

Steelcase Talent Privacy Policy

Respecting your privacy is essential to us. We respect the privacy rights of all individuals and we are committed to handling personal data responsibly and in accordance with applicable law. This privacy policy set out what types of personal data we (Steelcase Inc and its affiliates) may receive from you directly or from your interaction with us, how we may use it, who we may share it with, how we protect it and keep it secure and your rights around your personal data about you as candidates and future hires.

This notice is not intended and shall not be read to create any express or implied promise or contract for employment, for any benefit, or for specific treatment in specific situations. Nothing in this notice should be construed to interfere with Steelcase's ability to process employee data for purposes of complying with its legal obligations, or for investigating alleged misconduct or violations of company policy or law, subject to compliance with internal policy and local legal requirements.

Steelcase's processing of personal data is in all cases subject to the requirements of local law, internal policy, and any consultation requirements with worker representatives (where appropriate). To the extent this notice conflicts with local law in your jurisdictions, local law controls.

Who we are ?

Steelcase Inc is responsible for the personal data that you share with us, as well as each entity of Steelcase Group that interacts with you as your potential future employer. When we say “Steelcase”, “us”, “our”, “we”, this is who we are referring to.

Steelcase is the Data Controller for the purposes of applicable data protection laws.

Steelcase Inc –901 44th Street SE, Grand Rapids, Michigan 49508 USA, represented by DeKoekkoek, Matthew.

Data we may collect from you directly

Type of data collected	Purpose / Activity	Lawful basis for processing	Data retention duration
<p>Online Browsing Information collected by cookies or similar technologies as part of your browsing on Steelcase Talent Website and/or on third-party website.</p> <p>Depending on how much you are interacting with us, those data may include :</p> <ul style="list-style-type: none"> • Data related to your use of our websites/ app • Where you came from • Pages you looked at • Content you click on or tap • Jobs you search • Duration of your visit 	<p>Deliver proper functioning of our website</p>	<p>Legitimate interest to improve our services</p>	<p>After 6 months of inactivity</p>

<ul style="list-style-type: none"> Jobs you selected to create your basket 			
<p>Technical Information</p> <p>Depending on how much you are interacting with us, those data may include:</p> <ul style="list-style-type: none"> IP Address Browser information Device information A unique identifier granted to each visitor and the expiration date of such identifier 	<p>Ensure the website / app is secure , safe and protect you against fraud or misuse of our websites or services .</p> <p>Run statistics :</p> <ul style="list-style-type: none"> To avoid visitors to be recorded twice, To know users’ reaction to our content and campaigns To improve our offers To know how you discovered our websites 	<p>Legitimate interest to secure our tools</p>	
<p>Newsletter Subscription</p> <p>When registering to our Website/ app, you can choose to opt-in to Newsletters.</p> <p>Depending on how much you are interacting with us :</p> <ul style="list-style-type: none"> Email address Name and surname Personal description or preferences Social media profile 	<p>Send you marketing communication</p> <p>Run analytics statistics</p>	<p>Consent</p>	<p>Till you decide to opt-out</p>
<p>Job Alert Subscription</p> <p>When registering to our Website/ app, you can choose to opt-in to receive similar job Alert.</p> <p>Depending on how much you are interacting with us, those data may include:</p> <ul style="list-style-type: none"> Email address Browsing history Departments of interest Countries of interest 	<p>Send you job offers alert</p>	<p>Consent</p>	<p>Till you decide to opt-out</p>
<p>Applying with your LinkedIn profile (or any other social media) for job browsing</p> <p>When you decide to log-in using your LinkedIn profile, we have</p>	<p>To tailor our services for you:</p> <ul style="list-style-type: none"> To get a more personalized browsing experience To provide you with job recommendations 	<p>Consent</p>	<p>Maximum 2 years, and depending on countries after having received prior consent.</p>

<p>access to your “Basic Profile” information, notably:</p> <ul style="list-style-type: none"> • Name and surname • Headline • Location • Industry • Summary • Most recent items you have shared on linkedin • Specialties • Positions • Profile picture 			
<p><u>Candidate account creation and management, when applying to a job or a Program</u> Information collected during the creation of an account on Steelcase Talent websites/ apps, through a social media login or physically.</p> <p>Depending on how much you are interacting with us, those data may include:</p> <ul style="list-style-type: none"> • Name and surname • Email address • Address • Phone number • Photo • Birthday or age range • ID, Username and password • Preferred language • Work experience/ CV • Education History • Personal description or career related preferences • Social media profile 	<p>Manage your application</p> <p>Evaluate your competencies in a recruitment perspective</p> <p>Respond to your questions and otherwise interact with you</p> <p>Provide you with similar job opportunity</p> <p>Allow you to manage your preferences and applications</p>	<p>Performance of a service</p> <p>Consent</p>	<p>Maximum 2 years, and depending on countries after having received prior consent.</p>
<p><u>Recruitment process</u></p> <p>Depending on how much you are interacting with us, those data may include :</p> <ul style="list-style-type: none"> • Name and surname • Gender • Email address • Address • Phone number 	<p>Organize the recruitment process, assessments and interviews</p> <p>Share data within Steelcase Group to people involved in your recruitment process</p> <p>Evaluate your competencies in a recruitment perspective</p>	<p>Performance of a service</p> <p>Consent</p>	<p>Maximum 2 years, and depending on countries after having received prior consent.</p>

<ul style="list-style-type: none"> • Photo • Birthday or age range • Nationality • ID, username, and password • Marital status and family information • Personal interests • Preferred language • Application letter • Recommendations • Work experience / CV • Education history • Personal description or career related preferences • Social media profile • Financial information 	<p>Respond to your questions and interact with you</p> <p>Provide you with similar job opportunities</p>		
<p><u>Onboarding Process</u></p> <p>When you decide to accept a job offer, additional data may be required (depending on countries' local requirement) :</p> <ul style="list-style-type: none"> • National ID • Passport • Residency status • Work permit status • Social Security Number • Other taxpayer or government identification numbers • Criminal record data 	<p>Set up working contract</p> <p>Organize your integration to Steelcase</p>	<p>Performance of a contract</p>	<p>the time of the employment contract.</p>
<p><u>Enquiries</u></p> <p>Depending on how much you are interacting with us, those data may include :</p> <ul style="list-style-type: none"> • Name and surname • Phone number • Email address • Other information you have shared with us about yourself in relation to your enquiry. 	<p>Information collected when you ask questions relating to your application</p>	<p>Performance of a service</p>	<p>1 year</p>

Data we may collect from you indirectly

We may also collect personal data about you from third parties or public sources as needed to engage with you concerning job opportunities at Steelcase.

For example, before the course of your employment or assignment with Steelcase, we may collect information from public social media sources, such as your public LinkedIn profile, for recruitment purposes.

We also may conduct lawful background screenings, to the extent permitted by law, through a third-party vendor for information about your past education, employment, credit and/or criminal history.

Additionally, if there is an investigation of an employee matter, we may obtain information relevant to the incident from external sources including private parties, law enforcement or public sources like news sources and public social media posts.

How do we collect data about you ?

Sometimes you give this to us directly (e.g; when you create an account, when you contact us), sometimes we collect it (e.g. using cookies to understand how you use our websites/ app) or sometimes we receive your data from other third parties.

When we collect data, we indicate the mandatory fields via asterisks where such data is necessary for us to :

- Provide you with the service you have asked (e.g. to provide you with a newsletter)
- Assess your application for a position within Steelcase Group
- Answer to a request that you have sent us (e.g; to send you information about the progress of your application)
- Manage the recruitment and/or integration process (e.g. to identify you as a candidate for a job in our Application tracking System)
- Comply with legal requirements.

As a candidate applying to Steelcase job, if you do not provide data marked with an asterisk, this may affect our ability to review your application or the outcome of the recruitment process.

Depending on the purpose for which the data is used, the legal basis for the processing of your data can be

- Your consent
- Our Legitimate interest, which can improvement of our services and/ or securing our tools
- The performance of a service
- Legal obligations.

Change of purpose

We will only use your personal data for the purposes outlined in the table above or any purposes as may be reasonably compatible with the original purpose for which it was collected or when there is an alternative legal basis for the further processing.

Who may access your personal data ?

When you apply for a job, we may share your personal data within Steelcase Group, in a restricted way.

Given the global nature of our business and the centralization of certain business activities, personal data may be stored and processed internally at different group levels (e.g., global, regional, and local) for lawful purposes where Company or its affiliates, subsidiaries or service providers maintain facilities. We recognize that the EU/EEA countries have an omnibus data protection regime that generally restricts the transfer of personal information about individuals in the EU to the United States and certain other countries, unless there is “adequate protection” for such information when it is received.

To address this restriction and equal restrictions in other countries or regions, we apply a consistent set of rules to all transfers of personal information amongst Company entities regardless of their location whether within or outside of the EU/EEA countries. To provide adequate protection for transfers of personal data, Steelcase along with its affiliates, subsidiaries or trusted third party providers enter into the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (“Model Contract”) pursuant to European Commission Decision 2004/915/EC of 27 December 2004.

Please visit Steelcase Website, for further details on [Steelcase Group](#) and its [locations](#)

Whenever we permit a trusted third-party providers to access personal data, we will make sure the data is used in a manner consistent with this notice (and any applicable internal data handling guidelines consistent with the sensitivity and classification of the data). And we will only share your personal data with those who have a legitimate need for it, as follows:

1. In order to carry out the uses of personal data described above
2. To enable third parties to provide services to us.
3. To comply with our legal obligations, regulations or contracts, or to respond to a court order, administrative or judicial process, such as a subpoena, government audit or search warrant. Categories of recipients would include counter-parties to contracts, judicial and governmental bodies;
4. In response to lawful requests by public authorities (such as national security or law enforcement);
5. To seek legal advice from external lawyers and advice from other professional advisers such as accountants, management consultants, etc.;
6. As necessary to establish, exercise or defend against potential, threatened or actual litigation (such as adverse parties in litigation);
7. Where necessary to protect Steelcase, your vital interests, or those of another person;
8. In connection with the sale, assignment or other transfer of all or part of our business (such as a potential purchaser and its legal / professional advisers); or
9. Otherwise in accordance with your consent.

Please note that where legal requirements and/or internal policy limit the sharing of your data, Steelcase will respect such requirements.

Where We Store and Process Personal Data

As said above Steelcase operates at the global level and therefore personal data may need to be transferred to countries outside of where it was originally collected. For example, because we are headquartered in the United States, information collected in other countries is routinely transferred to the United States for processing. When we transfer your personal data to a different country, we will ensure that this transfer complies with applicable laws and legislation. And as said above, Steelcase has Model Contractual Clauses in place for the collection, use, and retention of personal data transferred from the European Union to other countries.

Our Retention of your Personal Data

Your personal data will be stored according to applicable laws or regulatory requirements and kept as long as is necessary to fulfill the purposes for which the personal data was collected. However, in no event, and only after getting your prior consent, your Personal Data will be kept for longer than 24 months.

We may retain some personal data to comply with our legal or regulatory obligations, as well as to allow us to manage our rights (for example to assert our claims in courts) or for statistical or historical purposes.

When we no longer need to use your personal data, it is removed from our systems and records or anonymized so that you can no longer be identified from it.

Security of Your Personal Data

Steelcase is committed to protecting the security of your personal data and taking all reasonable precautions to do so.

We use a variety of security technologies and procedures to help protect your personal data from unauthorized access, use, or disclosure. For example, we store the personal data you provide on computer servers with limited access that are located in controlled facilities, and, when we transmit certain highly confidential or sensitive personal information, we protect it through the use of encryption.

We contractually require that trusted third parties who handle your personal data for us do the same.

Your rights and choices

Data Protection legislation provides you with rights when it comes to the processing of your personal data. These are :

- ➔ The right to be informed
- ➔ The right to access your personal data, and obtain a copy
- ➔ The right to correct your personal data you have provided that is inaccurate,
- ➔ The right to delete your personal data that is no longer necessary to fulfill the purposes for which it was collected, or does not need to be retained by Steelcase for other legitimate purposes,
- ➔ The right to restrict / object processing
- ➔ The right to transfer your personal data to another company.

You can exercise your rights at any time by contacting us at privacy@steelcase.com .

Please note that we may request specific information from you to enable us to confirm your identity and right to access, as well as to search for and provide you with the personal data that we hold about you. We may, in limited circumstances, charge you a reasonable fee to access your personal data; however, we will advise you of any fee in advance.

Changes to this Privacy Notice

We may occasionally update this privacy notice.

If there are material changes to this notice or in how Steelcase will use your personal data, we will use reasonable efforts to notify you either by prominently posting a notice of such changes before they take effect or by directly sending you a notification.

We encourage you to periodically review this privacy statement to learn how Steelcase is protecting your personal data.

How to Contact Us

To ask questions about this Privacy Policy and/ or raise concerns about Steelcase's privacy policies, please contact Privacy@Steelcase.com.

Our addresses are:

Steelcase Inc., Attn: Global Privacy Lead, 901 44th Street SE, Grand Rapids, Michigan 49508 USA.

Steelcase S.A.S, Attn: Data Protection Officer, Espace Europeen de l'Enterprise, Schiltigheim 67300 France.

