

Privacy and Data Protection Policy

SILBO SELECT takes the issue of security and data protection very seriously. This policy has been designed to meet the requirements of GDPR (General Data Protection Regulation) a European Union statutory instrument which aims to harmonise European data protection laws. In all matters of personal information data, we adhere to guidelines published in the United Kingdom Data Protection Act of 1998.

SILBO SELECT is committed to ensuring that your privacy is protected. This Privacy Policy describes how we use the personal information that we collect from you, or that you provide, when you:

- visit any of our websites or portals (the "Website")
- use the recruitment consultancy and agency services (together the "Services") that we provide
- We also collect personal information from you when you communicate with us for any reason, including by email, postal mail or telephone, and when you use our Services

Information We Collect

CANDIDATE DATA: There are two main ways in which we collect your personal data:

1. Directly from you; and
2. From third parties.

We collect personal information from you through forms, which may be on paper or on our Websites, such as when you contact us to receive information on or register your interest in a current vacancy to access our Services. We also extract information from your CV or resume as this helps us develop an accurate picture of you, your skillset and your ambitions. Where appropriate and in accordance with local laws and requirements, we may also use your personal data for things like marketing, profiling and diversity monitoring. Where appropriate, we will seek your consent to undertake some of these activities.

We will only share your information with prospective employers to increase your chances of securing the job you want.

- CLIENT DATA: There are two main ways in which we collect your personal data:
 - 1 Directly from you; and
 - 2 From third parties (e.g. our Candidates) and other limited sources (e.g. online and offline media).

The main reason for using Client data is to ensure that the contractual arrangements between us can be properly managed and help our relationship run smoothly.

We only share your data and information with certain Candidates to facilitate the recruitment process.

Safeguarding Data

We are committed to taking reasonable and appropriate steps to protect the personal information that we store from misuse, loss, or unauthorised access. To achieve this, we have a range of technical and organisational measures. These include measures to deal with any suspected data breach.

Data Retention

If we have not had contact with you (or, where appropriate, the company you are working for or with) for two years, we will attempt to contact you to update our information and renew your consent to allow us to retain your data. If we are unable to renew your consent within an additional thirty days we will erase your personal data from our systems unless we believe in good faith that the law or other regulation requires us to preserve it (for example, because of our obligations to tax authorities or in connection with any anticipated litigation)

Your rights to access, amend or remove data

If we already hold your personal data, you have rights in relation to it. To get in touch about these, please contact us. We will seek to deal with your request without undue delay, and in any event in accordance with the requirements of any applicable laws. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

- **Right to withdraw consent:** Where we have obtained your consent to process your personal data for certain activities (e.g. profiling your suitability for roles), or consent to market to you, you may withdraw your consent at any time.
- **Right to object:** If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (legislation allows us to extend this period in some cases). Generally, we will always respect your position if you disagree with us using your information.
- **Data Subject Access Requests (DSAR):** Because the data we hold relates to you, you can ask us to confirm what information we hold about you at any time. You can also ask us to modify, update or delete such information. At this point we may simply comply with your request or, do one of the following:
 - we might request that you verify your identity, or ask for more information about your request; and
 - where we are legally permitted to do so, we may decline your request, but if we do decline your request we will clearly explain why.
- **Right to erasure:** In some situations (e.g. where we have processed your data unlawfully), you have the right to request that we "erase" your personal data. We will

respond to your request within 30 days and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will delete your data but will generally assume that you would prefer us to keep a note of your name on our register of individuals who would prefer not to be contacted. That way, we will reduce the chance of you being contacted in the future where your data is available to us in later, unconnected circumstances. If you would prefer us not to do this, you are free to say so.

- Right of data portability: If you wish, you have the right to transfer your data from us to another data controller. We will help with this – either by directly transferring your data for you, or by providing you with a copy in a commonly used machine-readable format.

SSPRIV0418