Privacy Policy

The controller for the collection of personal data for the Qdrant Cloud Service is:
Qdrant Solutions GmbH
Chausseestr. 86
10115 Berlin
(hereinafter: “Qdrant” or “we/us”).

Questions regarding data protection and the processing of your personal data can be addressed to us in writing at any time. Or write an e-mail to privacy@qdrant.com.

General information on the collection and processing of data
We collect and process personal data if you provide it to us when contacting us or via an input form on the Qdrant Cloud Service. We also collect and process data that is generated when you use the Qdrant Cloud Service. Personal data is any information relating to an identified or identifiable natural person.

In the following, we refer to “data” in general terms when explaining the collection and processing operations in detail. Your data will be processed in accordance with the provisions of the EU General Data Protection Regulation (GDPR), the German Federal Data Protection Act (BDSG) and the German Telecommunications Telemedia Data Protection Act (TTDSG).

In the following, we explain in detail how we process which data on which legal basis. In addition, we will explain what rights you have and how long your data will be stored.

Legal basis for the processing of personal data
The processing of your personal data may be necessary for various reasons. The processing is partly based on legal regulations, e.g. according to Art. 6 para. 1 letter b) of the GDPR for the purpose of fulfilling a contract or for the implementation of pre-contractual measures that take place upon your request, or according to Art. 6 para. 1 letter f) of the GDPR due to our or third parties’ legitimate interests, e.g. in responding to any other request you may have addressed to us.

If no such legal permission for the processing of personal data exists, we ask for your consent before we process personal data.

Processing of data by means of log files
When the Qdrant Cloud Service is called up, so-called log files are stored on the basis of Art. 6 para. 1 letter f) of the GDPR, in which certain access data are stored. The thereby stored data set contains the following data:

- the IP address,
- the date,
- the time,
- which file was accessed,
- the status,
- the request that your browser has made to the server,
- the amount of data transferred,
- the Internet page from which you came to the requested page (referrer URL), as well as
- the product and version information of the browser used, your operating system, and the country from which the request was made.

The temporary storage of this data is technically necessary in order to be able to call up the Qdrant Cloud Service in your browser. IP addresses are generally only stored for a maximum of seven days and then deleted.

Our legitimate interest in the further processing of your data is outlined below: We continue to store the log files in anonymized form after deletion of the IP address. We can use this data for statistical evaluations, e.g. to find out on which days and at which times the Qdrant Cloud Service is particularly popular and how much data volume is generated on the Qdrant Cloud Service. In

addition, the log files may enable us to detect errors, e.g. faulty links or program errors. Thus, we can use the logfiles for the further development of the Qdrant Cloud Service.

We reserve the right to use log files before deleting the IP address to identify you in the event that certain facts give rise to the suspicion that users are using the Qdrant Cloud Service and/or individual services in violation of the law or the Cloud Service Agreement. In the event of such suspicion, IP addresses may have to be stored longer than usual or forwarded to investigating authorities. However, we will immediately delete the IP addresses as soon as they are no longer needed or further investigations appear futile.

Contact options for the Qdrant Cloud Service

If we provide contact forms within or in connection with the Qdrant Cloud Service, you can enter your contact details via these forms, e.g. in order to request offers regarding our services. For this purpose, you can also use the contact data stored in the imprint and, if applicable, also elsewhere on the Qdrant Cloud Service and contact us by telephone or e-mail. In these cases, we process the data provided by you in accordance with Art. 6 para. 1 letter b) of the GDPR for the purpose of fulfilling your (pre-)contractual request addressed to us.

If you send us other inquiries and provide us with personal data in the process, we process your data pursuant to Art. 6 para. 1 lette f) of the GDPR based on our legitimate interest in responding to your inquiry.

Registration for and use of the Qdrant Cloud Service

To use the Qdrant Cloud Service, your registration is required. The legal basis for the processing of your data is Art. 6 para. 1 letter b) of the GDPR, insofar as we require your data for the establishment and implementation of the contract for the use of the Qdrant Cloud Service. In the context of registration and profile creation, we process data as follows:

a) Registration

Registration only requires you to provide an email address. You will also be asked to select a password. To protect your profile from unauthorized access by third parties, we recommend using a strong password that consists of at least eight characters and combines letters, numbers, and special characters. Also, be sure to keep the password to yourself and do not share it with third parties.

For registration you can also use your login data from Github or Google, provided you have an active account with these services. By means of this so-called single sign-on procedure, we want to make it easier for you to register and log in to the Qdrant Cloud Service. Because in this way you do not have to remember any further access and login data for your use of the Qdrant Cloud Service. If you use a single sign-on procedure, we receive the information from the relevant provider that you have released for transmission. The legal basis for processing by us is your express consent pursuant to Art. 6 para. 1 letter a) of the GDPR. This information may be, in particular, your name, your e-mail address, the user ID with the provider concerned and, if applicable, a profile picture.

We would like to point out that, in accordance with the data protection conditions and terms of use of the providers, there may also be a transfer of further data when consent is given if this has been marked as "public" in your privacy settings or otherwise approved by you for transfer for the purposes of the single sign-on procedure. However, of the data transmitted to us, we only process the data that is necessary for registration and login to the Qdrant Cloud Service (Art. 6 para. 1 letter b) of the GDPR); we delete any further data transmitted to us immediately upon receipt.

For the purpose and scope of data transmission in the context of the use of single sign-on procedures and the further processing and use of your data by the providers, as well as your rights in this regard and setting options for protecting your privacy, please refer to the data protection notices of the providers concerned:

Google: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; https://policies.google.com/privacy
Github: Github B.V., Prins Bernhardplein 200, Amsterdam, 1097JB, The Netherlands: https://docs.github.com/en/site-policy/privacy-policies/github-privacy-statement

To further secure the registration process and to offer the single sign-on procedure, we also use the "Auth0" service of the provider Auth0, Inc., 10800 NE 8th Street, Suite 600, Bellevue, WA 98004, U.S.A ("**Auth0**"). Auth0 and its subcontractors act for us as processors (Art. 28 of the GDPR) and process data solely for the purposes specified by us. In some cases, data may be transferred to and processed in countries outside the EU or the European Economic Area for this purpose ("**Third Countries**"). We have entered into an agreement with Auth0 which contains the standard contractual clauses pursuant to the EU Commission's Implementing Decision (EU) 2021/914 of 04.06.2021. Auth0 has also taken supplementary security measures, in particular implemented comprehensive encryption mechanisms, to ensure an adequate level of data protection even when processing your data in the U.S., and Auth0 has committed itself to the principles established under the EU-US Data Privacy Framework. The EU-US Data Privacy Framework has been acknowledged by the EU Commission as an adequate data transfer mechanism with respect to data transfers from the EU to the United States (Art. 45 of the GDPR).

b) Use of the Qdrant Cloud Service

Upon registration or receipt of an invitation e-mail, you may, at your sole discretion, create a user account to access and use the Qdrant Cloud Service. Using the Qdrant Cloud Service requires adherence to the terms and conditions of the agreement concluded between us and our customer. As set out therein in further detail, your account is a personal account, and only you are allowed to use the Qdrant Cloud Service under your user account. Thus, we will process your personal data that (a) you submit in the course of the registration or account creation procedure, and (b) we collect or generate in connection with your use of the Qdrant Cloud Service (including without limitation, any information related to your computer, server, or laptop that is part of your company's systems or network and that accesses, is managed or tracked by, or is registered to access, the Qdrant Cloud Service. We will process such personal data for the purposes of entering and maintaining a contractual relationship with our customer (Art. 6 para. 1 letter b of the GDPR), surveilling your compliance with and enforcing the agreement, ensuring system

availability, IT and data security, all these purposes and processing activities serving and being required for our legitimate interest to run and constantly improve the Qdrant Cloud Service for the benefit of our customers, yourself as a user and ourselves (Art. 6 para. 1 letter f of the GDPR).

Please note, however, that we will not use for our own business purposes any data (including your personal data), information or material you provide, submit or upload to the Qdrant Cloud Service unless: (a) to support our customer's and your use of the Qdrant Cloud Service and prevent or address service or technical problems; (b) in order to create aggregated data in accordance with our agreement with our customer; or (c) as our customer expressly permits in writing. In this respect, we have entered into an agreement in accordance with Art. 28 of the GDPR with our customer. Inasmuch as this data processing agreement allows us to create aggregated data, your personal data will by anonymized such that it does not include any identifying information of, or reasonably permit the identification of, our customer or any individual (including yourself).

c) Storage Periods

If you, upon registration or receipt of an invitation e-mail, decide to use and subscribe to the Qdrant Cloud Service, we will process your personal data as described above and store such personal data for as long as it is required for the respective purposes. However, we shall delete your personal data upon termination or expiry of the agreement between us and our customer at the latest. This does not apply, and we will be under no obligation to delete your personal data, if and inasmuch as we are under a statutory retention obligation, in which case we will delete your personal data as soon as such obligation has expired.

Payment

The use of the Qdrant Cloud Service may be subject to a fee. For billing purposes, we may use data from contact persons within the company. This data, along with other billing information, is also transmitted to our service provider Stripe, Inc., 510 Townsend Street San Francisco, CA 94103 USA ("**Stripe**"). Stripe is represented in the EU by Stripe Payments Europe, Ltd., The One Buidling,
1 Lower Grand Canal Street, Dublin, D02 HD59 Ireland (Art. 27 GDPR), but nonetheless also processes data in the U.S.A. We have entered into an agreement with Stripe that includes the standard contractual clauses pursuant to the EU Commission's Implementing Decision (EU) 2021/914 of 04 June 2021. Stripe has also taken supplementary security measures to ensure an adequate level of data protection also when processing your data in the U.S., and Stripe has committed itself to the principles established under the EU-US Data Privacy Framework. The EU-US Data Privacy Framework has been acknowledged by the EU Commission as an adequate data transfer mechanism with respect to data transfers from the EU to the United States (Art. 45 of the GDPR).

Marketing

We have a legitimate interest to inform our customers and people using the Qdrant Cloud Service about the activities of our company, current developments relating to our services, special offers, promotions, events, and competitions. The legal basis is Art. 6 para. 1 letter f of the GDPR, §7 para. 3 of the German Act Against Unfair Competition (UWG), if we have received your e-mail

address in connection with an order placed with us, unless you have objected to receiving such advertising.

You can object to the use of your e-mail address for direct advertising at any time without incurring any costs other than the transmission costs according to the basic rates. To do so, simply click on the link at the end of our newsletter or write a message to privacy@qdrant.com. After your objection, we will permanently store your address on a so-called blacklist to ensure that we do not send you any more newsletters in the future.

Links to other websites

Our Qdrant Cloud Service may contain links to websites of other providers. We point out that this information on data protection applies exclusively to the websites and other offers of Qdrant. When accessing the websites of other providers, please check the data protection information stored there. We have no influence on and cannot control that such other providers comply with the applicable data protection provisions at all times and in full.

Categories of recipients of data; data transfers to a third country

We have commissioned various service providers who process data of the users of the Qdrant Cloud Service on our behalf. These include, for example, cloud providers for software that we use, or e-mail service providers, but also our host provider on whose servers the Qdrant Cloud Service is operated. As a matter of principle, we carefully select all service providers and oblige them to maintain the protection of personal data. Data is not transferred to third countries unless expressly described otherwise herein.

In addition to the service providers mentioned above, we use Mailchimp as an e-mail service. Mailchimp is a service provided by The Rocket Science Group, LLC, 675 Ponce De Leon Ave NE, Suite 5000, Atlanta, GA 30308, United States ("**Mailchimp**") Mailchimp also processes data in the U.S.A. We have entered into an agreement with Mailchimp that includes the standard contractual clauses pursuant to the EU Commission's Implementing Decision (EU) 2021/914 of 04 June 2021. Mailchimp has also taken supplementary security measures to ensure an adequate level of data protection also when processing your data in the U.S., and Mailchimp has committed itself to the principles established under the EU-US Data Privacy Framework. The EU-US Data Privacy Framework has been acknowledged by the EU Commission as an adequate data transfer mechanism with respect to data transfers from the EU to the United States (Art. 45 of the GDPR).

Encryption

If you enter data on the Qdrant Cloud Service, this data is transmitted via the Internet using SSL encryption. We secure our Qdrant Cloud Service and other systems in an appropriate manner (Art. 24, 32 of the GDPR) by technical and organizational measures against loss, destruction, access, modification or distribution of your data by unauthorized persons.

Your rights

a) Rights as a data subject

Pursuant to Art. 15 of the GDPR, you have the right to request information free of charge about the personal data that has been stored about you. In accordance with Art. 16, 17 and 18 of the

GDPR, you also have the right to correct incorrect data and to restrict the processing or deletion of your personal data. All these rights exist in each case under the legal conditions or to the extent provided by law.

You are also entitled, under the conditions set out in Art. 20 of the GDPR, to receive the personal data relating to you that has been stored in a structured, common, and machine-readable format and to transmit this data to another person responsible or to have it transmitted by us.

b) In particular: Your right to object

In addition, pursuant to Art. 21 para. 1 of the GDPR, you have the right to object to the processing of personal data concerning you which is carried out on the basis of Art. 6 para. 1 letter f) of the GDPR, including profiling, on grounds relating to your particular situation. We will comply with this objection insofar as the legal requirements for its assertion are met.

If your personal data is processed for direct marketing purposes, you have the right to object at any time to the processing of your data for such marketing, including profiling, insofar as it is related to such direct marketing, in accordance with Art. 21 para. 2 of the GDPR. In such a case, we will no longer use your personal data for the purposes of direct marketing.

c) Contact address for exercising your rights

Please address any requests regarding your personal data to the contact details provided at the beginning of this privacy policy.

d) Right of appeal to the supervisory authority

You also have the right to lodge a complaint with a data protection supervisory authority about our processing of personal data.

Duration of storage and routine deletion

Unless otherwise expressly stated in this Privacy Policy, we process and store personal data only for the period of time necessary to achieve the purpose of the processing or as soon as provided for by laws or regulations to which we are subject.

If the purpose of storage no longer applies or if a legally prescribed storage period expires, the personal data will be routinely restricted in its processing or deleted in accordance with the statutory provisions.

Status: 15 September 2023