Cloudflare Group of Companies

Candidate Privacy Notice

When you apply to work with any of the Cloudflare Group of companies (Cloudflare, Inc. and its wholly owned subsidiaries as listed in our Privacy Policy (together, “Cloudflare” or “we”), we will collect the personal data contained in your application. In this case, we are a "data controller.” This means that we are responsible for deciding how we hold and use personal data about you.

This notice provides applicants (whether for an employee, worker or contractor position) with information about the personal data we collect, how and why your personal data will be used, and how long we will retain it. It also provides you with certain information that we are required to provide you under Applicable Data Protection Laws. Applicable Data Protection Laws means all data protection laws and regulations of the jurisdictions of the aforenamed Cloudflare companies that are applicable to the processing of personal data.

Your personal data will be processed for the purposes of managing our recruitment and hiring-related activities, which include setting up and conducting interviews and tests for applicants, evaluating and assessing the results thereto, conducting reference and/or background checks, and as is otherwise needed in the recruitment and hiring processes. We process your information as necessary for our legitimate interests (that is, the solicitation, evaluation, and selection of applicants for employment) or where we have your consent to do so.

Data protection principles

We will comply with data protection laws and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Retained only as necessary for the purposes we have told you about.
- Kept securely.

Information we collect

In connection with your application for work with us, we will collect your personal data from you, from recruitment agencies (who may provide us with information such as CVs, and your named references. We gather, store, and use the following categories of personal data about you:

- The information you have provided to us in your resume, curriculum vitae, and/or cover letter.
- The information you have provided on our application form, including but not limited to name, title, address, telephone number, personal email address, date of birth, gender, employment history, and qualifications.
- Any information you provide to us during an interview.
- Test results (if applicable to the role) and work sample.
- Any information your references provide to us during a reference check.

In some cases, we may perform a background and/or credit check. When we do that, we may collect the following categories of information from a background check provider: name, title, address, telephone number, personal email address, date of birth, employment history, national ID, references, education. Section 4, below, provides more information about the "special categories" of Sensitive Personal Information we may collect, store, and use.

How we will use information about you

We will use the above-described categories of personal data we collect about you to:

- Assess your skills, qualifications, and suitability for the work.
- Carry out background and reference checks as appropriate and in accordance with applicable law.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.

It is in our legitimate interest to decide whether to appoint you to a role as it would be beneficial to our business to appoint someone to that role. We also need to process your personal data to decide whether to enter into a contract of employment or contract for services with you. We may use your information to re-engage with you for future employment opportunities.

If you fail to provide personal data

If you fail to provide information when requested, and that information is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require a credit check or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

Sensitive Personal Information we may collect, and how we use it

We may collect the following "special categories" of more sensitive personal data: information about your race or ethnicity, religious beliefs, sexual orientation and political opinions, if you choose to give us that information ("Sensitive Personal Information"). We will hold this information for the purposes of legal compliance, diversity and equal opportunities. We will use Sensitive Personal Information in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

In addition, we will collect, store, and use information about your criminal convictions history if we perform a background check. Typically, we perform background and/or credit checks if we would like to offer you the role. Such an offer is usually conditional on checks and any other conditions, such as references, being satisfactory. We are entitled to ask you to apply for a basic criminal record check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. Every role at Cloudflare requires a high degree of trust and integrity and therefore requires a criminal background check. Such background checks are conducted in accordance with applicable law.

We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

How we may share your personal data with third parties

We share the above-described personal data with third-party service providers, including other entities in the Cloudflare Group for business purposes. These service providers help us manage our recruiting and hiring processes, communicate with applicants, schedule interviews, and, when appropriate, conduct background checks. The service providers we use include:

- Greenhouse Software, Inc., a cloud services provider located in the United States of America and engaged by Cloudflare to help manage the recruitment and hiring process on Cloudflare's behalf.
- Talent Wall, a cloud services provider located in the United States of America and engaged by Cloudflare to help facilitate the recruitment process on Cloudflare's behalf.
- Interview Scheduler, a cloud services provider located in the United States of America and engaged by Cloudflare to help manage interview scheduling on Cloudflare's behalf.
- HireRight, a cloud services provider located in the United States of America and engaged by Cloudflare to help manage background checks on Cloudflare's behalf.
- Checkr, a cloud services provider located in the United States of America and engaged by Cloudflare to help manage background checks on Cloudflare's behalf.
- HackerRank, a cloud services provider located in the United States of America and engaged by Cloudflare to administer coding tests to candidates on Cloudflare's behalf.
- Eightfold, a cloud services provider located in the United States of America and engaged by Cloudflare to help manage and re-engage with previous applicants on Cloudflare's behalf.
- Urbanbound, a cloud services provider located in the United States of America and engaged by Cloudflare to assist with relocation for new hires on Cloudflare's behalf.
- Santa Fe Relocation, a relocation services company based in London, United Kingdom. They provide moving, destination services, immigration and assignment management services.
- Pana, a cloud services provider located in the United States of America and engaged by Cloudflare to assist with candidate travel during the interview on Cloudflare's behalf.

When you submit your personal data to any Cloudflare entity outside the United States, your personal data will be transferred to Cloudflare, Inc. in the United States. This transfer will be subject to appropriate additional safeguards under either the EU standard contractual clauses or the EU-US and Swiss-US Privacy Shield frameworks.

All our third-party service providers and other entities in the Cloudflare Group (Cloudflare, Inc. and its wholly-owned subsidiaries) are required to take appropriate security measures to protect your personal data in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes or to sell your personal data. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Cloudflare will not “sell” candidate personal information or “share” candidate personal information for the purposes of conducting behavioral or targeted advertising, as “sell” and “share” are defined under Applicable Data Protection Law.

How we secure your data

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors, and other third parties who have a business need-to-know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality. Details of these measures may be obtained from privacyquestions@cloudflare.com.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

How long we keep your information

We will retain your personal data for a period of up to 3 years after we have communicated to you our decision about whether to appoint you to a role. We retain your personal data for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal data in accordance with internal policies and procedures.

Your rights of access, correction, erasure, and restriction

Under certain circumstances, by law you have the right to:

- **Request access** to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully

processing it. If you are a California resident, you can also request the following:

- categories of personal information,
- the categories of sources from which the personal information is collected,
- the business or commercial purpose for collecting, selling, or sharing personal information,
- the categories of third parties to whom we disclose personal information, and
- the specific pieces of personal information that we have collected about you.

- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.

- **Request the limitation or restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it. If you are a resident of California, you may have the right to limit some uses of your Sensitive Personal Information.

- **Request the transfer** of your personal data to another party.

- **Non-discrimination** for exercising your privacy rights.

If you want to make a request in respect of your rights relating to your personal data, , please send your request to sar@cloudflare.com in writing.

Please note, that we may be required to ask you for further information in order to confirm your identity before we provide the information requested. Specifically, we may send a separate email to verify your email address on file. We will respond to your request as soon as reasonably possible. Should we not be able to respond to your request within thirty (30) days after receiving your request, we will inform you in writing

within thirty (30) days of the time by which we will be able to respond to your request. If we are unable to provide you with any personal data, make a correction or delete personal data requested by you, we shall generally inform you of the reasons why we are unable to do so (except where we are not required to do so under Applicable Data Protection Laws).

California residents also have the right to designate an authorized agent to make a request on their behalf. If you would like an authorized agent to submit a request on your behalf, we require that either (a) you must directly confirm with us that you provided the authorized agent permission to submit the request, (b) you must provide the authorized agent with your power of attorney in accordance with the law of the jurisdiction in which you are located, or (c) the request must otherwise be submitted in accordance with Applicable Laws.

You also have the right to object to our processing of your data where we are processing such data in our legitimate interests or to withdraw your consent for processing where our processing is based on having received your consent. To object or withdraw your consent, please contact us at sar@cloudflare.com.

Data protection officer

We have appointed a Data Protection Officer ("DPO") to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal data, please contact the DPO at dpo@cloudflare.com.