

memoQ Privacy Policy

We need some of your personal data to provide you with products and services, or to engage with you online. We never collect more personal data than absolutely necessary for the purposes listed below. We will only use your personal data for the purposes below, and nothing else.

We will never sell or hand over your personal data to any third parties. However, sometimes we need to use external services (data processors) to deliver services or communications to you. In this Privacy Policy, we list all the external data processors, and explain how they receive or process your personal data.

A. Details of the controller

When we collect personal data from you, we are the controller and you are the data subject. Our details as the data controller are as follows:

memoQ Zrt.

Rákóczi út 70-72. II. em.

Budapest, 1074 Hungary

compliance@memoq.com

<https://memoq.com/legal>

Business registry number: 01-10-140071

Tax ID: 25429356-2-42

B. Data Protection Representative, Chief Information Security Officer

The person responsible for the protection of your personal data is our Data Protection Representative, **Anett Guth** (she/her; based in Budapest). To contact her—or memoQ Zrt. in general about data protection matters—, please write to [**data-protection@memoq.com**](mailto:data-protection@memoq.com).

The person responsible for the actual security measures, including technical and organizational, is called the Chief Information Security Officer (CISO in short). Our CISO is Zsolt Farkas (he/him). To contact the CISO, please write to [**information-security@memoq.com**](mailto:information-security@memoq.com).

C. Short summary

We will give you more details below, but we wish to point out that we will not sell personal data to anyone. We will not send personally identifiable information in e-mail to unauthorized third parties. We will do everything in our power to ensure that customer data are properly protected from unauthorized access, copying, altering, or theft.

Please read every section that might apply to you.

D. Details about collecting, storing, and processing your information

D.1. When we provide products or services to you or your organization

1. *What personal data are we collecting and processing?*

We directly collect the following types of personal data from you:

- a. name,
- b. e-mail address,
- c. organization (company) (if applicable),
- d. country,
- e. city,
- f. phone number,
- g. your purchase history, and
- h. a profile description. The profile description is a single phrase, describing the user group or the type of organization you belong to (individual/freelancer, translation company, other company, educational institution etc.). You will be asked to choose one from several pre-defined profile descriptions.

When you visit our website, we will also send cookies to your browser. Some of these cookies are necessary for the memoQ website to open. For more details, see the section called “When you are a visitor”.

Also, when you visit our website, you may interact with a chatbot. The chatbot may offer to collect your e-mail address. Providing the information is voluntary, and if you do not specify the e-mail address, you can still browse the website.

2. *What is the purpose of processing the personal data?*

Your personal data are being collected because you are our customer as a freelance professional, or else you represent an organization that is our customer. We use your personal data so that we can provide products and services to you or to the organization which you are working for. In addition, we may send you offers or information; we may also collect feedback from you. More specifically, this means the following:

- a. Checking if you are or your organization is eligible for certain product licenses, or certain services;
- b. Contacting you or your organization about services or changes to services and service terms;
- c. Billing you or your organization for paid licenses and services you purchase or subscribe to;
- d. Sending notices about the licenses you are or your organization is using;
- e. Sending expiry notices about licenses and services you are or your organization is using, as well as information about available upgrades. This includes follow-up e-mails when you are or your organization is trialling memoQ;
- f. Operating a chatbot to provide customer service for you or your organization;
- g. E-mail advertising: Sending promotion offers through mass e-mailing or through social media targeting;
- h. Inviting you or your organization to surveys about our products, services, or plans, for the purpose of quality assurance as well as more accurate planning;
- i. Market research: Collecting market information where the personal data collected from you may determine which profile group(s) you or your organization belong(s) to. Such groups will determine the types of offers (discounts or product types) we may make to you or your organization later on. We may make these assignments by automated means;
- j. Targeted or retargeted advertisements through Facebook, Twitter, LinkedIn, and Google (and their affiliated networks). This may or may not use your personal data. Most of the time we use cookies to do targeting, but sometimes your e-mail address is also used;

- k. Inviting you or your organization to provide reviews, case studies and testimonials for specific target groups.

3. What is our legal basis to collect and process these personal data?

If you enter into an agreement with us as a natural person, we process your data, regarding items of a) through f) in the list above, to fulfil our contract with you—we need to perform those activities to be able to provide you with products and related services or conclude a relevant contract, i.e. the processing of your personal data is necessary to perform the contract between you and us or take steps based on your request(s) prior to entering into a contract [Article 6 (1) b) of the GDPR]. If you represent an organization, our data processing is based on our legitimate interest to perform our contract with your organization by processing your data as its contact person [Article 6 (1) f) of the GDPR].

If you provided your personal data to us as a private individual (and not as a business entity or the representative of a business entity), our processing according to g) through k) is based on your consent. This is done through a consent box in the form where your data are collected. You can withdraw your consent for your data to be used for these activities any time and free of charge by sending a note to **data-protection@memoq.com**. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

4. What about cookies?

On our website, some cookies are necessary for the website to open. These cookies come from CookieBot, DoubleClick.net, Hubspot, and Hotjar (see data processors later). Their purpose is as follows:

- a. Checking if your browser can receive cookies;
- b. Remembering your choice about marketing and convenience cookies;
- c. Distinguishing between humans and bots, in order to create more accurate statistics of the site visits;
- d. Remembering your browser or your session so that different parts of the website will know that you are the same visitor.
- e. Distributing the traffic across different web servers so you receive a faster response from the website.
- f. Displaying embedded YouTube videos on the website, which would not be functional without relevant cookies.

Necessary cookies will not follow you to websites of third parties, and cannot be used to identify you or take personal information from you. We use these cookies out of our legitimate business interest. Most of the time, these cookies prevent the website from asking you the same question again and again, or from being misdirected within various pages.

The memoQ website also uses performance, convenience, and marketing cookies, subject to your consent. For more information, see <https://www.memoq.com/legal/cookies-policy>.

5. Who receives the personal data?

As a rule, we ourselves use the data we collect to provide products and services to you or your organization. We do not collect data on behalf of other organizations, and we do not sell or otherwise hand over the data to third-party controllers.

However, we regularly use external service providers to perform the activities listed above. These service providers are listed in [Appendix 2](#). When you are, or your organization is, our customer, the following providers may receive your data as processors (we are the controller):

- Hubspot: This is where we keep all customer data, including purchase history and communication. Hubspot is also the system that sends out reminders and promotion e-mails to recipients who consented to receive them. Hubspot is an American company, but they have a branch and a data center in Ireland. Still, they may

need to occasionally transfer our (or your) data to America. For this purpose, we have concluded a data processing agreement with them that contains the Standard Contractual Clauses that apply to data transfers between the European Economic Area (“EEA”) and the USA.

- Postmark: We occasionally use this service to send e-mails to remind you of an expiring subscription or service period. Postmark receives your name and e-mail address only. This data processing is transactional, the data are not preserved on the processor’s side. They are based in the USA. They automatically provide a data processing agreement that refers to GDPR’s Standard Contractual Clauses when data are transferred from the EEA to the USA.
- Zendesk: This provider runs our helpdesk. Whenever you send us a support request, either through our website or in e-mail, the data get into this system. It receives your name, organization, e-mail address and the contents of the support request. This provider is also based in the USA. We have a data processing agreement with them, which refers to GDPR’s Standard Contractual Clauses for data transfers between the EEA and the USA.
- Szamlazz.hu and In Mid Air ERP: These providers run our invoicing and accounting systems. They are based in Hungary, just like we are. They receive your name and either your billing information or the billing information of your organization. With them, your data do not leave the EEA.
- Atlassian Jira: This service runs our internal project and ticket management. Your personal data doesn't always get into Jira, only when there is a development task that is related to a request from you or your organization. Atlassian have data centers in the EEA, however, they may need to transfer your data to the USA or Australia. Because of this, we have concluded a data processing agreement with them, which includes GDPR’s Standard Contractual Clauses to handle data transfer from the EEA to the USA.
- Microsoft 365 and Microsoft Azure: Microsoft runs our IT infrastructure. We store all the data in SharePoint. Microsoft stores these data in EEA-based data centers; these data do not leave the EEA. We also use Microsoft Azure as a subprocessor: we store the systems we host for our customers there. When you or your organization ask us to host your memoQ system for you, you can choose the geographical region to store your data in.
- CodeTwo e-mail signatures: E-mails that our staff send you may go through this provider. It is connected to Microsoft 365. The provider is based in Poland, and the data do not leave the EEA while processed by them.

If you participate in surveys, send us ideas or feature requests, attend webinars or e-learning courses, other service providers may also receive your data—or they may collect personal data from you themselves. Further relevant external providers may also be listed in other sections below.

6. Will these personal data be transferred out of the EEA or to an international organization?

Your personal data may be transferred out of the EEA, but not to international organizations. For details about data transfers outside the EEA, see the list above. We have made every precaution so that these transfers happen without a personal data breach and remain otherwise safe.

7. How long do we store these personal data?

If your personal data is necessary to perform a contract with you or your organization, we store your personal data as long as we have a contract with you, and for 5 years after our contract ends, unless a legal dispute emerges between us.

By Hungarian law, we must keep the billing information for 8 years after the last financial transaction with you or your organization. In most cases, this means 8 years after the last invoice was issued to you.

If the data processing is based on your consent, we will also stop storing and processing your data if you withdraw your consent for us to do so; in that case, we will delete the personal data, unless we also process it for other specified, explicit and legitimate purposes.

8. Where do the personal data come from?

We use data that we directly collect from you or your organization. Either we collect the data in e-mail or through a conversation, or else you specify your details in a form on our website. The memoQ.com website also contains a chatbot that may collect an e-mail address. The chatbot is run by Hubspot (see Section D.2.5). We do not purchase or otherwise obtain personal data from third parties.

9. Will we use automated processes to make decisions about the personal data?

There is no profiling based on automated decision-making which produces legal effects concerning you or similarly significantly affects you.

D.2. When we reach out for information or feedback

1. What personal data are we collecting and processing?

When we reach out for feedback, information, or ideas, we usually do it through third-party services. Depending on the service and the actual data collection form, these services will either collect feedback anonymously, or they will collect your name and e-mail address. When we collect your name and e-mail address, your feedback will be associated with your person, and we may use this to follow up with you.

2. What is the purpose of collecting the personal data?

We use the data we collect to improve our products, or else to plan or design our future products, services, or events. We do not use the data for anything else, and we do not hand these data over to third-party controllers.

3. What is our legal basis to collect and process these personal data?

If you provide your data as a private individual, we collect and process these data based on your consent (because your contribution is completely voluntary) [Article 6 (1) a) of the GDPR]. If you represent a business entity, your data are collected and processed based on our (and your organization's) legitimate business interest. Providing us with information or feedback is voluntary: you may decide not to respond, and you also have the right to withdraw your response and have it removed from our systems, along with your contact details.

4. Who receives your personal data?

We normally collect feedback through the following external service providers. When your data are collected or processed, these external service providers are processors engaged by us.

- **Aha.io:** This service runs our Ideas Portal. You may send us ideas and feature requests after we invite you to this portal. We only invite our existing customers, and we reserve the right to select the particular customers we invite. When we invite you, we may submit your e-mail address to aha.io. This is based either on your consent you gave when you became our customer, or else the contract that exists between us—since the ideas you submit directly contribute to the improvement and future development of our products and services. We do not use your feedback for any other purpose. Aha.io is based in the United States, and our data processing agreement cites GDPR's Standard Contractual Clauses to cover for data transfers between the EEA and the USA.
- **SurveyMonkey (Momentive.ai):** We use this service to run various surveys and questionnaires. We do not submit names or contact details to SurveyMonkey, but we may send the link to a survey form to a select customers or contacts based on information stored in our customer relationship management system (Hubspot—see above). Most of the time, we collect information anonymously. When we collect personal identifying information (a name and e-mail address as a maximum), we do not share them with third parties, except for those data processors listed in the previous section. SurveyMonkey is based in the USA but operates through data centers in the EEA, too.

5. Will these personal data be transferred out of the EEA or to an international organization?

The personal data collected may leave the EEA, or more precisely, they may be collected through USA-based services. We maintain data processing agreements with these providers, referring to GDPR's Standard Contractual Clauses that cover data transfers between the EEA and the USA.

6. How long do we store these personal data?

We store these personal data as long as necessary to provide the services and perform analytics, and will delete them immediately afterwards. Generally, we store the personal data until the expiry of the civil law statute of limitation, which is 5 years counted from the event that might give rise to civil law claims, unless the processing of the data is necessary relating to the initiation, enforcement or defense of any legal claims or the applicable law prescribes a longer retention period. We will also delete your data if you specifically request so.

7. Where do the personal data come from?

Any personal data we collect when reaching out for feedback are collected directly from you. We will receive these data through the service provider we used to collect the data. We do not otherwise purchase or obtain such data from third-party controllers.

8. Will we use automated processes to make decisions about the data?

We do not make decisions in an automated way which produces legal effects concerning you or similarly significantly affects you. We may calculate statistics from anonymous or anonymized information, and use the statistics to make decisions, but we will not be able to identify you during such decision-makings and they would have no legal or similarly significant effect on you

D.3. When you are registering for or participating at an event

1. What personal data are we collecting and processing?

We use third-party services to provide for virtual or in-person events or e-learning courses. These events are advertised through social media, through advertising spaces in websites, or else through newsletters that we send to our customers. The information is collected by the third-party service, which acts as a processor. We receive the information from them through our account in each service.

We collect the following information:

- Name, e-mail address, and potentially the name of company your work for;
- Responses to polls and other input if it exists.

In case of e-learning courses on academy.memoq.com (run by Thinkific):

- Name
- E-mail address
- Company name
- Country
- Billing address
- VAT number if applicable
- Complete course and quiz history
- Purchase history (spending amounts)

2. What is the purpose of collecting the personal data?

We collect the data to actually run interactive events; to improve and plan future events; or in case of e-learning courses, to be able to issue certificates based on courses taken and progress achieved.

3. What is our legal basis to collect and process these personal data?

We collect and process personal data based on the performance of a contract between you and us [Article 6 (1) b) of the GDPR], or — if you represent an organization — our legitimate interest to perform our contract with that organization by providing you the possibility to attend those events [Article 6 (1) f) of the GDPR] (you register for an event—we plan and run the event; you register for an e-learning course—we provide the course and issue the certification).

The academy.memoq.com site (run by Thinkific) will place a few necessary cookies from Google on your browser. These cookies are there to distinguish between humans and bots and provide more accurate reports on the usage of the website. You will not be identified through these cookies, and they will not follow you to other websites. We process this information (whether it is a human or a bot visiting the site) based on our legitimate business interest to verify attendees.

4. Who receives the personal data?

The personal data are first received by the third-party service provider we use to provide the event or the e-learning course; we receive the data from them. We may process the data using the service providers listed in the first section. However, we do not hand over the data to any other third-party controllers or processors. We use two service providers to run events or courses:

- Zoom: We use Zoom to run webinars, panels, or other meetings. You register to these events through Zoom, where both Zoom and we ask for your consent to further process your data. You specify a name, an e-mail address, and a company name. You may also provide feedback during the event. Zoom is based in the USA, but normally uses a data center in the EEA. However, we have a data processing agreement with them, referring to GDPR's Standard Contractual Clauses, to secure the data transfers between the EEA and the USA.
- Thinkific: We use this service to run e-learning courses. You sign up and take the course entirely through the Thinkific site. However, we have access to your information through our Thinkific account. Thinkific is based in Canada, which, according to the EEA, counts as a country with adequate data protection regulations. We maintain a regular data processing agreement with them.

5. Will these personal data be transferred out of the EEA or to an international organization?

Both Zoom and Thinkific are based outside the EEA, so it is possible that your data leave the EEA or are even collected outside the EEA. We have made the necessary legal and technical precautions (see above).

6. How long do we store these personal data?

We store these data as long as necessary, and will delete them immediately afterwards. Given the nature of the information collected for this purpose, we cannot give a clear deadline. However, generally, we store the personal data until the expiry of the civil law statute of limitation, which is 5 years counted from the event that might give rise to civil law claims, unless the processing of the data is necessary relating to the initiation, enforcement or defense of any legal claims or the applicable law prescribes a longer retention period. We will also delete the data if you revoke your consent to store and process them.

7. Where do the personal data come from?

In this case, personal data may be collected through our website, or through the Thinkific or Zoom websites. We will receive these personal data through the service provider we used to collect the data. We do not otherwise purchase or obtain such data from third-party controllers.

8. Will we use automated processes to make decisions about the data?

We do not make decisions in an automated way which produces legal effects concerning you or similarly significantly affects you. We may calculate statistics from anonymous or anonymized information, and use the

statistics to make decisions, but these decisions will never be made from personal data or data that can be used to identify data subjects but we will not be able to identify you during such decision-makings and they would have no legal or similarly significant effect on you

D.4. If you are a visitor, considering to buy products or services

1. What personal data are we collecting and processing?

It is not necessary to enter any personal data to browse our website. We use cookies on the website, which are covered by our Cookies policy. You may sign up for a trial run of our products or subscription services, but the moment you do that, you become a customer with a contract—and then the first section applies.

However, some parts of the website (for example, e-books or recorded webinars) are only available through registration form. Registration forms may ask for some or all of the following information:

- a. name,
- b. e-mail address,
- c. organization (company),
- d. country,
- e. city,
- f. phone number, and
- g. a profile description

When filling in a registration form, we also ask for your consent to get in touch with you. You may withdraw this consent at any time. For all other cookies, please see our cookie policy.

2. What is the purpose of collecting the personal data?

Based on the content you accessed, we may contact you with specific offers and promotions, through e-mailed newsletters.

3. What is our legal basis to collect and process these personal data?

We process your personal data to get in touch with you based on your express consent [Article 6 (1) a) of the GDPR]. If you represent an organization, we process your personal data to contact you based on our legitimate interest to approach your organization as a potential customer [Article 6 (1) f) of the GDPR].

On our website, some cookies are necessary for the website to open. These cookies come from CookieBot, DoubleClick.net, Hubspot, and Hotjar (see data processors later). Their purpose is as follows:

- a. Checking if your browser can receive cookies;
- b. Remembering your choice about marketing and convenience cookies;
- c. Distinguishing between humans and bots, in order to create more accurate statistics of the site visits;
- d. Remembering your browser or your session so that different parts of the website will know that you are the same visitor.
- e. Distributing the traffic across different web servers so you receive a faster response from the website.

Necessary cookies will not follow you to websites of third parties; they cannot be used to identify you or take personal information from you. We use these cookies out of our lawful business interest. Most of the time, these cookies prevent the website from asking you the same question again and again, or from being misdirected within various pages.

4. Who receives the personal data?

The data is used by us—we are the data controller—but we may use third-party service providers to process them further (see the list in the first section).

5. Will these personal data be transferred out of the EEA or to an international organization?

Because we use third-party service providers to store and process your data, they may be transferred outside the EEA. We only use specific third-party service providers, and we maintain appropriate data processing agreements with all of them.

6. How long do we store these personal data?

We store the data as long as you have a contract with us (in case you sign up for a trial version of a product, or make a purchase through the website); or until you instruct us to delete them; or until you withdraw your consent to use your data.

7. Where do the personal data come from?

We only use personal data we directly collect through our website.

8. Will we use automated processes to make decisions about the personal data?

We do not make decisions in an automated way which produces legal effects concerning you or similarly significantly affects you.

D.5. Detecting illegal copies of memoQ and collecting usage statistics as you use the memoQ application

1. What personal data are we collecting and processing?

If you download the memoQ application, it will check your license to determine legitimate use. When it checks your license, it will send data to memoQ to detect illegal copies and to collect usage statistics. It will collect and send the following information:

- a. the language of Windows,
- b. the user interface language of the memoQ application,
- c. a hash of the serial number of your copy (it is enough to distinguish between two copies of memoQ but not enough to identify the user),
- d. the edition of your copy (4Free, Translator Pro, or Project Manager),
- e. your IP address (to be used to determine the country you are located; the IP address is not preserved in the database).

Based on the above data, we cannot identify you, and we do not make any attempts to, either.

2. What is the purpose of collecting the personal data?

Checking your license to use memoQ, and detecting illegal copies; collecting usage statistics based on user language and country. We use these data to determine memoQ's performance in specific geographical regions and to make decisions about languages the product is localized into.

3. What is our legal basis to collect and process these personal data?

We process these data based on our legitimate interest to provide memoQ to licensed users only and to detect illegal copies. We also have a legitimate interest in learning about the usage of our product [Article 6 (1) f) of the GDPR].

4. Who receives the personal data?

No third parties receive the data.

5. Will these personal data be transferred out of the EEA or to an international organization?

The data will not be transferred outside the EEA or to an international organization.

6. How long do we store these personal data?

We store the data as long as you have a contract (license) with us, or as long necessary to calculate statistics and provide for historical data. Generally, we store the personal data until the expiry of the civil law statute of

limitation, which is 5 years counted from the event that might give rise to civil law claims (in this case, the last use of the license).

7. Where do the personal data come from?

The data are collected by the memoQ application.

8. Will we use automated processes to make decisions about the personal data?

We do not make decisions in an automated way that would result in legal effects that concern you or significantly affect you.

E. Your rights

In accordance with the rules of the GDPR, you may request

- a) access to personal data concerning you, i.e. information on what personal data memoQ Zrt. processes about you. You may also request a copy of this data, provided that this does not adversely affect the rights of others (right to access);
- b) the correction of personal data concerning you (right to rectification);
- c) the erasure of personal data concerning you (right to erasure; “right to be forgotten”);
- d) the restriction of processing your personal data. In this case, the respective data will be marked and may only be processed by memoQ Zrt. for certain purposes (right to restriction);
- e) to receive the personal data provided by you to us in a structured, readable format and is also entitled to transfer this data to another data controller (right to data portability). The exercise of this right is subject to the condition that the data processing is based on your consent or the performance of a contract between you and us or on your request(s) to take steps prior to entering into a contract and that the data processing is automated.

You also have the right to object to the processing of your personal data in accordance with Art. 21 of the GDPR. When you object, we must stop processing your data, unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims. Exercising this right will not incur any additional costs. However, this right may only exist if the data processing is based on the legitimate interests of the controller or a third party. If your personal data is processed for direct marketing purposes and you object against such processing, we may no longer process your personal data for those purposes.

The rights above are not of absolute nature, and they may be limited due to reasons determined in the GDPR.

If the data processing is based on your consent, you have the right to withdraw their consent at any time, free of charge, without giving any reason. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

Furthermore, you have the right to lodge a complaint with the competent data protection supervisory authority competent in their Member State of residence or alleged infringement of the GDPR. In Hungary, the competent supervisory authority is the National Authority for Data Protection and Freedom of Information (“**NAIH**”) of which contact details are the followings:

Address: 1055 Budapest, Falk Miksa u. 9-11.; Hungary

Mailing address: 1363 Budapest, Pf.: 9.

Phone: +36-1-391-1400

Telefax: +36-1-391-1410

E-mail: ugyfelszolgalat@naih.hu

You may find the contact details of the competent supervisory authority for EU/EEA Member States with the associated contact details at the following link: https://edpb.europa.eu/about-edpb/about-edpb/members_en.

You may initiate court proceedings in certain cases for exercising their rights. However, we recommend that a complaint is always directed to us in the first instance.

You can also contact the information security officer of memoQ Zrt. (Data-protection@memoq.com).

F. Security of personal data

Finally, we wish to point out that we make every effort to protect your personal data from data breaches or from unauthorized access, copying, or theft. To that end, we maintain an information security management system, certified against the ISO/IEC 27001:2017 standard. For more information, see [Appendix 3](#).

memoQ Privacy Policy

Appendix 1: Data processing activities

| Section | Data processing activity | Personal data collected | Legal basis of processing | Retention time |
|--------------------|---|--|---|---|
| D1 | Providing products and services to you or your organization | a. name, b. e-mail address, c. organization (company) (if applicable), d. country, e. city, f. phone number, g. your purchase history, and h. a profile description | fulfilment of contract | as long as we have a contract with you, and for 5 years after our contract ends; for billing data, this is 8 years from the last transaction per legal requirement |
| D1 | Market research or targeted or retargeted marketing communication to existing customers | see above | legitimate interest (business entities) or consent (private individuals) | see above |
| D2 | Reaching out for information or feedback | Name and e-mail address (through 3 rd -party provider) or anonymous data collection | legitimate interest (business entities) or consent (private individuals) | Generally, until the expiry of the civil law statute of limitation, which is 5 years counted from the event that might give rise to civil law claims |
| D3 | Assist users to register for or participate at an event | Name, e-mail address, and potentially the name of company your work for; Responses to polls and other input if it exists. <i>For e-learning courses:</i> Name E-mail address Company name Country Billing address VAT number if applicable Complete course and quiz history Purchase history (spending amounts) Necessary cookies on websites | fulfilment of contract (events, e-learning courses) or legitimate interest (in case of necessary cookies) | Generally, until the expiry of the civil law statute of limitation, which is 5 years counted from the event that might give rise to civil law claims |
| D4 | Assist, learn about, and provide some documents/services to visitors of the website | No personal data are necessary to browse the website. Forms collect the following (or less): name, e-mail address, organization (company), country, city, phone number, and a profile description | legitimate interest (business entities, and for necessary cookies), express consent (private individuals) | As long as you have a contract with us (in case you sign up for a trial version of a product, or make a purchase through the website); or until you instruct us to delete them; or until you withdraw your consent to use your data |

| Section | Data processing activity | Personal data collected | Legal basis of processing | Retention time |
|--------------------|---|--|---------------------------|---|
| | | Necessary cookies for a) cookie management b) cookie choice, c) distinguishing human visitors, d) remember returning visitors, e) website performance | | |
| D5 | Detecting illegal use and collecting usage statistics (country, language, edition) as you use memoQ | <p>Collected by memoQ:</p> <ul style="list-style-type: none"> a. the language of Windows, b. the user interface language of the memoQ application, c. a hash of the serial number of your copy (it is enough to distinguish between two copies of memoQ but not enough to identify the user), d. the edition of your copy (4Free, Translator Pro, or Project Manager), e. your IP address (to be used to determine the country you are located; the IP address is not preserved in the database). <p>Based on the above data, we cannot identify you, and we do not make any attempts to, either.</p> | Legitimate interest | a maximum of 5 years (this is the expiry of the civil law statute) counting from last license use |

memoQ Privacy Policy

Appendix 2: External Data Processors

| Service | Purpose | Data collected and processed | Privacy Policy section |
|-----------------------------|---|--|---|
| aha.io | receive and respond to feature requests and ideas related to the product | Name, e-mail, profile picture, language, time zone + usage | D.2. |
| Atlassian Jira | Issue tracking and agile project management | personal data may be embedded in testing data | D.1. , D.2. |
| CodeTwo Email Signatures | Apply unified and branded signatures to outgoing e-mails | outgoing e-mail may contain personal data; CodeTwo do not look at them | D.1. |
| Hotjar | collect usage information and insights through online services; no direct personal identification | Usage information, potentially linked to cookie identification or user login | D.1. , D.4. |
| Hubspot | Customer Relationship Management (CRM) system: store and process main customer information with detailed profile data, execute sales and marketing automation based on the data; send marketing communication e-mails | Name, e-mail, address, phone number, affiliation, purchase and usage history, geography, sector, user category | D.1. , D.3. |
| In Mid Air ERP | central accounting system | name, billing information, purchased items, invoice sums | D.1. , D.3. |
| Microsoft 365 | General cloud infrastructure for internal operation | all customer data internally | D.1. |
| Microsoft Azure | Hosting customer data and services | data added by customer | |
| Postmark | transactional e-mailing, some marketing communication | name, e-mail address, e-mail contents | D.1. |
| SurveyMonkey (Momentive.ai) | Collect answers on survey forms; receive user or customer feedback to improve service or enhance customer (profile) data accuracy | name, e-mail, survey contents | D.2. , D.3. |
| Szamlazz.hu | Invoicing system | name, billing information, purchased items, invoice sums | D.1. , D.3. |
| Thinkific | E-learning platform where memoQ prospects, users, customers can access custom e-learning courses provided by memoQ. | name, e-mail, course history, course progress information | D.3. |
| Zendesk | helpdesk system to process customer support requests | name, e-mail address, contents of support request | D.1. |
| Zoom | Webinar and teleconferencing system to host public webinars and other events | name, e-mail, country, affiliation | D.3. |

memoQ Privacy Policy**Appendix 3: Technical and Organizational Measures**

At memoQ, we do everything in our power to protect your data, especially personal data. Among other things, we do the following:

1. Data minimization: We do not collect and process more data than absolutely necessary to do our job.
2. We operate an Information Security Management System by the ISO27001:2017 standard. This system includes strict user authentication (using multi-factor authentication), monitoring and enforcing user permissions where no-one in the company gets more permissions than absolutely necessary for their jobs.
3. Regular vulnerability tests on our own systems and systems operated by us.
4. Regular information security training for our staff and contractors.
5. Regular monitoring and liaising with external data processors. This includes regular updates to the data processing agreements, as well as attempts to control the location of data storage.
6. Information Security Governance team to oversee and ensure the monitoring and the response to information security incidents.
7. Regular legitimate interest balancing tests and data transfer impact assessments to ensure legal basis of processing.