

Superhuman Global Candidate Privacy Notice

This Candidate Data Privacy Notice describes how Superhuman Platform Inc. and its subsidiaries (collectively, “**Superhuman**”) collects and processes your Personal Data when you apply for employment at any entity within the Superhuman group. By “Personal Data,” we mean information relating to an identified or identifiable natural person.

This notice does not apply to our data practices in the context of your role as a user of Superhuman’s services (our Privacy Policy applies there). For a short summary of what Personal Data we collect and why we collect it, see our quick table below. For more information, please keep reading our full notice.

What info?	What will Superhuman use it for?
<ul style="list-style-type: none">● Identity (e.g., name, nationality)● Contact info● Education and work experience● Information collected as part of your interview process● Application data (e.g., info in your résumé and from references)	<ul style="list-style-type: none">● To process your application and determine your eligibility for the role you have applied for● To communicate with you about future job opportunities● To comply with laws, internal policies, and other obligations● To communicate with you, including connecting you to Superhuman employees and vendors

What Personal Data do we collect and process?

We collect, store, and use Personal Data through the recruiting and hiring processes. We collect that information directly from you or (where applicable) from another person or entity, including from an employment agency, recruitment or professional networking website, background check provider, or reference. If you join our team, we will collect additional Personal Data throughout the course of engagement or employment with us.

We may collect the following information about you:

- Identification materials such as name, addresses, telephone numbers, email addresses,

photo, and government-issued identification documents (e.g., a driver's license or passport)

- Sensitive personal information such as government identification numbers (e.g., Social Security number, Social Insurance number), COVID-19 vaccination status, and driver's license number
- Professional information, including information provided through an application process (including in your résumé); information from interviews; recordings of your interviews (for which we would ask for your consent); work history; education history; information about skills, qualifications, experience, and preferences (e.g., mobility)
- Race/ethnicity data or other personal information that you voluntarily provide to Superhuman (e.g., veteran status)

When you share your references' contact details or other Personal Data with Superhuman, please keep in mind that you have a personal responsibility to obtain consent from them.

How do we use your information?

In our recruiting process, we collect, use, share, and store Personal Data for: ● Recruiting and workforce planning, including interviewing, communicating with candidates, job advertising for future potential roles, and selecting and hiring staff ● Legal matters and compliance, such as complying with regulatory obligations, seeking legal advice, and responding to and cooperating with legal requests and investigations

Superhuman also processes your information for background checks to the extent permitted by applicable law. Superhuman will not process your Personal Data for performing automated decision-making.

Who do we share your Personal Data with?

Superhuman discloses your Personal Data to third parties for reference purposes or who support our employment processes — including, for example, service providers for travel-booking and expenses process, vendors assisting in insurance and healthcare, payroll support services, etc. We may also disclose your information to other third parties to comply with legal obligations (including court orders and subpoenas), defend against potential, threatened, or actual litigation, or when we are legally obliged to share an employee's information with law

enforcement.

How long does Superhuman store your Personal Data?

If you are hired, Superhuman will store your Personal Data for the term of your employment and for as long as permitted, including as described in our employee privacy notice (which will be provided when you are onboarded as an employee) or as required by law to comply with our legal obligations or resolve disputes.

If you are not hired, Superhuman will retain your data for two years. However, we may store your data for extended periods if a longer retention period is required by applicable law or you provide your consent to maintain your data for future recruitment at Superhuman.

If you don't want us to retain your information for consideration for other roles, please reach us at recruiting.privacy@Superhuman.com. However, please keep in mind that Superhuman may retain your Personal Data if required by law or if we need to protect ourselves from legal claims.

How does Superhuman protect your Personal Data?

To protect the security of your Personal Data, we use state-of-the-art technical and organizational security measures, including access controls, firewalls, network intrusion detection, and more. We will not circulate your Personal Data outside of our systems or provide access to anyone not involved in our recruitment process (and, even then, only on a need-to-know basis).

EU, UK, and Switzerland residents: What is Superhuman's legal basis for processing your data?

Where applicable, the law requires Personal Data to be processed according to a legal basis. We process your Personal Data for the purposes described above based on the following legal bases:

- Legitimate interests when considering you for employment, managing our recruitment process, background checks, etc.
- Consent, which may be withdrawn by you at any time
- Necessity to comply with our legal obligations

- Necessity to protect vital interests

EU, UK, and Switzerland residents: Does Superhuman perform international data transfers?

For the purposes of Superhuman's recruitment operations, we may transfer your Personal Data internationally. International data transfers will be subject to additional safeguards under the standard contractual clauses approved by the European Commission. Please contact us at recruiting.privacy@Superhuman.com to obtain a copy of the standard contractual clauses.

EU, UK, and Switzerland residents: What rights do you have related to your Personal Data?

Under the General Data Protection Regulation (GDPR) and the UK GDPR, you have the right to request access to your Personal Data, to request that your Personal Data be rectified or erased, and to request that the processing of your Personal Data be restricted. You also have the right to data portability. In addition, you may lodge a complaint with an EU supervisory authority.

California residents: What rights do you have related to your Personal Data?

Under the California Consumer Privacy Act, California residents have rights regarding their Personal Data. Subject to certain exceptions, you may request:

- Access to your Personal Data, including the right to know the categories of Personal Data we have or will collect about you and the reason we will or have collected such information
- Correction of the Personal Data that we have or will hold about you that is inaccurate
- Deletion or removal of your Personal Data

There are certain exceptions to these above rights. For instance, we may retain your Personal Data if it is reasonably necessary for us (or our service providers) to provide a service that you have requested or to comply with law or to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity or prosecute those responsible for that activity.

We also will take reasonable steps to verify your identity before responding to a request. In doing so, we may ask you for verification information so that we can match at least two

verification points with information we maintain in our files about you. If we are unable to verify you through this method, we shall have the right, but not the obligation, to request additional information from you.

California law places certain obligations on businesses that “sell” Personal Data to third parties or “share” Personal Data with third parties for cross-context behavioral advertising. We do not “sell” or “share” the Personal Data collected pursuant to this policy.

You also have the right not to be discriminated against for exercising your rights.

Ukraine residents: What privacy rights do you have related to your Personal Data?

Candidates residing in Ukraine have the data privacy rights as described in [Article 8](#) of the Law of Ukraine on Personal Data Protection. For example:

- Access your personal data that GRAMMARLY UKRAINE LLC processes
- Deletion of your personal data from our systems
- Correction of the personal data that we have or will hold about you that is inaccurate

Please see more details about your privacy rights in Article 8 of the Law of Ukraine on Personal Data Protection.

Additional Information

- GRAMMARLY UKRAINE LLC is the controller of your Personal Data.
- In Ukraine, the statutory regulator is Ukrainian Parliament Commissioner for Human Rights. For contact details, please see [here](#).
- If you have any questions concerning this Notice, please reach out to recruiting.privacy@Superhuman.com.

Questions?

We may update this policy from time to time and will post the date of last revision. If you have questions about our collection, use, or disclosure of Personal Data, or to exercise one of the rights above, please contact us by email at recruiting.privacy@Superhuman.com or write to us at: Superhuman, Inc., 2261 Market Street, Suite 85232, San Francisco, CA 94114, United States.

ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

1. Я, "Кандидат" усвідомлюю, що ТОВ "ГРЕММЕРЛІ УКРАЇНА", з місцезнаходженням у м. Київ (Україна) (надалі – "Товариство") має необхідність накопичувати, зберігати та іншим чином обробляти певну інформацію про мене як Кандидата, що претендує на отримання роботи в Товаристві, для здійснення прав та виконання обов'язків, пов'язаних із розглядом моєї заявки на роботу, а також для інших цілей, прямо визначених у Загальному повідомленні про обробку персональних даних кандидата (надалі – "Повідомлення").
2. Виходячи з вищевикладеного, цим я надаю Товариству беззастережну згоду на обробку моїх персональних даних, наданих мною або отриманих Товариством від третіх осіб чи із загальнодоступних джерел, для цілей, зазначених у Повідомленні.
3. Я встановлюю наступний порядок відкликання цієї Згоди на обробку персональних даних: за моїм запитом на recruiting.privacy@superhuman.com згідно з Повідомленням. Якщо я здійснюю таке відкликання, Товариство може продовжувати обробку моїх персональних даних у тій мірі, наскільки це потрібно для виконання встановлених законодавством обов'язків та здійснення або захисту прав Товариства та/або третіх осіб, включаючи як це може бути необхідно для обґрунтування, задоволення або захисту правової вимоги.

CONSENT TO PROCESSING PERSONAL DATA

I, the "Candidate", hereby acknowledge that "GRAMMARLY UKRAINE LLC", a limited liability company located in Kyiv (Ukraine) (the "Company"), needs to accumulate, maintain, and/or otherwise process certain data about me as a Candidate applying for a job position at the Company to exercise its rights and perform its obligations connected with processing of my job applications, as well as for other purposes expressly listed in the [Global Candidate Data Privacy Notice](#) (the "Candidate Privacy Notice").

Based on the above, I hereby grant my free and unconditional consent to the Company for processing my personal data whether provided by me or received by the Company from third parties or from publicly available sources, for the purposes stated in the [Candidate Privacy Notice](#).

I hereby define the procedure for revocation of this Personal Data Processing Consent as follows: by my request to recruiting.privacy@superhuman.com as mentioned in the [Candidate Privacy Notice](#). If such revocation is made, then the Company has the right to continue processing my personal data to the extent necessary to fulfill statutory obligations or to protect or enforce the rights of the Company and/or of third parties, including as may be necessary for justifying, satisfaction or defense of a legal claim.