to do so by law. In particular the GDPR. This obliges us to always be able to base data processing operations on a legal basis. These legal bases are standardized in Art. 6 para. 1 GDPR. Here we list the most common legal bases on which we process your personal data.

- Consent - Art. 6 para. 1 lit. a GDPR: Your data will only be processed if you have consented to this processing after we have provided you with sufficient information about its scope and purposes.
- To fulfill a contract - Art. 6 para. 1 lit. b: Your data will only be processed if it is necessary for the fulfillment of a contract between us or for the implementation of pre-contractual measures.
- Legitimate interest - Art. 6 para. 1 lit. f GDPR: Your data will only be processed if this is necessary to safeguard a legitimate interest on our part and your interests or fundamental rights and freedoms regarding the protection of your data do not outweigh this.

We only process personal data for clear purposes (Art. 5 para. 1 lit. b GDPR). As soon as the purpose of processing ceases to apply, your personal data will be deleted or protected by technical and organizational measures (e.g. by pseudonymization).

The same applies to the expiry of a prescribed storage period, subject to cases in which further storage is necessary for the conclusion or fulfillment of a contract. In addition, there may be a legal obligation to store the data for a longer period or to pass it on to third parties (in particular to law enforcement authorities). In other cases, the storage period and type of data collected as well as the type of data processing depends on which functions you use in the individual case. We will be happy to provide you with information on this in individual cases in accordance with Art. 15 GDPR.

2.3. We process these categories

Data categories are 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 entries, 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 referrers).

2.4. These are the security measures we meet

In accordance with legal requirements and taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the different probabilities of occurrence and the extent of the threat to your rights and freedoms, we take appropriate technical and organizational measures to ensure a



level of protection appropriate to the risk.

In particular, the measures include ensuring that your data is stored and processed confidentially, with integrity and available at all times. Furthermore, the security measures we implement include controls on access to your data as well as access, input, disclosure, ensuring availability and their separation from data of other natural persons. Furthermore, we have established procedures to ensure the exercise of data subject rights (see under Section 5), the deletion of data and responses in the event of a risk to your data. Furthermore, we already consider the protection of personal data during the development of our software as well as through procedures that comply with the principle of data protection through technology design and through data protection-friendly default settings.

2.5. This is how we transfer personal data

In the course of our processing activities of your personal data, it may happen that this data is transferred or disclosed to other bodies, companies, legally independent organizational 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 website. If we transfer or disclose your personal data to third parties, we comply with the legal requirements and, in particular, conclude appropriate contracts or agreements that serve to protect your data with the recipients of your data.

2.6. This is how a third country transfer takes place

If this privacy policy indicates that we transfer your personal data to a third country, i.e. a country outside the EU or outside the EEA, the following applies. If we process your data in a third country or if the processing takes place in a third country as part of the use of third-party Services, this will only take place in accordance with the legal requirements. Furthermore, a third country transfer usually only takes place with your express consent. Whether or not such consent is given, we ensure that we have contractual or legal authorization to transfer and process your data in the third country in question. Furthermore, we only allow your data to be processed by Service providers in third countries that, in our view, have a recognized level of data protection. This means that a corresponding adequacy decision exists between the EU and the country in which we transfer your personal data, for example. An "adequacy decision" is a decision adopted by the European Commission under Article 45 of the GDPR that determines that a third country (i.e., a country that is not bound by the GDPR) or an international organization provides an adequate level of protection for personal data. Alternatively, e.g. if there is no adequacy decision, a third country transfer will only take place if, for example, contractual obligations exist between us and the Service provider in the third country through so-called standard contractual clauses of the EU Commission and further technical security precautions have been taken that ensure an adequately equivalent level of protection to that in the EU or the Service provider in the third country can provide data protection certifications and your data is only processed in accordance with internal data protection regulations (Articles 44 to 49 GDPR. Information page of the EU Commission: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en).

As part of the so-called "Data Privacy Framework" ("DPF"), the EU Commission has recognized the level of data protection for certain companies from the USA as secure within the framework of the adequacy decision of 10.07.2023. A list of certified companies and further information on the DPF can be found on the website of the US Department of Commerce at <https://www.dataprivacyframework.gov/>. As part of this privacy policy, we will inform you which Services we use are certified under the Data Privacy Framework.



2.7. Deletion of data

The data processed by us will be deleted in accordance with the legal requirements as soon as the consent given for processing is revoked or other permissions no longer apply (e.g. if the purpose for processing this data no longer applies or it is not required for the purpose). If the data is not deleted because it is required for other and legally permissible purposes, its processing is restricted to these purposes. This means that 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 defense of legal claims or to protect the rights of another natural or legal person.

As part of this privacy policy, we may provide information on the deletion and retention of data that applies specifically to the respective processing procedure.

2.8. Storage of and access to data on your end device

If we do not obtain your consent, the storage of or access to information on your terminal device is carried out in accordance with Section 25 (2) No. 2 of the Act on Data Protection and Privacy in Telecommunications and Digital Services (TDDDG), as the storage of and access to this information is absolutely necessary in order to provide the desired functions of our Services. If we obtain consent for this, the legal basis is Section 25 (1) TDDDG. Our Services use cookies, tokens, beacons or other technologies that may be stored on your end devices and without which the provision of our Services would not be possible.

Cookies, tokens, beacons or other technologies are generally text files that are stored on your device and can be read by us and third parties when you access our Services. Many of the aforementioned technologies contain their own ID. Such an ID is a unique identifier of the respective technology used. It consists of a character string through which websites and servers can be assigned to the specific internet browser or the specific service or end device used in which cookies, tokens, beacons or other technologies have been stored. This enables the operators of websites and analysis Services to identify you as a user and distinguish you from others.

2.9. Processing on behalf

If we use external Service providers to process your data, they will be carefully selected and commissioned by us. If the Services provided by these Service providers are commissioned processing within the meaning of Art. 28 GDPR, the Service providers are bound by our instructions and are regularly monitored. In this context, our order processing contracts comply with the strict requirements of Art. 28 GDPR as well as the specifications of the German data protection authorities.

3. Data subject rights

If your personal data is processed, you are a data subject within the meaning of the GDPR and you are entitled to the following rights as a user against the controller:



3.1. Right to information

You may request confirmation from the controller as to whether personal data concerning you is being processed by us.

If such processing exists, you may request information from the controller about the following:

- The purposes for which the personal data are processed;
- the categories of personal data which are processed;
- the recipients or categories of recipients to whom the personal data concerning you have been or will be disclosed;
- the planned duration of the storage of the personal data concerning you or, if concrete 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 you, a right to restriction of processing by the controller or a right to object to such processing;
- the existence of a right of appeal to a supervisory authority;
- any available information about the origin of the data, if the personal data are not collected from the data subject;
- the existence of automated decision-making, including profiling, pursuant to Article 22 (1) and (4) of the GDPR and, at least in these cases, meaningful information about the logic involved and the scope and intended effects of such processing for the data subject.
- You have the right to request information about whether personal data concerning you is transferred to a third country or to an international organization. In this context, you may request to be informed about the appropriate safeguards pursuant to Art. 46 GDPR in connection with the transfer.

3.2. Right to rectification

You have a right to rectification and/or completion vis-à-vis the controller if the processed personal data concerning you are inaccurate or incomplete. The controller shall carry out the rectification without undue delay.

3.3. Right to restriction of processing

Under the following conditions, you may request the restriction of the processing of personal data concerning you:

- if you contest the accuracy of the personal data concerning you for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and you object to the erasure of the personal data and request instead the restriction of the use of the personal data;
- the controller no longer needs the personal data for the purposes of processing, but you need them for the establishment, exercise or defense of legal claims; or
- if you have objected to the processing pursuant to Article 21 (1) GDPR and it has not yet been determined whether the controller's legitimate grounds override your grounds.
- If the processing of personal data concerning you has been restricted, such data may - apart from being stored - only be processed with your consent or for the assertion, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or a Member State.

If the restriction of processing has been restricted in accordance with the above conditions, you will be informed by the controller before the restriction is lifted.



3.4. Right to erasure

3.4.1. You may request the controller to erase the personal data concerning you without undue delay, and the controller is obliged to erase this data without undue delay, if one of the following reasons applies:

- The personal data concerning you are no longer necessary for the purposes for which they were collected or otherwise processed.
- You withdraw your consent on which the processing was based pursuant to Art. 6 (1) lit. a or Art. 9 (2) lit. a GDPR and there is no other legal basis for the processing.
- You object to the processing pursuant to Art. 21 (1) GDPR and there are no overriding legitimate grounds for the processing, or the You object to the processing pursuant to Art. 21 (2) GDPR.
- The personal data concerning you has been processed unlawfully.
- The erasure of the personal data concerning you is necessary for compliance with a legal obligation under Union or Member State law to which the controller is subject.
- The personal data concerning you has been collected in relation to information society Services offered pursuant to Article 8 (1) GDPR.

3.4.2. If the controller has made the personal data concerning you public and is obliged to erase it pursuant to Article 17(1) of the GDPR, it shall take reasonable measures, including technical measures, having regard to the available technology and the cost of implementation, to inform data controllers that process the personal data that you, as the data subject, have requested that they erase all links to or copies or replications of such personal data.

3.4.3. The right to erasure shall not apply to the extent that the processing is necessary:

- For the exercise of the right to freedom of expression and information;
- for compliance with a legal obligation which requires processing under 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) lit. 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 (1) is likely to render impossible or seriously prejudice the achievement of the purposes of such processing; or
- for the assertion, exercise or defense of legal claims.

3.5. Right to information

If you have asserted the right to rectification, erasure or restriction of processing against the controller, the controller is obliged to inform all recipients to whom the personal data concerning you have been disclosed of this rectification or erasure of the data or restriction of processing, unless this proves impossible or involves a disproportionate effort.

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

3.6. Right to data portability

You have the right to receive the personal data concerning you that you have provided to the controller in a structured, common and machine-readable format. In addition, you have the right to transfer this data to another controller without



hindrance from the controller to whom the personal data was provided, provided that the processing is based on consent pursuant to Art. 6 (1) lit. a GDPR or Art. 9 (2) lit. a GDPR or on a contract pursuant to Art. 6 (1) lit. b GDPR and the processing is carried out with the help of automated procedures.

In exercising this right, you also have the right to obtain that the personal data concerning you be transferred directly from one controller to another controller, insofar as this is technically feasible. Freedoms and rights of other persons must not be affected by this.

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

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

The controller shall no longer process the personal data concerning you unless it can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defense of legal claims.

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

If you object to the processing for direct marketing purposes, the personal data concerning you will no longer be processed for these purposes.

You have the possibility, in connection with the use of information society Services - notwithstanding Directive 2002/58/EC - to exercise your right to object by means of automated procedures using technical specifications.

3.8. Right to revoke your declaration of consent under data protection law

You have the right to revoke your declaration of consent under data protection law at any time. The revocation of consent does not affect the lawfulness of the processing carried out on the basis of the consent until the revocation.

The processing is lawful until your revocation - the revocation thus only affects the processing after receipt of your revocation. You can declare the revocation informally by mail or e-mail. The processing of your personal data will then no longer take place, subject to permission by another legal basis. If this is not the case, your data must be deleted immediately after the revocation in accordance with Art. 17 (2) GDPR. Your right to revoke your consent subject to the above conditions is guaranteed.

Your revocation should be addressed to:

Gentlent GmbH
Am Trippelsberg 92
40589 Düsseldorf
Germany

Anschrift / Address
Gentlent GmbH
Am Trippelsberg 92
40589 Düsseldorf
Germany

Kontakt / Contact
E-Mail: support@gentlent.com
Tel.: +49 (0) 211 86843 - 0
Fax: +49 (0) 211 86843 - 999
Web: <https://www.gentlent.com>

Rechtliches / Legal Details
Amtsgericht Düsseldorf
HR-Nr.: HRB 103552
USt.-ID: DE366296666
CEO: Tom Klein, Florian Oliver Elke

Bankkonto / Bank Account
bunq B.V. Niederlassung Deutschland
IBAN: DE56 3701 9000 1010 9445 44
BIC: BUNQDE82



support@gentlent.com

Tel: +49 211 86843 - 0

Fax: +49 211 86843 - 999

3.9. Right to complain to a supervisory authority

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

The supervisory authority to which the complaint has been lodged will inform the complainant of the status and outcome of the complaint, including the possibility of a judicial remedy under Article 78 GDPR.

3.10. Automated decisions in individual cases including profiling

Automated decisions in individual cases including profiling do not take place.

3.11. Notification obligations of the responsible party

If your personal data have been disclosed to other recipients (third parties) with legal grounds, we will notify them of any rectification, erasure or restriction of the processing of your personal data (Art. 16, Art. 17 (1) and Art. 18 GDPR). The notification obligation does not apply if it involves disproportionate effort or is impossible. We will also inform you about the recipients upon request.

4. Information on the cookies and other technologies used

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

4.1. How we use cookies and other technologies

We want you to be able to make an informed decision for or against the use of cookies and other technologies that are not absolutely necessary for the technical features of the Services. Therefore, we enable you to make a voluntary decision when you first visit our Services and then permanently in appropriate settings to choose which cookies and other technologies you allow. Functional cookies and other technologies are mandatory for visiting our Services and are

Anschrift / Address
Gentlent GmbH
Am Trippelsberg 92
40589 Düsseldorf
Germany

Kontakt / Contact
E-Mail: support@gentlent.com
Tel.: +49 (0) 211 86843 - 0
Fax: +49 (0) 211 86843 - 999
Web: <https://www.gentlent.com>

Rechtliches / Legal Details
Amtsgericht Düsseldorf
HR-Nr.: HRB 103552
USt-ID: DE366296666
CEO: Tom Klein, Florian Oliver Elke

Bankkonto / Bank Account
bunq B.V. Niederlassung Deutschland
IBAN: DE56 3701 9000 1010 9445 44
BIC: BUNQDE82



therefore already permitted via our default settings. Statistics and marketing cookies and other technologies are optional. You can allow them by consenting to the setting of these cookies and other technologies in the consent banner. Alternatively, you can reject statistics and marketing cookies and other technologies. Please note that you may also be shown advertising if you refuse the use of statistics and marketing cookies and other technologies. However, this advertising will then be less focused on your interests. However, you will still be able to use the full functionality of the Services.

4.2. Storage duration of cookies and other technologies

Unless we provide you with explicit information about the storage period of cookies (e.g., within the cookie banner), you can assume that the storage period can be up to two years. If cookies were set on the basis of your consent, you have the option at any time to revoke any consent you have given or to object to the processing of your data by cookie technologies (collectively referred to as "opt-out").

4.3. Types of cookies and other technologies

We distinguish between

- **Functional (necessary) cookies / technologies:** These are required for the basic technical functions of the Services. They enable, for example, a secure login and the storage of the progress of order processes. They also enable us, for example, to save your login data, the contents of your shopping cart and the uniform presentation of page content.
- **Statistics cookies / technologies:** These enable us to analyze the Services so that we can measure and improve their performance. You can change your personal statistics settings by clicking on the corresponding opt-out link.
- **Marketing cookies / technologies:** These are used by us to provide you with advertising that may be relevant to your interests. They enable, for example, the sharing of pages via social networks and the posting of comments. Offers that may match your interests are also displayed. You can change your personal marketing settings by clicking on the corresponding opt-out link.

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

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

5.1. Informational use of our Services

The purely informational use of our Services requires the processing of the following personal data and information: Browser type and browser version, operating system used, address of previously visited websites, address of the terminal device with which you access our Services (IP address), and the time of the call to our Services. All this information is automatically transmitted by your browser if you have not configured it in such a way that transmission of the information is suppressed.



This personal data is processed for the purpose of the functionality and optimization of our Services, as well as to ensure the security of our information technology systems. These purposes are at the same time legitimate interests according to Art. 6 para. 1 lit. f GDPR, the processing is thus carried out with legal grounds.

5.2. Use by Registration

5.2.1. Registration

Beyond purely informational use of our Services, you have the option to register for our Services and access our full range of offerings. In this context, we process, in particular, master and contact data such as your name, email address, and password. Additionally, we automatically process connection data such as the date, device information, and IP address. After registering, you can use our Services in the free version and optionally upgrade to paid premium versions. Our Services allow you to select various features and access the respective included content. This use of our Services may require the processing of personal data and information in the manner described in Section 5.

Some processing steps may also be carried out by third-party providers. The data processing by such third parties is subject to the terms of their respective privacy policies. In cases where processing is carried out by third-party providers, this may constitute commissioned data processing within the meaning of Article 28 GDPR. Such processing is subject to strict legal requirements, which we comply with as part of our contractual agreements with our data processors.

The data processing operations associated with use following registration and login may differ from those involved in purely informational use. The collection of data associated with your profile is carried out for the purpose of verifying your status and fulfilling our contractual obligations to you. These are legitimate purposes pursuant to Article 6(1)(b) GDPR. If a particular processing operation requires your consent, we will obtain it at the appropriate time (e.g., via an opt-in option in a consent banner when you first use our Services). If you have further questions, we are happy to assist you within the scope of your right of access pursuant to Article 15(1) GDPR.

5.2.2 User Account

You can create a user account (hereinafter also referred to as a “profile”) within our Services to make use of our Services and their features. When you do so, the personal data you enter will be transmitted from your device to us and stored in our IT systems. Your IP address and the time of registration will also be stored. When you log into your profile, our service stores tokens on your device to allow you to remain logged in—even if you need to reload our Services in the meantime. By creating a profile, you are able to access and use the features of our Services.

The processing activities associated with creating a profile serve the purpose of assigning future usage actions to you and providing access to the full range of our Services. When ordering any additional features or products, the processing of your data is also necessary for contract performance and is therefore based on a specific purpose and justified pursuant to Article 6(1)(b) GDPR.

The storage of the IP address and the time of registration is necessary to ensure the security of our IT systems. This also constitutes our legitimate interest, which is why the processing is lawful under Article 6(1)(f) GDPR.

The personal data you enter will be stored until such time as you delete the data within your profile or until your profile is completely deleted from our systems. Notwithstanding this, we will only continue to process certain personal data if



we are legally or contractually authorized to do so. This is the case, for example, when we are permitted to retain contractual or payment data even after your profile has been deleted—for billing or other reasons necessary for the proper execution of our contractual relationship.

5.3. Functions of our Services

Depending on your registration and the specific IT Service you have selected, the corresponding booked features of our Services will be made available to you. All features are provided to enable you to fully utilize the scope of our Services according to your chosen plan and to ensure the best possible outcome in our collaboration. We do not disclose the data you enter to unauthorized third parties, but process it solely for the purpose of fulfilling the contractual relationship established with you, in particular the user agreement you entered into by using our Services. The legal basis for processing your data therefore arises from Article 6(1)(b) GDPR.

5.4. Chat- & Messagesystem

Within our Services, we provide you with the opportunity to communicate with other users via integrated chat and messaging functions, exchange information, and potentially initiate or conclude contracts. The categories of data processed in this context include master data, contact data, and, if applicable, content data, contract data, and payment data. We transmit these data to the person you contacted only to the extent that you have explicitly approved such transmission or have included the data yourself in your messages. Additionally, we receive information about the time and participants of any communication initiated via our chat and messaging functions. Furthermore, the personal data you enter is transmitted to us by your browser and stored in our IT systems. Your IP address and the time of registration are also stored.

The processing operations associated with the use of our chat and messaging systems serve the purpose of assigning usage actions to specific users and enable you to access the full range of our Services. Since the use of chat and messaging functions is a core element of our Services, the processing of your data is necessary for the performance of the contract and is therefore purpose-bound and required in accordance with Article 6(1)(b) GDPR.

The storage of your IP address and the time of use of our chat and messaging functions is necessary to ensure the security of our IT systems. This also constitutes our legitimate interest, which is why the processing is lawful pursuant to Article 6(1)(f) GDPR.

The personal data you enter will be stored until the deletion of your profile with us and, beyond that, only as long as the processing is necessary to fulfill any contractual obligations. There is no intention to share your data with any other third parties.

5.5. Community-Function

Our Services give you the opportunity to view posts published by other users, to comment on them, and to publicly interact with others. The categories of data processed in this context include master data, contact data (where applicable), and content data (where applicable). These data are published in publicly accessible areas of our platform. Furthermore, the personal data you provide is transmitted to us by your browser and stored in our IT systems. Your IP address and the time of registration are also stored.

Anschrift / Address
Gentlent GmbH
Am Trippelsberg 92
40589 Düsseldorf
Germany

Kontakt / Contact
E-Mail: support@gentlent.com
Tel.: +49 (0) 211 86843 - 0
Fax: +49 (0) 211 86843 - 999
Web: <https://www.gentlent.com>

Rechtliches / Legal Details
Amtsgericht Düsseldorf
HR-Nr.: HRB 103552
USt.-ID: DE366296666
CEO: Tom Klein, Florian Oliver Elke

Bankkonto / Bank Account
bunq B.V. Niederlassung Deutschland
IBAN: DE56 3701 9000 1010 9445 44
BIC: BUNQDE82



The processing activities related to the community function serve the purpose of enabling users to exchange ideas and experiences regarding our Services and their application, and to make full use of our service offerings. As the use of the community function is an essential part of our Services, the processing of your data is carried out for the performance of the contract and is therefore purpose-bound and necessary pursuant to Article 6(1)(b) GDPR.

The storage of your IP address and the time of use of the community function is necessary to ensure the security of our IT systems. This also constitutes our legitimate interest, which makes the processing lawful under Article 6(1)(f) GDPR.

The personal data you enter will be stored until your profile is deleted. Beyond that, data will only be retained as long as necessary for contractual performance and where technically feasible.

There is no intention to transfer your data to other third parties.

6. Communication Services

6.1. Contact

We process your personal data that you provide to us when you contact us for the purpose of responding to your inquiry, your email or your callback request. The processed data categories are master data, contact data, content data, possibly usage data, connection data and possibly contract data. In individual cases, we forward this data to companies affiliated with us or third parties that we commission to process orders. The legal basis for the processing depends on the purpose of the contact. With your request in the contact form or by contacting us by e-mail, you declare that you would like answers or information on certain topics. You also leave your data for this purpose. We answer your request as requested and process your data for this purpose. Therefore, the authorization to process your data is based on Art. 6 para. 1 lit. b GDPR, as we process it to answer your request and thus to fulfill the contract.

6.2. Support

We process the personal data you provide to us in the context of support requests for the purpose of assisting you with your support issue. The categories of data processed in this context include master data, contact data, content data, and, if applicable, usage data, connection data, and contract data. We forward this data to third parties, in particular to Intercom R&D Unlimited Company, 124 St Stephen's Green, DC02 C628, Dublin 2, Ireland, which we have engaged to support us in handling support processes. If Intercom transfers this data to a third country (e.g., the United States), this will only occur in individual cases, on the basis of a data processing agreement concluded with Intercom and in accordance with standard contractual clauses agreed with Intercom and other safeguards permitted under the GDPR. These safeguards ensure that your personal data is processed with a level of protection equivalent to that within the EU, in particular on the basis of the EU-U.S. Data Privacy Framework (DPF). The legal basis for processing depends on the purpose of your support request. By submitting a support request, you are indicating that you wish to receive assistance on certain topics. For this purpose, you provide your data. We and our service provider Intercom process this data in order to respond to your request. Therefore, the legal basis for processing your data is Article 6(1)(b) GDPR, as we process the data to respond to your request and thereby fulfill the corresponding contract. The legal basis for involving Intercom as a service provider for handling support processes is Article 6(1)(f) GDPR. We have a legitimate interest in processing your support requests as efficiently as possible so that we can provide you with timely and accurate results. We achieve this goal through the integration of Intercom's Services. Your personal data is not unduly affected in this



context, as support requests typically relate not to personal data, but rather to system-related content.

6.3. Application Management

We process your personal data that you provide to us as part of the application process (e.g. via the corresponding contact form in our Services) for the purpose of processing your application and carrying out the application process. At your request, we will also consider your application in future application procedures with us or our subsidiaries. The processed data categories are master data, contact data, content data, usage data (not for postal applications), connection data (not for postal applications), contract data. The legal basis for the processing of your data in the context of applicant management is based on Art. 88 para. 1 GDPR i.V.m. § Section 26 para. 1 sentence 1 BDSG (German Federal Data Protection Act). The legal basis for applications to subsidiaries and for storage for future application procedures is Art. 6 para. 1 lit. a GDPR in conjunction with Art. 7 GDPR, § 26 para. 2 BDSG; Art. 6 para. 1 lit. f GDPR.

6.4. ChatGPT

In our Services, we use the "ChatGPT" service from OpenAI in the version OpenAI API. The recipient of the data is OpenAI Ireland Limited, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland (as joint controller pursuant to Art. 26 GDPR). The categories of data processed include master data, contact data, content data, if applicable usage data, connection data, and contract data. If OpenAI transfers this data to a third country (e.g., the USA), this is done based on a data processing agreement concluded with OpenAI and in accordance with standard contractual clauses agreed with OpenAI and other safeguards permitted under the GDPR, which ensure the security of your personal data processing with a level of protection equivalent to that within the EU, in particular based on the EU-U.S. Data Privacy Framework (DPF). ChatGPT is an artificial intelligence integrated into our Services, used for the automated generation and creation of texts and content, as well as for process optimization. The purpose of data processing is to provide the intelligent system that processes all interactions in the most efficient and beneficial way for you. In providing our Services or parts thereof, ChatGPT serves as an essential basis for the corresponding data processing without which we cannot offer our Services. Therefore, the processing of your data by ChatGPT serves the performance of the contract, is purpose-bound, and necessary pursuant to Art. 6(1)(b) GDPR. The use of personal data by OpenAI for its own training purposes is excluded.

6.5. WhatsApp Business

For communication purposes, especially for the preparation, execution, mediation, clarification, or billing of order processes, we use the instant messaging service "WhatsApp" provided by WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2. In this context, personal data such as name, phone number, email address, postal address, customer number, i.e., master data, contact data, and usage data are processed. WhatsApp accesses all contacts from your individual phonebook. WhatsApp may share all data with other companies within and outside the Meta corporate group. Further information can be found in WhatsApp's privacy policy at: <https://www.whatsapp.com/legal/privacy-policy-eea>. If WhatsApp or Meta transfers this data to a third country (e.g., the USA), this occurs only in individual cases, based on a data processing agreement concluded with Meta and in accordance with standard contractual clauses agreed with Meta and other safeguards permitted under the GDPR, ensuring the security of your personal data processing with a level of protection equivalent to that within the EU, particularly based on the EU-US Data Privacy Framework (DPF). The legal basis for using WhatsApp is Art. 6(1)(a) GDPR. If you have not



given us your consent for the use of WhatsApp (no opt-in or revocation of consent), we will no longer use WhatsApp to communicate with you.

7. Payment

For the processing of payment claims, we offer various payment methods. To this end, we integrate the payment service providers described below. This is done for the purpose of properly and appropriately providing our Services. The data processed in this context include usage data, connection data, master data, payment data, contact data, or contract data, such as account numbers or credit card numbers, passwords, TANs, checksums, as well as contract-, amount-, and recipient-related information. These details are required to carry out the transactions. The entered data are processed and stored exclusively by the payment service providers. We do not receive any account- or credit card-related information, but only information about the confirmation or rejection of the payment. In some cases, your data may be transmitted by the payment service providers to credit agencies. This transmission serves the purpose of identity and creditworthiness verification. For this, we refer to the terms and conditions 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 you through our Services and thereby fulfill our contractual obligations if we use third parties, such as payment service providers, to process payment transactions. We have concluded data processing agreements with each of the payment service providers to ensure the security of your data processing at all times.

Payment Service Provider

Stripe

If you choose a payment method from the payment service provider Stripe, the payment processing will be carried out by the payment service provider Stripe Payments Europe Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland, to whom we transmit the information you provide during the ordering process along with information about your order (name, address, account number, bank code, possibly credit card number, invoice amount, currency, and transaction number) in accordance with Art. 6(1)(b) GDPR. Further information on Stripe's data protection can be found at <https://stripe.com/de/privacy#translation>.

Stripe reserves the right to conduct a credit check based on mathematical-statistical methods to safeguard its legitimate interest in assessing the user's creditworthiness. The personal data necessary for the credit check and received during payment processing may be transmitted by Stripe to selected credit agencies, which Stripe discloses to users upon request. The credit report may contain probability values (so-called score values). Where score values are included in the credit report result, these are based on a scientifically recognized mathematical-statistical method. The calculation of the score values includes, among other things but not exclusively, address data. Stripe uses the result of the credit check regarding the statistical likelihood of payment default to decide on the authorization to use the selected payment method.

You may object to this processing of your data at any time by sending a message to Stripe or the commissioned credit agencies.

However, Stripe may still be entitled to process your personal data if this is necessary for the contractual payment processing.



8. Hosting

8.1. Provision of our services

In order to provide you with our Services, we use the Services of a web hosting provider. Our Services are accessed from the servers of these web hosting providers. For these purposes, we use the web hosting provider's infrastructure and platform Services, computing capacity, storage space and database Services, as well as security Services and technical maintenance Services.

The processed data includes all such data that you enter or that is collected by you in the course of your use and communication in connection with your visit to our Services (e.g. your IP address). Our legal basis for using a web hosting provider to provide our Services results from Art. 6 para. 1 lit. f GDPR (legitimate interest).

8.2. Collection of access data and log files

We ourselves (or our web hosting provider) collect data on each access to the server (server log files). The server log files may include the address and name of the Services and files accessed, the date and time of access, the volume of data transferred, notification of successful access, browser type and version, your operating system, referrer URL (the previously visited page) and, as a rule, IP addresses and the requesting provider.

The server log files may be used on the one hand for security purposes, e.g. to prevent server overload (especially in the event of abusive attacks, so-called DDoS attacks) and on the other hand to ensure the utilization of the servers and their stability. Our legal basis for using a web hosting provider to collect access data and log files results from Art. 6 para. 1 lit. f GDPR (legitimate interest).

9. Tracking & Tools

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

Google Analytics

We use Google Analytics for the purpose of statistically analyzing your use of our Services. Your IP address is collected by us before it is anonymized by Google by shortening it before it is permanently stored on their servers. Processed data is usage data & connection data. The recipient of the data is Google Ireland Ltd, Gordon House, Barrow Street Dublin 4 Ireland (as joint controller, Art. 26 GDPR). If Google transfers this data to a third country (e.g. the USA), this will only be done on a case-by-case basis, on the basis of an order processing contract concluded with Google and in accordance with standard contractual clauses agreed with Google and other security measures permitted by the GDPR, which ensure the security of the processing of your 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 the use of the Google Analytics is your consent



(e.g. via an opt-in in the consent banner), provided that you have given us this consent during your visit to our Services and therefore results from Art. 6 para. 1 lit. a GDPR. On the basis of your consent, cookies, so-called "beacons" or similar (text) files are stored on your end device and personal data is read out as a result. If you have not given us your consent to use the Google Analytics (no opt-in in the consent banner or revocation of your consent), we will not (or no longer) use the Google Analytics during your visits to our Services.

ReCaptcha

We integrate the "ReCaptcha" function to detect bots, e.g., during inputs in online forms, into our Services. Using ReCaptcha, your behavior (e.g., mouse movements or queries) is evaluated to distinguish humans from bots. The processed data includes usage data and connection data. The recipient of the data is Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland (as joint controller under Art. 26 GDPR). Should Google transfer this data to a third country (e.g., the USA), this only occurs in individual cases, based on a data processing agreement concluded with Google and in accordance with Google's agreed standard contractual clauses and other GDPR-approved security measures that ensure the protection of your personal data at a level equivalent to that in the EU, particularly based on the EU-US Data Privacy Framework (DPF). The legal basis for using ReCaptcha is your consent (e.g., via opt-in in the consent banner), provided you have given it during your visit to our Services, and therefore results from Art. 6(1)(a) GDPR. Based on your consent, cookies, so-called "beacons," or similar (text) files are stored on your device and personal data is read out. If you have not given your consent for the use of ReCaptcha (no opt-in in the consent banner or revocation of your consent), we will no longer use ReCaptcha during your visits to our Services or may no longer be able to properly provide you with our online forms.

Hotjar

We use Hotjar to analyze your surfing and clicking behavior in our Services, to create so-called "heatmaps" based on this analysis, and to optimize and tailor our Services to your needs. Processed data includes usage data & connection data. The recipient of the data is Hotjar Ltd., Level 2, St Julian's Business Centre, 3, Elia Zammit Street, St Julian's STJ 1000, Malta. No transfer of data to a third country outside the EU takes place.

The legal basis for using Hotjar is your consent, which you may give us, for example, via an opt-in in the consent banner (Art. 6 para. 1 lit. a GDPR). Based on your consent, cookies, so-called "beacons," or similar (text) files are stored on your device, allowing personal data to be read. If you have not given or have withdrawn your consent to the use of Hotjar, we will not (or no longer) use Hotjar during your visits to our services.

10. Newsletter

With your consent (usually given by subscribing), we send you newsletters, emails, and other electronic notifications (hereinafter "Newsletters"). Our newsletters typically contain technical, commercial, and promotional information about our Services.

To subscribe to our newsletter, it is generally sufficient to provide your email address. If necessary, we may also ask you to provide additional information such as your name or similar details.



The subscription to our newsletter always takes place using a so-called double opt-in procedure. After subscribing, you will receive an email asking you to confirm your subscription by clicking a confirmation link. This confirmation is necessary to prevent someone else from subscribing to the newsletter with your email address. We log newsletter registrations for the purpose of being able to prove the subscription process in accordance with legal requirements. For this purpose, we store the registration and confirmation time as well as your IP address. Changes to the data stored by the email service provider are also logged.

You can unsubscribe from our newsletter at any time. Simply click on the "Unsubscribe" button contained in the footer of every newsletter. If you unsubscribe, your email address may be stored for up to three years based on our legitimate interests before we delete it, in order to be able to prove your previously given consent.

If we engage a service provider to send emails, this is based on our legitimate interest in an efficient and secure sending system.

Our newsletters may contain so-called "web beacons." A web beacon is a pixel-sized file that is retrieved from our server (or from the server of the service provider) when the newsletter is opened. During this retrieval, technical information such as information about your browser and system, your IP address, and the time of access are collected.

This information is used to technically improve our newsletters based on the technical data or the target groups and their reading behavior, based on their access locations (which can be determined using the IP address) or the access times. This analysis also includes determining whether the newsletters are opened, when they are opened, and which links are clicked. For technical reasons, this information can be assigned to individual newsletter recipients. However, it is neither our intention nor, if used, that of the service provider to monitor individual users. Instead, the evaluations serve to understand the reading habits of our users and to tailor our content to them or to send different content according to the interests of our users.

The evaluation of the newsletter and the measurement of success are carried out, subject to the explicit consent of the users, based on our legitimate interests for the purpose of operating a user-friendly and secure newsletter system that serves both our business interests and the expectations of the users.

The legal basis for sending newsletters and thus also for the use of web beacons is your consent, which you give by subscribing to the newsletter, and therefore results from Art. 6 para. 1 lit. a GDPR. If you have not given your consent to receive newsletters, we no longer send newsletters to you. This also automatically excludes the use of web beacons.

11. Fanpages on Social Media

We maintain fan pages on the websites of social networks on the Internet and process personal data in this context in order to communicate with the users active there or to offer information about us. We would like to point out that your data may be processed outside the European Union when you visit our fan pages. The operators of the respective social networks are responsible for this. You can find a detailed description of the respective forms of processing and objection options (e.g. opt-out) in the privacy policies of the operators of the respective social networks.

Facebook

We operate a Facebook fan page for our company on Facebook. When you visit the Facebook fan page, Facebook can evaluate your usage behavior and provide us with information obtained from this ("Insights"). Page Insights are used for the purposes of economic optimization and needs-based design of our Services. The categories of data processed may



include master data, contact data, content data, usage data and connection data. The recipient of the data is Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland, as joint controller pursuant to Art. 26 GDPR. The legal basis for the processing of the data in accordance with the provisions mentioned here results from our legitimate interest and thus from Art. 6 para. 1 lit. f GDPR.

Facebook is responsible for implementing your rights as a data subject. Facebook informs you about your rights as a data subject at: https://www.facebook.com/legal/terms/information_about_page_insights_data. You can also assert your rights against us; we will then forward your request to Facebook immediately.

Instagram

We operate a so-called Instagram fan page for our company on Instagram. When you visit the Instagram fan page, Meta can evaluate your usage behavior and provide us with information obtained from this ("Insights"). The page insights are used for the purposes of economic optimization and needs-based design of our website/Services. The categories of data processed may include master data, contact data, content data, usage data and connection data. The recipient of the data is Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland, as joint controller pursuant to Art. 26 GDPR. The legal basis for the processing of the data in accordance with the provisions mentioned here results from our legitimate interest and thus from Art. 6 para. 1 lit. f GDPR.

Meta is responsible for implementing your rights as a data subject. Meta will inform you about your rights as a data subject at: <https://privacycenter.instagram.com/policy>. You can also assert your rights against us; we will then forward your request to Meta immediately.

LinkedIn

We operate a LinkedIn fan page for our company on LinkedIn. When you visit and use the LinkedIn fan page, LinkedIn can evaluate your usage behavior and provide us with information obtained from this. This information is used for the purposes of economic optimization and needs-based design of our website/Services. The categories of data processed are master data, contact data, content data, usage data and connection data. The recipient of the data is LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland, as joint controller pursuant to Art. 26 GDPR. The legal basis for the processing of the data in accordance with the provisions mentioned here results from our legitimate interest and thus from Art. 6 para. 1 lit. f GDPR.

LinkedIn is responsible for implementing your rights as a data subject. LinkedIn informs you about your rights as a data subject at: <https://linkedin.com/legal/privacy-policy>. You can also assert your rights against us; we will then forward your request to LinkedIn immediately.

TikTok

We operate a so-called TikTok Fanpage for our company on TikTok. When you visit the TikTok Fanpage, TikTok may analyze your usage behavior and share information obtained from this with us. The use of this information serves the purpose of economically optimizing and appropriately designing our website/Services. The categories of data processed may include master data, contact data, content data, usage data, and connection data. The recipient of the data is TikTok Technology Limited, 10 Earlsfort Terrace, Dublin D02 T380, Ireland, acting as a joint controller in accordance with



Art. 26 GDPR. The legal basis for processing the data as described here is our legitimate interest pursuant to Art. 6 para. 1 lit. f GDPR.

TikTok is responsible for implementing your data subject rights. TikTok informs you about your data subject rights at: <https://www.tiktok.com/legal/privacy-policy>. You may also assert your rights directly with us, and we will promptly forward your request to TikTok.

X

We operate an X Fanpage for our company on X. When you visit and use our X Fanpage, X may analyze your usage behavior and share information obtained from this with us. The use of this information serves the purpose of economically optimizing and appropriately designing our website. The categories of data processed include master data, contact data, content data, usage data, and connection data. The recipient of the data is Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2, Ireland, acting as a joint controller pursuant to Art. 26 GDPR. The legal basis for processing the data as described here is our legitimate interest pursuant to Art. 6 para. 1 lit. f GDPR.

X is responsible for implementing your data subject rights. X informs you about your data subject rights at: <https://www.twitter.com/privacy>. You may also assert your rights directly with us, and we will promptly forward your request to X.

YouTube

We operate a channel about our company on YouTube. When you visit and use our YouTube channel, Google can evaluate your usage behavior and provide us with information obtained from this. This information is used for the purpose of economic optimization and needs-based design of our website. The categories of data processed are master data, contact data, content data, usage data and connection data. The recipient of the data is Google Ireland Ltd, Gordon House, Barrow Street Dublin 4 Ireland, as joint controller pursuant to Art. 26 GDPR. The legal basis for the processing of the data in accordance with the provisions stated here results from our legitimate interest and thus from Art. 6 para. 1 lit. f GDPR.

YouTube is responsible for implementing your rights as a data subject. YouTube will inform you about your rights as a data subject at: <https://www.youtube.com/howyoutubeworks/our-commitments/protecting-user-data/#privacy-guidelines>. You can also assert your rights against us; we will then forward your request to YouTube immediately.