

Privacy policy

1. General

At RiVe Juridiska Byrå, we want you to feel secure when you provide us with your personal data. This policy explains how we obtain, use, disclose and store your personal data.

2. Who is the personal data controller?

2.1 RiVe Advokatbyrå AB, with corporate ID number 556892 – 8369 and address at Box 338, 781 24 Borlänge, is the personal data controller for processing your personal data when we provide services and in other contact with us such as visits to our offices or via e-mail and telephone. As the personal data controller, we are responsible for ensuring that your data is processed correctly and securely.

2.2 According to the Electronic Communications Act, which entered into force on 1 July 2011, those who visit a website that uses cookies must be informed of that fact.

We wish to inform you that we use so-called "cookies" on this website. A cookie is a text file that is stored on your computer. It contains no personal data, but helps us arrange our website to make it unique or to provide recurring functions and features on the website. They are used for functions that provide information on what's new since the user last visited the website in question. As a user, you can use your browser settings to block us from being able to store cookies on your computer. However, if you choose to block cookies, some features of this website will cease to work correctly.

3. What personal data on you do we process?

We collect and process different categories of personal data on you as a client when you issue an order for our services or when you contact us.

Contact details such as name, title, e-mail address, telephone number, nationality, gender, age, income, employment history, customer identification number, identification information such as personal identity number and corporate ID number, services ordered, order date, order history, credit information, correspondence with us, audio recordings of calls, notes, e-mail communications, computer identification that can trace an individual computer and devices, device information, time zone, operating system, IP address, location information, educational level, any known public or political background (to protect officials in particularly vulnerable or sensitive positions) and any other information that you yourself provide or that otherwise emerges on you in connection with the performance of the assignment.

4. From what sources do we obtain data on you as a customer?

4.1 We obtain your personal data directly from you when you issue an order for our services, visit our website or, in general, when you contact us or have been in contact with us or when that data is supplied to us by you yourself or is obtained by us in other ways when carrying out the legal assignment for which you engaged us. Information on you is obtained on these occasions to enable you to enter into an agreement with us and to enable us to provide you with services and safeguard your legal interests and rights through the assignment for which you engaged us.

Privacy policy

5. The purpose for which your personal data is processed

We process data on you to enter into agreements or comply with existing agreements with you, for example for carrying out the legal assignment for which you engaged the firm. The firm must also store certain data for a particular period in order to fulfil obligations under the Bookkeeping Act and must also save certain data to safeguard its own interests, such as to protect it against crime and abuse and in the event that any litigation arises to which the firm is a party.

6. For how long do we store your personal data and is it disclosed to anyone else?

6.1 We will store your personal data for as long as is necessary to fulfil the purposes for which we hold your personal data. The length of time depends on the purpose of the assignment in question. Each week, we remove personal data that no longer needs to be stored.

6.2 We may disclose your data to foreign authorities if such is required under an imperative law in Sweden or an imperative decision by a public authority.

6.3 We may disclose your data to Swedish authorities such as the Swedish Tax Agency, the Police Authority, the Financial Supervisory Authority, the Security Police, the Swedish Armed Forces or others to which we are required to disclose your personal data under an imperative law or decision by a public authority. We are not required to report any suspected or known offences committed by a client, except for suspicions of terrorist financing and money laundering. The categories of data we disclose on any such occasion consist of data that the firm is required to disclose under an imperative law or decision by a public authority. We may also disclose your personal data if so required to enable us to safeguard our own interests, for example in the case of disclosure to the Swedish Enforcement Authority during recovery of payment from a former client or for our own litigation in a court, supervisory procedures, control and accounting measures or any similar contexts relating to a public authority in which the firm is a party and disclosure of certain personal data is intended to protect the firm's interests or rights.

6.4 We may disclose your personal data to an expert engaged for the assignment or to our own subcontractor, for example, if any expert or subcontractor has been engaged for the performance of the legal assignment you ordered.

6.5 We will never sell or transfer your personal data to a third party.

7. Your rights?

7.1 We are responsible for ensuring that your personal data is processed correctly and in accordance with the law. We will correct, de-identify, delete or add data according to requirements at any given time. You can also request correction of inaccurate data. You are entitled to access personal data stored on you. However, in the case of a repeat request, you may be charged an administration fee for processing the repeat request.

7.2 Contact regarding correction or disclosure of personal data is managed (unless you are a client known to us) only through a physical visit to our head office. This is because the firm must carry out identity checks before an individual's personal data can be disclosed since the firm is the personal data controller and must therefore, by law, adopt necessary measures to protect the personal data.